EXPLORING THE VIEWS AND PERCEPTIONS OF CYBERSECURITY AMONG SOUTH AFRICAN MILITARY OFFICERS

Kyle John Bester

Dissertation presented for the degree of Doctor of Philosophy in the Faculty of Military Science at Stellenbosch University

Supervisor: Dr Michelle Nel

Co-supervisor: Prof. Francois Vreÿ

March 2023

DECLARATION

By submitting this dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third-party rights, and that I have not previously, in its entirety or in part, submitted it for the purpose of obtaining any other qualification.

Date: March 2023

ACKNOWLEDGEMENTS

I am grateful to the Heavenly Father for being merciful and granting me the strength to embark on my doctoral journey.

To my wife, Dr Danille Bester, thank you for encouraging me and having my back whenever I felt like giving up. I appreciate your constant motivational messages and prayers, which I believe carried me through. Without you the journey would not have been possible. Thank you for supporting me on my academic writing journey and for the space to share my arguments and ideas with you.

To my son, Callum Bester, while you are still very young, thank you for giving me smiles and hugs. These meant a great deal to me, especially whenever I felt overwhelmed. Never stop smiling. I dedicate this dissertation to you, my son.

To my mother, Velma Solomons, thank you for the support and prayers and for being my sounding board whenever I feel life’s pressure. To my mother-in-law, Magdalene Arendse, your encouragement and support at home allowed me to write and press on with my dissertation – thank you. To my late mother, Tanya Bester, thank you for instilling a sense of grit in me and for emphasising perseverance – these qualities made me who I am today. You would have been proud.

To my colleague and friend, Dr Mbhiza, your encouragement and our conversations allowed me to persevere with this dissertation. Your friendship during this period meant a great deal.

I would like to thank my supervisors for their input and having patience with me throughout my writing of this dissertation. Thank you to Colonel (Dr) Michelle Nel for the knowledge you imparted to me and especially being willing to listen to my theoretical arguments on securitisation theory. Thank you to Prof. Francois Vreÿ for sharing valuable information with me regarding aspects linked to security and for your input related to my questions during supervision.

Thank you to the National Institute for the Humanities and Social Sciences (NIHSS) for funding my study and believing in me. The support you offered through the writing retreats allowed me to grow as an academic. The financial assistance of the NIHSS, in collaboration with the South African Humanities Deans Association (SAHUDA), towards this research is hereby acknowledged. Opinions expressed and

conclusions arrived at are those of the author and are not necessarily to be attributed to the NIHSS and SAHUDA.

To my editor, Mrs Wilna Swart, your words of encouragement and motivation allowed me to gain a sense of pride in my work. Your praise of my work during the last phase of my thesis allowed me to persist and regain my vision for this research project.

I would like to thank myself for enduring throughout this process. There were so many moments when things could have been different, but I persisted. To my future self, know that you are not an imposter and that you are enough.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: REVIEW OF LITERATURE ON CYBERSECURITY AS AN EMERGING THREAT

CHAPTER 3: SECURITISATION AS A THEORETICAL FRAMEWORK

CHAPTER 4: RESEARCH METHODOLOGY

CHAPTER 5: PHASE 1: CONTENT ANALYSIS (CA)

CHAPTER 6: PHASE 2: DESCRIPTIVE AND THEMATIC ANALYSES

CHAPTER 7: DISCUSSION OF INTERVIEW THEMES AND CYBERSECURITY ORIENTATION QUESTIONNAIRE (COQ) FINDINGS

CHAPTER 8: CONCLUSION

APPENDICES

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial intelligence
APT	Advanced persistent threat
BYOD	Bring Your Own Device
CA	Content analysis
COQ	Cybersecurity Orientation Questionnaire
CS	Copenhagen School
CSIR	Council for Scientific and Industrial Research
CSIRT	Computer Security Incident Response Team
DoD	Department of Defence
GCI	Global Cybersecurity Index
ICT	Information and communications technology
IR	International relations
IT	Information technology
ITU	International Telecommunications Union
NATO	North Atlantic Treaty Organization
NCO	Non-commissioned officer
NCPF	National Cybersecurity Policy Framework
PAIA	Promotion of Access to Information Act
PMG	Parliamentary Monitoring Group
RSA	Republic of South Africa
SA Army	South African Army
SAAF	South African Air Force
SAMA	South African Military Academy
SAMHS	South African Military Health Service
SAN	South African Navy
SANDC	South African National Defence College
SANDF	South African National Defence Force
SANSA	South African National Space Agency
SANWC	South African National War College
SPSS	Statistical Package for the Social Sciences
ST	Securitisation theory
SU	Stellenbosch University
UN	United Nations
US	United States
USB	Universal serial bus

ABSTRACT

Cyberspace is expanding at a rapid pace and extends its reach into the functioning of society. The pervasive nature of cyberthreats poses a significant security challenge to governments, businesses, organisations, and individual users. The contribution this study makes to the field of cybersecurity lies in its methodological approach to focusing on South African military officers, which is a hitherto under-researched subject in the South African domain. This study locates itself within the securitisation theory, which suggests that the military is a key tool in orchestrating a “security move”. This research explored perceptions of cybersecurity among South African military officers. Three sample groups were selected from institutions where South African military education, training, and development are provided. The military is often considered a unique population and is therefore frequently overlooked. The overarching aim of this study was to provide an exploration of the perceptions that govern the views of the military officer regarding cybersecurity in the South African National Defence Force. This study utilised a mixed-methods research design, which was conducted in two phases. A sequential design was also used in order to engage in the two phases of the study. Furthermore, this study utilised purposive sampling in Phase 1 of the research. Phase 1 used a qualitative approach by conducting semi-structured interviews at the South African National Defence College. Thereafter, the researcher constructed the Cybersecurity Orientation Questionnaire, which was quantitative. Cluster sampling was used for data collection in Phase 2. The researcher administered the questionnaire at two South African military education, training, and development institutions, namely the South African Military Academy and the South African National War College. In doing so, the researcher determined that cybersecurity awareness was a central factor in identifying cyberthreats and that amended security behaviour could play a role in resolving potential vulnerabilities. Furthermore, cybersecurity best practices and policy guidelines in the organisation were identified as requiring greater emphasis across units. Cultivating cybersecurity in the organisation was found to be challenged by the knowledge and experience relating to cyberspace usage. The way technology is viewed was also found to challenge prevailing efforts to develop a digital culture. The study found that a need exists for efficient technology in the organisation.

SAMEVATTING

Die kuberruimte brei teen ’n snelle pas uit en die invloed daarvan het die funksionering van die samelewing bereik. Die verreikende aard van kuberbedreigings verteenwoordig ’n betekenisvolle sekuriteitsuitdaging vir regerings, sakeondernemings, organisasies, en individuele gebruikers. Die bydrae wat hierdie studie tot die veld van kubersekuriteit maak berus in die metodiese benadering tot die fokuspunt van Suid-Afrikaanse offisiere in die militêre magte; ’n onderwerp waaroor dusver min navorsing in die Suid-Afrikaanse domein onderneem is. Hierdie studie is gelokaliseer in die teorie vir sekuritering, wat aan die hand doen dat die militêre magte ’n sleutelrol speel in die meebring van ’n “sekuriteitsbeweging”. Hierdie studie het ondersoek ingestel na die persepsies wat Suid-Afrikaanse militêre offisiere van kubersekuriteit het. Drie steekproefgroepe is by Suid-Afrikaanse instellings gekies waar militêre onderrig, opleiding, en ontwikkeling plaasvind. Die weermag word dikwels as ’n unieke bevolking beskou en word dus gereeld oorgesien. Die doel van hierdie navorsing was om ondersoek in te stel na die wyse waarop militêre offisiere in die besonder bewustheid van die kubberruimte en die konstuksie van kuberbedreigings in die konteks van die Suid-Afrikaanse Nasionale Weermag konseptualiseer. Hierdie studie het die gemengde navorsingsontwerp gebruik, wat in twee fases onderneem is. Die aaneenlopende ontwerp is verder gebruik om aan die gebruik van die twee fases van hierdie studie gestand te doen. Verder is ’n doelbewuste steekproefmetode vir Fase 1 van die studie gevolg. Fase 1 het ’n kwalitatiewe benadering gevolg deur die voer van semi-gestruktureerde onderhoude by die Suid-Afrikaanse Nasionale Weermagkollege. Daarna het die navorser die Kubersekuriteitsoriëntasievraelys, wat kwantitatief was, saamgestel. Die klos-steekproefmetode is in Fase 2 vir die insameling van data gebruik. Die navorser het die vraelys by twee Suid-Afrikaanse militêre instellings aangebied waar opleiding, onderrig, en ontwikkeling plaasvind, naamlik die Suid-Afrikaanse Militêre Akademie en die Suid-Afrikaanse Nasionale Krygskollege. Hierdeur het die navorser vasgestel dat bewustheid van kubersekuriteit ’n sentrale faktor in die herken van kuberbedreigings is en dat die aanpassing van sekuriteitsgedrag ’n rol in die uitskakeling van moontlike swakhede kan speel. Daarby is bevestig dat beste praktyk in kubersekuriteit en beleidsriglyne in die organisasie oor eenhede meer benadruk moet word. Daar is bevind dat die ontwikkeling van kubersekuriteit in die organisasie bemoeilik word deur

die bestaande kennis en ondervinding rakende die gebruik van die kuberruimte. Hoe tegnologie beskou word was ook as ’n uitdaging geïdentifiseer vir huidige pogings om ’n digitale kultuur te ontwikkel. Die studie het bevind dat daar ’n behoefte aan doeltreffende tegnologie in die organisasie is.

CHAPTER 1: INTRODUCTION

1.1 Introduction

The exploration of emerging domains such as cybersecurity and cyber warfare is viewed in the so-called grey zones (Wirtz, 2017). Grey zones are considered to be where criminal activity is performed – the space between active warfare and peacetime. Cybersecurity becomes more intricate when confronted with a variety of actors that are connected to criminal activities such as espionage and those committed by hacktivists (Stevens, 2020). Cybersecurity protects users and the larger part of society from harm done by data breaches performed by nefarious actors using computer systems (Stevens, 2020). Traditionally, security as a concept has been identified as negative, which implies a failure of the state to address the matter coherently and to introduce mechanisms to deal with challenges relating to normal politics (Wæver, 1998). However, there has been a shift away from the dominant emphasis on state interest. Instead, the focus is on multiple threat sectors in society. Threats originating from the maritime and cyberspace sector could be regarded as examples of this (Bueger, 2015; Larsen et al., 2022).

The increasing digitisation in Africa allows opportunities in multiple sectors to advance (Cilliers, 2020). However, Cilliers (2020) indicates that Africa's potential to promote stability among its various governments lies in developing its capacity to enforce security and advance human development. While Cilliers (2020) did not explicitly focus on cyberspace and cybersecurity, the concept of digitisation and technological integration is highlighted. Cyberspace thus becomes an important dimension in facilitating these aforementioned elements of development in Africa, as noted by Cilliers (2020). The users of cyberspace navigate between the physical domain (which requires devices and infrastructure) and the digital domain (which refers to software and cyberspace). Individuals, businesses, organisations, and government entities all interact with cyberspace in order to carry out their daily activities. These actors all interact with cyber matters and have the human component in common. The level of security attributed to the safety of these actors is linked to their level of awareness of security and potential threats, knowledge linked to precautions, online security behaviour, training and education in cybersecurity, and their level of trust in specific platforms (Chandarman & Van Niekerk, 2017; Mukiibi, 2019; Potgieter, 2018). The construction of security framed within the cyber domain is equally important for understanding cybersecurity and developing awareness thereof (Lehto, 2015). In expanding the aforementioned notions, the current reality of these modern times rests on the idea that the Internet is entirely integrated into people's lives (Zwilling et al., 2020). Lehto (2015) believes that the types of Internet-connected devices will increase over time. Zwilling et al. (2020) agree with this by suggesting that, along with the increase in the demand for Internet-connected devices, the issue of dependence on these devices cannot be avoided. However, along with a growing dependence on Internet-connected devices comes the risk of vulnerability and possible victimisation of governments, institutions, individuals, systems, and society at large.

1.2 Chapter overview

This chapter commences with a discussion of the proliferation and expansion of cyberspace in Africa. Internet usage and its implications for economic progression are emphasised. The focus then moves to the development of cyberspace in the South African context. The military is introduced, along with its connection to cyberspace as a domain. Furthermore, the chapter emphasises how cyberspace might be an emerging threat in the armed forces context. The focus then shifts to the South African military officer as a key human component in the cybersecurity process. The final component of this chapter is a discussion of the securitisation theory (ST) and how cybersecurity could be identified as an emerging threat.

The literature component is followed by the study's methodological considerations and the pertinent research questions. Firstly, the problem statement is presented, followed by the rationale of the research. The research questions and research design used in this study are discussed. The data collection, description of the participants, and methodological approach used to collect data are presented in this chapter, with reference to the three institutions where South African military education, training, and development take place. The final part of this chapter comprises the delineation of the chapters that follow.

1.3 Cyberspace as an emerging threat to armed forces

Cyberspace has increased the vulnerability of user information and sensitive state data. The volumes of data that are housed in government organisations might increase the vulnerability to potential cyberthreats and data hacks, which necessitates the need for precautionary measures to safeguard against security challenges (Toch et al., 2018). Furthermore, housing volumes of data gathered by cybersecurity systems may also pose a threat to users' privacy and even enable access to sensitive information connected to government organisations (Toch et al., 2018). Apart from infrastructural vulnerabilities, Zukic (2020) denotes that enhancing the knowledge of members of the military in matters relating to cyberspace is crucial as it is a maturing space that poses significant threats to national security. In addition, the armed forces' relationship with cyberspace and emerging technology can be described as a double-edged sword. While the domain and technology can be integrated to act as force multipliers, it may also pose a security risk to its personnel (Martin, 2020; Sayler, 2020). There is an expectation that the armed forces context is responsible for protecting national cybersecurity and preserving the cyber sovereignty of the state but the specific perception and expectation are not without vulnerabilities (Kolton, 2017).

Cybersecurity has become a global security matter for a variety of reasons: (1) nation states are advancing their cybersecurity capability in order to compete with their adversaries and nefarious groups (Lehto & Henselmann, 2020; Gazula, 2017), (2) cyberthreats and attacks have devastating consequences for the socio-economic capacity of a country; therefore, whatever measures are taken should ensure that civil society and national security interests are taken into account (Hlase, 2018), and (3) nations also invest in cybersecurity so that they are not only able to build and maintain modern armed forces, but also to use cyber capabilities and protect themselves from cybersecurity threats (Mulazzani & Sarcia, 2011). This includes armed forces that either lock onto civilian programmes or develop their own awareness programmes to equip their personnel to deal with potential cyberthreats. Moreover, a global movement has been started that is geared towards the establishment of military divisions that are mandated to create a firm stance towards and being a presence in cyberspace. According to the United States (US) Army Joint Chiefs of Staff (2018), there is a shift in the understanding and conceptualisation of cyberspace as a new domain of warfare, which demands a new way of thinking. Cyberspace has a connection with the physical world and while it is established in the realm of the information environment, it is firmly entrenched in the features of air, land, the maritime arena, and space (US Army Joint Chiefs of Staff, 2018). Cyber is therefore being integrated into military activities such as intelligence-gathering operations, surveillance measures, and reconnaissance activities (Sayler, 2020). Apart from military systems using cyberspace and emerging technologies, civil society is also becoming more dependent on cyberspace as more daily functions are associated with online platforms, where communication, education, and monetary transactions take place (Van der Waag-Cowling, 2017).

Furthermore, the borderless nature of cyberattacks and the rise of new technology with a wide range of capabilities pose greater geopolitical risks to nation states. This can be identified in the strategic air strikes launched by Israel against a Hamas target that was believed to be engaging in cyber warfare (Sverdlov, 2020; Allen, 2021). A distinction must be made regarding the military engaging in cyber warfare for offensive or defensive purposes. Kinetic warfare best describes an armed force being active and using means such as missiles and armed land vehicles along with weaponry to engage military targets. Kinetic activity is typically engaged in the four domains of warfare: land, air, sea, and space. The type of action taken during cyber warfare may dictate whether there are physical casualties or not. This view demonstrates the multifaceted capability of cyber warfare (Lehto & Henselmann, 2020; Gazula, 2017). Kinetic activity uses physical tools to carry out offensive and defensive measures (Lehto & Henselmann, 2020). However, cyber measures have the ability to jam certain tools or machinery and computers used for offensive tactics. Furthermore, the military is able to conduct cyberattacks and engage in cyber defence operations if there is a threat to national security. Cyber warfare[1] is a more cost-effective way of engaging in warfare. Gazula (2017) suggests that smaller militaries might benefit from engaging in asymmetrical warfare as an entire cyber warfare campaign can be launched for the cost of replacing a tank. Whereas kinetic warfare is considered expensive for smaller militaries, the use of a cyberattack for offensive and defensive purposes makes this domain attractive (Gazula, 2017).

Manley (2015) highlights that armed forces and private organisations often work in collaboration when engaging in issues such as cyberthreats that have national and

[1] It is worth noting that the terms “cyber warfare” and “cyberattack” are colloquial and do not necessarily represent the true meaning of war or an attack.

international implications for security. This indicates that civil-military collaborations are possible but are influenced by factors such as a restricted military budget and low broadband Internet connection (MacNamara, 2019; Lewis & Timlin, 2011). These collaborative efforts are often challenged by the anonymity of threats and the responses to threats (MacNamara, 2019). Stevens (2020) argues that the aforementioned makes it increasingly difficult for security clusters in nation states to engage with cybersecurity threats as cyberspace locates itself in grey zone territory, which makes it challenging to locate threat actors and enforce measures positioned between warfare and peace in the 21st century (Stevens, 2020; Lewis & Timlin, 2011). Furthermore, research that has been conducted in the field of cybersecurity focused on users external to the military context. The reason for this might be that the military is a site where information is considered restricted and is withheld from the public. However, not all information that is in flow in the military context can be declared as classified information. Owing to the integration of the Internet in operational activities, it has become increasingly difficult for the military to be immune to cyberthreats (Geers, 2011).

1.4 Information sharing and its importance to cybersecurity

The previous section noted that information is an important element for the armed forces context; however, not all information may be considered restricted. This section focuses on the notion of information sharing in organisational contexts by briefly addressing the activities and the prominence thereof in the South African context.

Information sharing is described as the activity where information is shared between the sender and the receiver (Pala & Zhuang, 2019). In the context of cybersecurity, information sharing becomes an integral element to the notion of trust in organisational settings. Information sharing is commonly associated with trust (Ahmad & Huvila, 2019). It is noted that there are two types of information-sharing activities that may be conducted in relation to cybersecurity, namely cyberthreat indicators and defensive measures. Cyberthreat indicators can be linked to information-sharing activities where the vulnerabilities of the organisation are disclosed. This information regarding the organisation’s vulnerability might be of a sensitive nature. Defensive measures, on the other hand, include information situational awareness, guidelines, and best practices to manage the threat (Pala & Zhuang, 2019). Linking the activities to the armed forces context, the researcher argues that to address cybersecurity in the organisation, both information-sharing activities need to be in place for effective communication on the subject matter. It is argued that within the information-sharing activities indicated, the perception of the interpretation of the activity becomes important. Information sharing is thus worth exploring, especially pertaining to elements of decision making, communication, and collaboration. Pala and Zhuang (2019) note that information sharing is an act that requires participation. With the notion of cybersecurity in organisational contexts, the sharing of threat information and acting thereon are essential for the foundation of security in any organisation.

From a wider focus on literature regarding information sharing, Ahmad and Huvila (2019) engage with the idea that change in organisational settings and trust among employees may have an impact on information-sharing activities. Falco et al. (2019) argue that the information-sharing activity is essential for the political value of decision making by the state to be considered by communities. In terms of local literature on information sharing, studies conducted by researchers in the South African context have focused on the role of trust in information-sharing activities (Chinje & Chinomona, 2015). Additionally, Nelwamondo and Njenga (2021) explored information-sharing activities between communities and the South African government. The researcher argues that in the South African context, the notion of information sharing has not yet taken a position where it is viewed within the armed forces perspective, although aspects of knowledge management practices have been engaged from a governmental perspective (Mange, 2019).

1.5 Impact of cyberspace on the South African National Defence Force (SANDF)

When viewing the role of the military as a state entity that is serving the executive, it must be highlighted that the role of the armed forces is to respond as directed by the political authorities to any external threat that is identified by the state (Montesh & Basdeo, 2012). This, according to Huntington (1957), can be carried out on the basis that an external threat compromises the civil liberties of its inhabitants when the equilibrium of the two tenets is threatened. Relating this to cybersecurity and the accompanied threats in this space, it should be emphasised that cyberthreats and defence have been a focal point in South Africa in recent times, as noted in the South

African Department of Defence's (DoD) annual report (Republic of South Africa [RSA], 2020b). The report states that a Cyber Defence Action Plan is currently in the approval phase, which is owing to immediate threats that could challenge the network security of the SANDF. The DoD's annual report (RSA, 2020b) suggests that data breaches and malware that continuously threaten network systems, as well as artificial intelligence (AI) used for hacking organisational systems, were identified as the main threats to DoD systems.

For example, Gerber (2017) reports that sensitive SANDF information pertaining to operations and personnel information was leaked on social media platforms. In addition, a memo related to the deployment of military members during the COVID-19 outbreak also surfaced online (Tshwane, 2020). The Policy on the Disclosure of Defence Information (RSA, 2011c) states that, ultimately, the dissemination and sharing of DoD information may only be done by the Chief of Defence Intelligence. The leaking of information and a breach of policy may also suggest that when security is not acknowledged and applied in practice as a priority, non-state actors may strategically disrupt and change the flow of data, which places the organisation and its users at greater risk (Bontea, 2017).

Tsagourias and Buchan (2018) further argue that legislation can be used by the state to exercise authority in cyberspace. However, enforcing legislation that can protect users and their information in cyberspace is but one way to create cyber defence other than by forming collaborative partnerships with private entities. This is reflected in the South African context by the efforts being made to create collaborative associations concerning cybersecurity measures. Daniels (2020) indicates that the Council for Scientific and Industrial Research (CSIR) collaborates with the SANDF regarding capacity building and knowledge sharing relating to cyber warfare. The reason for the state entering into these public-private partnerships is that most physical infrastructure is owned by the private sector. Entities that own critical infrastructure may therefore hold power and in the case of the state being unable to purchase and own all forms of critical infrastructure, might force the state into public-private partnerships (MacNamara, 2019).

Armed forces are dependent on cyberspace to secure national interests and maintain sovereignty (Nielsen, 2016). The increasing cyberthreat rate poses a major problem for armed forces as strategic operations now rest on a combination of conventional and unconventional approaches to adopting symmetrical and asymmetrical methods (RSA, 2015b; Grobler & Jansen van Vuuren, 2012). This development denotes that military Internet users must adapt their approach to cyberspace to lower vulnerabilities to unconventional or asymmetrical threats (Leenen & Jansen van Vuuren, 2019). The emphasis should therefore be placed on cybersecurity awareness training on the perception of cyberthreats, knowledge, and psychological constructs, which might indicate some possible risk factors relating to individuals (Van't Wout, 2019). Van der Waag-Cowling (2017) suggests that training and education in cybersecurity in the SANDF should consider following well-defined learning streams. In order to develop a cyber corps that is robust in mitigating threats, Van der Waag-Cowling (2017) asserts that the SANDF should adopt an approach through which its members can use tertiary education presented at various institutions and training offered by a tertiary military institution. This implies that the only relevant tertiary military education institution is the South African Military Academy (SAMA).

Modern armed forces tend to develop their cyber capabilities as force multipliers against the potential of being threatened by cyberattacks that could pose a danger to the flow of information (Bontea, 2017; Aschmann et al., 2015). Leenen and Jansen van Vuuren (2019) suggest that cultivating a digital security culture is important for military personnel. Furthermore, in order to cultivate a cybersecurity culture, the relevant stakeholders must be mindful of perceived knowledge and perhaps a generational gap in organisations (Leenen & Jansen van Vuuren, 2019). Creating a culture motivated by maintaining online security behaviour will promote the appropriate security behaviour in cyberspace, as well as when engaging in information security practices. Aschmann et al. (2015) suggest that educating military personnel is necessary for creating an African cyber army. Garcia (2017) adds that cybersecurity capacity is following a development pathway in the context of the South African armed forces.

This section indicates that cyberspace has entered the armed forces domain together with its own type of security risks. National security alongside a variety of threats and vulnerabilities is impacted by this emerging domain. One of these is the aspect of training and capacity building in military organisations to respond to the threats and opportunities that arise. The section that follows discusses the role of the military officer as a key human component in developing cybersecurity capacity, which has strong connections with the current section.

1.6 The South African military officer as a key human component in developing cybersecurity capacity

The SANDF serves in a democratic dispensation and is subject to the civil authorities of the state (Janse van Rensburg, 2019). It is worth noting that civil control of the military denotes the hierarchical nature of armed forces, which serve the executive branch of the state (Aldis & Drent, 2008). In addition, the relations between the state and the military rest on the idea that there is a mutually exclusive relationship between the political powers of a state, the armed forces, and society. The armed forces context is an important component in the quest for national security and they are essentially only as good as the human capital they recruit, train, and employ. The human factor is thus central to cybersecurity in organisations (Van't Wout, 2019).

Four central reasons underpin the human factor as being the weakest link in the cybersecurity chain, namely:

1) A military officer can be misled by nefarious online actors into disclosing sensitive organisational information that is important to operational activities by targeting human psychological vulnerabilities (Zwilling et al., 2020; Rauf, 2019).
2) The Internet is integrated into the everyday lives of people, especially with the use of mobile devices. The bridge between organisational and personal information being shared on convenient communication platforms such as WhatsApp may therefore pose a security risk to the online security credibility of the organisation (Ani et al., 2019).
3) The military officer might also be vulnerable and create involuntary or voluntary points of access for malicious software into organisational networks, which means that these officers might be exploited by nefarious actors to enter the organisation's network (Ani et al., 2018; McMahon, 2020; Rauf, 2019).
4) The increasing importance placed on information security and how users respond to threats by using security protocols and behaviour is a factor in individual cybersecurity awareness (Zwilling et al., 2020).

The South African military officer is therefore placed in a unique position concerning cybersecurity as he or she ultimately forms part of an organisation that needs to ensure that the sovereignty of the country is protected at all times (Van der Waag-Cowling, 2017; RSA, 2015b). It is further argued that the military officer is entrenched in the civilian domain, and functionally in the wider military community. The military officer is endowed with specific security mandates and accountability. This domain duality has largely to do with the nature of cyberspace and the element of threats that may target anyone. This view also alludes to the vulnerability of the human element; thus also posing a challenge for the military officer. What makes the military officer unique is that cyberthreats might have a detrimental impact on a variety of sectors that are critical for the sound functioning of the country. In addition, cybersecurity threats do not discriminate, which implies an even greater risk to the armed forces and the sovereignty of a nation. Moreover, cyberthreats are not conventional and require the military officer to adapt to the cyber domain and an adversary that is unseen.

According to the National Cybersecurity Policy Framework (NCPF) (RSA, 2015b), the military is a key organisation in the South African security cluster that is responsible, along with other stakeholders, for preventing and managing cyberattacks and threats. The military officer must therefore not only protect his or her own individual cybersecurity, but must also be in a position to protect and maintain national sovereignty. The military has an interest in cyberspace as it allows for the identification of internal and external countermeasures, as well as increasing opportunities to achieve greater resilience against threats, thereby extending operational activities and protecting its own interests and maintaining national cybersecurity (Couldry & Mejias, 2019; Garcia, 2017; Bardwell et al., 2017; Nielsen, 2016; RSA, 2015b). Cybersecurity perception is an important component of the adoption and retention of security behaviours, as well as for understanding this (Jibril et al., 2020). Based on the aforementioned view, exploring the perceptions of the military officer concerning cybersecurity appears to be a way to contribute to achieving cybersecurity.

Consequently, further emphasis should be placed on exploring military officers' perceptions concerning cybersecurity as the human component has already been identified as the main vulnerability in managing security (McMahon, 2020). Military officers are but a small component of the military in comparison with the greater number of lower-ranking members such as non-commissioned officers (NCOs) and other members. The senior military officer is in a position to display leadership skills and is able to provide recommendations for policy and best practices, as well as issue guidelines in their respective units. Furthermore, senior military officers are primarily decision makers. Those who are in leadership and decision-making positions have the ability to influence the perceptions of lower-ranking officers. The knowledge of the senior military officer regarding a social phenomenon may influence the strategies that will be used in planned activities (Kacała, 2020; 2015). This section notes that the military officer is an essential component in the cybersecurity chain as they need to practise and speak security. This view is aligned with the importance placed on cybersecurity in the Defence Review (RSA, 2015a). The military officer can engage in decision making and inform cybersecurity directives; exploring the perceptions of these officers is therefore key to understanding the element of awareness and the precautionary behaviour applied in cyberspace. The element of decision making is an important facet in the role of the military officer, as they develop and execute policy and doctrine decisions, but are still vulnerable in their behaviour. Military officers are therefore custodians, as well as weak links, through their information-sharing behaviour. These military practitioners are key for maintaining cybersecurity in the SANDF, as well as for employing policies and directives. Military officers are said to have specialised skills and knowledge pertaining to the defence force but may also possess a higher form of abstract thinking (Djozo et al., 2015). In this regard, Djozo et al. (2015) argue that military officers have educational and professional experience, which supports the idea that they are active problem solvers and embrace collaborative learning. In addition, the creation of defence policy generally takes place at the national level (Louw, 2013). National security is therefore to a larger extent still influenced by the military and its members, in particular the officers.

The NCPF (RSA, 2015b, p. 29) states the following regarding the SANDF taking the stance of being a custodian of cybersecurity in South Africa:

> The Department of Defence and Military Veterans (DOD&MV) has overall responsibility for coordination, accountability and implementation of cyber defence measures in the Republic as an integral part of its National defence mandate. To this end, the Department will develop policies and strategies pursuant to its core mandate.

The direct quotation above suggests that the SANDF has been granted overall responsibility to direct and manage cyber defence activities in the country. The argument may be made that cybersecurity also threatens the safety of military officers; not only in the professional context, but also in their personal context. The elevation of cybersecurity as a contemporary threat to national security is therefore linked to the notion that the threat landscape is widening as the functioning of the armed forces is threatened, along with security in the public ambit.

1.7 Understanding cybersecurity from the securitisation theory (ST) perspective

The previous section focused on the role of the military officer as a key human element in the cybersecurity process. This section focuses on the study's theoretical framework of choice, namely ST. This study is positioned within the security studies discipline and explores cybersecurity threats as a new security challenge in the context of ST to understand how threats are recognised, communicated, and responded to. ST is used in this study to capture the security process aspect of cyber in the context of the armed forces and to highlight the actors involved. Cyberspace securitisation is an issue of contention, specifically in the use of policies and how threats are identified, as well as responded to through official governmental means (Bote, 2019). In order to describe securitisation, the constituent elements of its definition must be identified. Securitisation is defined as follows:

> ... the discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object and to enable a call for urgent and exceptional measures to deal with the treat (Buzan & Wæver, 2003, p. 491).

Buzan and Wæver's (2003) definition describes the securitisation process as emphasising the presence of a security issue that is moving to a level classified as an existential threat. An existential threat can be narrowly defined as a threat to survival (May et al., 1958). Not all threats can, however, be classified as existential or demand an emergency response (Philipsen, 2018). The traditional approach of ST has been criticised for being rigid and not flexible enough to address newer threats. This study engages with cybersecurity as a later conceptualisation of how threats enter national security agendas, with emphasis on non-traditional security threats emanating from cyber actions and vulnerabilities. According to Van Ooijen (2020), the way threats are verbalised and responded to can be measured on a scale. Philipsen (2018) denotes that not all security threats require an extraordinary response from actors in the securitisation process. Philipsen (2018) points out that security iterations change over time and that securitisation is never the same across contexts as new meaning is progressively added. Buzan et al. (1998) argue that through the securitisation process the extraordinary response is justified based on the severity of the issue. Securitisation denotes the process through which a normal threat transitions from the ordinary to existential and therefore acts as a threat to an individual’s safety. Floyd (2020) highlights that securitisation is not a once-off event, but rather a political process where issues are transformed into security threats through a series of steps over time. Floyd (2020) outlines the process of securitisation by stating the sequence, which commences with the securitising actor who engages in a speech act or makes a securitising move. The speech is geared towards a declaration about a referent object being threatened (Floyd, 2020). This is followed by the audience, who must accept the securitising move, which then enables the deployment of extraordinary responses required to deal with the perceived threat (Floyd, 2020). Philipsen (2018) highlights that these securitising moves may not always be applicable in all contexts and that the process of addressing a threat with extraordinary reactions is not always necessary.

Van Ooijen (2020) argues that the discourse regarding cyberattacks is gradually increasing and while the effects of the attacks can be felt in a physical space, the ultimate consequences are often only experienced by those with expertise in and access to the cyber arena. Cybersecurity can be seen as the ultimate response to threats in the digital space. Bourbeau et al. (2015) acknowledge that the state is by far not the only referent object that is threatened by security issues. Philipsen (2018) suggests that new actors may intervene and challenge the traditional conceptualisations of security. New actors may thus redefine elements of “what” and “who” constitutes a referent object other than the state. As the spectrum of national security is widened to embrace a collective system, one that is inclusive of technical and social systems, factors greater than the state and its political regime could be threatened, and often more severely so (Bourbeau et al., 2015). Philipsen (2018) notes that while there might be new actors in the securitisation process, new conceptualisations of security may still rely on older ideas of security; therefore not completely limiting the role of the military and the state. The development of ST thinking to include newer threats in the security debate allows for alternative conceptualisations of threats and security to be introduced. Adding to this, new actors, and institutions other than only politicians and the military, are able to enter, emphasise, and address threats through security measures (Philipsen, 2018). Security concerns are therefore no longer a strict or dominant political-military concern, but space is created for more actors to enter a broader range of security concerns to enter the securitisation process and debate.

Furthermore, Floyd (2020) suggests that perceptions are of central relevance as they establish the legitimacy of securitisation, although very little is mentioned in the literature about those who execute the securitisation process. It is therefore important to explore the perceptions of the actors that need to implement the securitisation process. The implementation of securitisation would follow after such a process has elevated cyberthreats in the overall risk profile of the country and its institutions. The ST directed the research questions of this study, which were formulated to explore the defining features of cybersecurity among South African military officers and as how dangerous they viewed cyberthreats to be to the national interest and that of their own organisation.

The SANDF recognises that cyberthreats are a serious concern and the perceptions of South African military officers of cybersecurity play an important part in how the organisation’s views of cyberthreats and responses unfold. The researcher also argues that the referent object is both the SANDF as an organisation and the military officer, which together represent the security attached to the human factor. The reason for this is that the military is an important factor in the security cluster, which maintains national security and carries out strategic operations relating to national security (Van der Waag-Cowling, 2017). Adding to the aforementioned information, it is important to establish why the South African military officer is an important element in the cybersecurity process, but more specifically their role in securitisation. Philipsen (2018) notes that security actors need to perform and speak security. The South African military officer takes on two positionalities in ST, namely (1) the military officer must implement the security measures as directed by the SANDF, and (2) the military officer must engage in a vocabulary act that acknowledges that cyber is a threat and that the topic requires the necessary attention. The military officer is also in a unique position to inform decision making and to inform the directives that are used in the organisation to address security issues. The military officer typically takes on a role of being involved in the planning, organisation, and execution of operations in the organisation. This role of being a security actor aligns itself with the notion that the securitising actor does not always have to be part of the political elite or powerful decision-making entities. The actor must merely speak security to capture the essence of the security threat (Philipsen, 2018). Philipsen (2018) expresses this role to distinguish from “anyone” becoming an actor by noting that the presence of power should be evident in the security process. However, it is worth noting that historically institutionalised actors still have a very strong hold on displaying power in the speech act.

It is argued that while the first two positionalities may take the form of performative actions, there is a third role that undoubtedly connects with the notion that the military officer is not isolated from society. This refers to the idea that while the military officer takes on a performative stance within the ST process, he or she may also be vulnerable to threats and is impacted by the security measures employed. Cybersecurity has become a defence responsibility as noted in the NCPF (RSA, 2015b). It is argued that the acting of security and speech acts beyond the military raised the prominence of cyber threats, which has led to the SANDF becoming a key actor responsible for maintaining cyber defence. This responsibility allows the military officer to enter the process of coordination, ensure accountability, and maintain cyber defence measures. These acts of ensuring cyber defence link with the notion that the military officer speaks and practises security, which is in alignment with the speech act and that security is a performative act.

Furthermore, there are many referent objects that need protection through emergency measures. Thus, although the state might be the referent object, as its national interests and sovereignty must survive at all costs, other referent objects also require consideration (Hirsch Ballin et al., 2020). The researcher believes that there are additional layers containing objects of reference that require survival and emergency measures to ensure their survival. The researcher also argues that if the threat becomes densely framed and repeated as a national security threat, it is bound to be taken up in the threat spectrum and that national decision makers must take note of it. It is worth noting that the new South African Minister of Defence highlighted in the budget speech debate on the Defence Vote 2022/2023 (RSA, 2022) that cybersecurity is one of the SANDF's primary defence directives by suggesting the following: "... protecting South Africa's intangible sovereignty through support to the National Cyber Resilience Initiative and ensuring Defence Digital Protection" (RSA, 2022, para. 44). This focus on cyber resilience is echoed in the South African Defence Review (RSA, 2015a). With the human factor (South African military officer) being the focus of this study, it is argued that the psychological vulnerabilities of the human must be protected as cyberthreats and attacks are engineered to exploit the behaviour and emotions of human users (Rauf, 2019). The discussion surrounding ST is developed in more detail in Chapter 3. The next section focuses on the problem statement of this study.

1.8 Problem statement

In the preceding section, the reviewed literature identified an increase in cybersecurity, as well as a theoretical framework that is able to capture the severity and increasing danger of threats.

The SANDF is linked with the cybersecurity debate and response to threats in cyberspace, along with several official policies, protocols, and legislation, as well as its own operating procedures and doctrine. With cyberthreats on the rise, it is of key relevance that the military human component, particularly military officers, has the knowledge and awareness to counteract cybersecurity threats in the digital domain (Bardwell et al., 2017). Exploring the perceptions of South African military officers of cybersecurity might provide insight into how the promotion and mitigation of cybersecurity threats are carried out. This leads to the question of how prepared and educated South African military officers are to fulfil this role of promoting or mitigating threats. In addition, this study focused on the exploration of the cybersecurity perceptions of South African military officers who were part of three cohorts at three different education or training institutions. The views of junior and senior military officers were important in this matter as they provided an indication of how the three cohorts approached cybersecurity. Moreover, the views of the three different cohorts were considered as sources that might also provide insight into how South African military officers choose to orientate themselves in cyberspace and how they apply their online security behaviour.

1.9 Research rationale

The overarching purpose of undertaking this study was to identify the significant gap that exists regarding knowledge production relating to the perceptions of cybersecurity among South African military officers (Van't Wout, 2019; Gcaza & Von Solms, 2017; Van der Waag-Cowling, 2013). However, regardless of the human element being the focus of the study, cybersecurity threats are posing a danger in the context of both civil society and the armed forces. Its escalation in both domains brings national security vulnerabilities into the mix. The Internet has transformed the manner in which individuals carry out their daily activities and, as a result, their dependence on technology and cyberspace. Cyberspace has become a beneficial tool to engage in communication, as well as to coordinate daily activities in the professional or personal space. Cybersecurity threats are increasing in South Africa, which requires users to have some knowledge and awareness of security behaviour and cyberthreats (Dlamini & Mbambo, 2019; Van't Wout, 2019). Taking all the aforementioned into consideration, it is important to highlight the interaction between humans and their behaviours as linked to maintaining cybersecurity (Ani et al., 2019). The human aspect that this study considered was therefore vested in the South African military officer. The individual user interacts with both the physical and digital space through official and personal connected devices. In addition, the military officer is not excluded from society and the researcher therefore argues that these officers also interact with the digital and physical space in their official and personal capacity. The response towards cyberspace and the potential threats it harbours requires an approach that centres on the human and experience, knowledge, behaviour, and values factors.

It is therefore important to place greater emphasis on cybersecurity awareness and the education of military officers (Bardwell et al., 2017). Bardwell et al. (2017) emphasise that education on cybersecurity threats is necessary for military officers to gain awareness of the topic. There is thus a need for the military officer to be agile and flexible, to meet the response to threats with efficient security behaviour, and to possess sufficient knowledge (Bardwell et al., 2017; Gcaza & Von Solms, 2017). Given the human element being the focus of this study, cultivating a cybersecurity culture in an organisation requires cognisance of the culture, values, norms, behaviour, knowledge, and experience of military officers (Aschmann et al., 2015; Van't Wout, 2019). Each military officer will have a different view of cybersecurity as various levels of exposure and training in cyberspace issues may have influenced these security-related perceptions. Apart from these facets, the level of awareness each individual has of cybersecurity may influence how users behave and apply security in the digital domain. Exploring these perceptions helps to provide an understanding of the contextual reality of South African military officers, as well as their view of security threats and vulnerabilities in this technical field (Van den Berg & Keymolen, 2017).

Hlase (2018) notes that cyberspace as a domain has produced new methods to address security issues. Research exploring the effects of and matters related to the manifestation of the Internet in economic, social, and political sectors is emerging and addresses the trends linked to digitisation in South Africa (Modiba, 2020; Naidoo, 2020). However, research highlighting the effects of the Internet does not necessarily focus on the armed forces context in South Africa. In addition, recent literature focusing on cybersecurity has not made the perceptions of the South African military officer a focus area (Leenen & Jansen van Vuuren, 2019; Du Toit et al., 2018). Moreover, literature on cybersecurity awareness in the South African context has become a central focus point, especially in organisational contexts (Chandarman & Van Niekerk, 2017; Gcaza & Von Solms, 2017; Van't Wout, 2019). This study expects to contribute to narrowing this gap in the literature by focusing on the human element in cybersecurity through investigating and recording the perceptions of selected military officers as part of South African society.

1.10 Research questions

The overarching aim of this study was an exploration of the perceptions that govern the views of the military officer of cybersecurity in the SANDF. The study explored how military officers conceptualised cybersecurity by specifically gauging their awareness and knowledge of how cybersecurity threats are perceived in the context of the SANDF. This aim was pursued by way of the primary research question of this study, which sought to ascertain the perceptions of South African military officers of cybersecurity. Furthermore, the exploration of perceptions assisted with viewing cybersecurity awareness through the lens of the military officer and their understanding of the subject matter, and consequently to draw certain inferences from their behaviour in cyberspace.

This study also pursued secondary research questions, which are presented below, to assist with answering the primary research question:

- How do South African military officers conceptualise cybersecurity awareness?
- How do South African military officers perceive cybersecurity threats within the SANDF?
- What are the perceptions of cybersecurity awareness through the lens of the military officer?

Overall, the study expected to contribute to the exploration of cybersecurity in the military context and to provide a multifaceted approach to exploring how perceptions might influence the awareness and behaviour related to cybersecurity in the SANDF.

1.11 Research design

Researchers pursuing a better understanding of social phenomena often integrate qualitative and quantitative approaches (Johnson et al., 2007). The combination of two approaches is known as a mixed-methods design (Johnson et al., 2007). The design of a study is pertinent as it can show how data may be obtained and how the methodological choices could guide these activities in the research process (Sileyew, 2019). This study followed a mixed-methods approach for two reasons: (1) the exploration of cybersecurity awareness was conducted in the context of the SANDF, and (2) the exploration of perceptions would assist the researcher in gauging military officers' levels of awareness of cybersecurity. Given these focal points, it was deemed appropriate to use both quantitative and qualitative approaches as doing so provided greater depth to the phenomenon central to the inquiry.

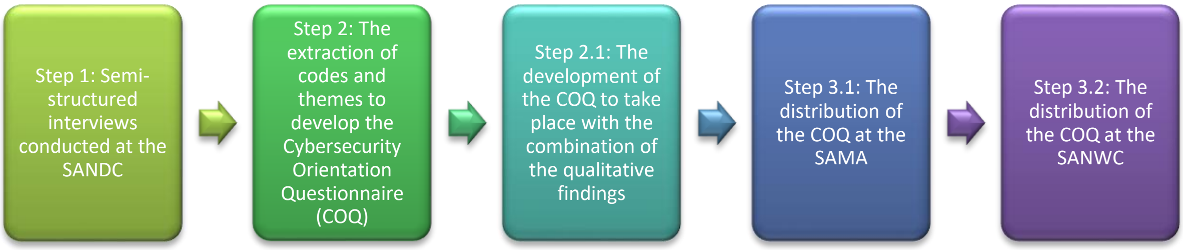
The exploratory sequential design is a technique used in mixed-methods approaches that consists of certain processes in the research that must be performed in a certain sequence (Roomaney & Coetzee, 2018). This study used the sequential design as it allowed the researcher to explore the perceptions and views of the military members by first engaging with the qualitative approach. The primary approach in the sequential design was therefore qualitative[2] and the focus was on the members of the

[2] The qualitative approach is associated with the interpretivist research paradigm that is interested in exploring the subjective worldviews of participants (Guba & Lincoln, 1989).

military. As part of the sequential approach, the second component of the mixed-methods approach was quantitative[3], which related to numerical data.

The first phase of the research utilised a semi-structured interview to gauge the perceptions and views of South African military officers at the South African National Defence College (SANDC). The second phase, which was quantitative, provided a structured questionnaire that focused on the ratings the participants provided in respect of facets related to cybersecurity. Two military institutions, SAMA and the South African National War College (SANWC), were the sites relevant to the second phase of the research. The presentation of the sequential process followed in this study is presented in Figure 1.1.

Figure 1.1: Map of sequential steps in the exploration of perceptions of cybersecurity


Step 1: Semi-structured interviews conducted at the SANDC
Step 2: The extraction of codes and themes to develop the Cybersecurity Orientation Questionnaire (COQ)
Step 2.1: The development of the COQ to take place with the combination of the qualitative findings
Step 3.1: The distribution of the COQ at the SAMA
Step 3.2: The distribution of the COQ at the SANWC

This study was cross-sectional, which denotes research conducted at one point in time and not over a prolonged period (Zangirolami-Raimundo et al., 2018). As stated earlier, the aim of this study was to explore the perceptions that govern the views of the military officer on cybersecurity in the SANDF. As alluded to above, to align the aim of the study with the selected methods, a mixed-methods approach was selected as it allowed the researcher to engage with the study’s objectives. In the mixed-methods design, the qualitative approach was considered appropriate for the exploration of certain individuals’ perceptions of cybersecurity. The qualitative approach thus formed part of Phase 1. The researcher used a semi-structured interview style to obtain the participants’ views. Consequently, as cyberspace is still considered an emerging domain of interest in the South African context, this study followed an exploratory approach, which at its core attempts to uncover something new in the social domain by engaging it in a research topic (Swedberg, 2018). The exploratory approach was deemed appropriate as cybersecurity among military officers and those

[3] The quantitative approach is grounded in the positivist research paradigm and is associated with the use of scientific methods to investigate phenomena (Comte, 1856).

in the armed forces context of the SANDF is a relatively new subject of interest in South Africa. The second approach used in the mixed-methods design was the quantitative approach. Phase 2 was also interested in the perceptions and contextual realities, which were derived from a questionnaire that explored the participants' functioning in the SANDF. The findings used in this phase played an integral part in the triangulation process. Furthermore, the mixed-methods approach allowed the researcher to engage with the study's objectives.

In addition, engaging in descriptive or explanatory research would not have done this study justice as it might not necessarily have explored the deeper social aspects related to cybersecurity from the view of the military officer. For that reason, exploring the perceptions and views of cybersecurity provided insight into how awareness of the topic was framed. Furthermore, exploring cybersecurity through the military members' lens and rank-related experience was expected to possibly provide insight into how they constructed security in this new, emerging domain.

1.12 Data-collection phases

The approaches used to collect data were used for triangulation[4] of the research findings. The sequential design highlighted that one of the two data-collection approaches should be used as the first and dominant approach. This study engaged in data collection in two phases. This section presents the two phases of data collection that were followed during this research.

1.12.1 Phase 1: Qualitative data collection

1.12.1.1 Purpose of Phase 1

The first phase focused on the collection of in-depth information from senior South African military officers as it related to the aim of the study and the secondary research questions. The purpose of Phase 1 was to lay the foundation for the development of the COQ. Furthermore, the focus of the first phase was to gain a qualitative perspective of the perceptions related to cybersecurity and institutional awareness of the phenomenon at the core of the study.

[4] Guion (2002) describes triangulation as a method utilised by qualitative researchers to verify and establish validity in research studies.

In order to obtain the perceptions of cybersecurity among a senior military sample population, face-to-face semi-structured interviews were used as a means to extract information from the participants. The SANDC was identified as the primary site of focus in Phase 1 as the college presents the most senior learning opportunities for senior officers of all arms of service. The SANDC offers professional military education and training. This site was identified as well positioned to address the research questions of this study as it is where senior military officers destined for general and flag officer ranks are trained and educated.

1.12.1.2 Description of the participants in Phase 1

The sample population for Phase 1 comprised senior military officers attending a year-long developmental course called the Security and Defence Studies Programme at the SANDC. These senior military officers has been exposed to the cyber concept in their respective units. Furthermore, the developmental course offered at the SANDC prepares senior military officers to function on a strategic level within the security environment, where they must deal with national security challenges. The Security and Defence Studies Programme focuses on developing critical and strategic thinking among senior military officers from all arms of service. The senior military officers are exposed to aspects focusing on leadership and strategy that are specifically in line with national security provisions (Defence Web, 2016).

1.12.1.3 Approach used to collect data in Phase 1

As indicated, semi-structured interviews were used to collect data in Phase 1. According to Adams (2015), semi-structured interviews are advantageous in mixed-methods studies when it is necessary to use questionnaires or undertake surveys at a later stage. Furthermore, it is also advisable for semi-structured interviews to be carried out in mixed-methods studies if the subject of the inquiry is emerging and requires exploration (Adams, 2015). The purpose of the selected data-collection technique was reliant on the availability of information in the military context. The sequence and aims of the study dictated the focus on military officers' perceptions and views of cybersecurity. The qualitative phase involved the researcher conducting face-to-face semi-structured interviews of between 25 and 45 minutes in duration. The items in the semi-structured interview guide were based on the literature and key themes highlighted in other research studies that aligned themselves to cybersecurity in the armed forces context (see Appendix A). The researcher approached the senior military officers located at the SANDC with interview questions that were linked to their experience of utilising cyberspace and how they navigated their online behaviour. The semi-structured face-to-face interview is said to fall between closed- and open-ended questions, which allows the researcher the flexibility to engage in further questions such as “how” and “why” (Adams, 2015).

1.12.2 Phase 2: Quantitative data collection

1.12.2.1 Purpose of Phase 2

The second phase of the study focused on engaging with two sample populations, located at the SANWC and SAMA. These two sites were important for Phase 2 of the study for purposes of triangulation. A quantitative approach was adopted for Phase 2, which included Likert-type items on a scale of 1 to 5. The findings obtained in Phase 2 assisted with the validation of the findings in Phase 1. The aim of including SANWC and SAMA participants was to increase the number of responses among a cross-section of senior and junior officers and to collect opinions of cybersecurity across institutions where officers undergo training and education. The second phase aimed to gain opinions related to the conceptualisation of cybersecurity awareness and the construction of threats in the SANDF. Phase 2 connected several chapters in this dissertation. The methodological considerations in Phase 2 are discussed in Chapter 4.

1.12.2.2 Description of the participants in Phase 2

The researcher used two sample population groups in Phase 2 of the research, namely officers at the SANWC and at SAMA. The sample group from the SANWC consisted of senior military officers who were enrolled for the Joint Senior Command and Staff Programme. The military officers at SAMA were studying towards a military degree and were junior officers.

1.12.2.3 Approach used to collect data in Phase 2

The second part, which was quantitative, focused on the ratings that SAMA and SANWC military officers attached to facets relating to cybersecurity. The COQ was used to collect data in Phase 2 (see Appendix E).

Phase 2 in the sequential process was relevant not only for constructing a basis for triangulation but also to focus on the development of the various items in the COQ that had a direct impact on the interpretation of the themes and sub-themes in Phase 1. The COQ also focused on short questions, which in turn focused on the narratives of the respondents from SAMA and the SANWC. Once all the data derived from the COQ had been collected, the researcher engaged in a data-cleaning process. Once completed, the data were transferred to the Statistical Package for the Social Sciences (SPSS) version 24 (IBM Corporation, 2016).

As highlighted, Phase 2 was descriptive in nature and aimed to answer the three secondary research questions and to achieve the aim of the study (see Section 1.10). Some theoretical features of ST and associated literature in Chapter 2 were used to construct certain items in the COQ. These scale items and short questions in the COQ allowed for the exploration of cybersecurity, which required in-depth analysis of how this emerging phenomenon is viewed in the South African military context.

1.13 Delineation of chapters

The introduction to this chapter included a short discussion of the proliferation and expansion of cyberspace in Africa. Thereafter, the development of cyber in the context of South Africa was discussed briefly. The chapter furthermore included a discussion of cyberspace as an emerging threat to the armed forces. The impact of cyberspace on the SANDF was also presented briefly in this chapter. In addition, the chapter contained a discussion of the military connection to cybersecurity. Thereafter, a discussion of how cyberspace is considered an emerging threat in the armed forces context was presented. A brief introduction to understanding cybersecurity from the ST perspective was presented. The focus of the chapter then moved to a review of the problem statement, research rationale, research questions, and the research design selected for this study. The data-collection phases at three SANDF training and education facilities for senior and junior officers used in this study were also presented in this chapter. Furthermore, the purpose of each research phase was explained. A description of the samples used for each research phase and the approach to collecting data concluded the discussion.

In Chapter 2, the literature review on cybersecurity as an emerging threat offers a discussion of the exploration of a definition of cybersecurity. The chapter also reports how the human element should be located at the centre of an operational definition linked to cybersecurity and provides a discussion of the complexity of cyberthreats. Thereafter, the chapter elaborates briefly on the impact of cyberthreats on society. In addition, the chapter offers a discussion of the legislative efforts by the South African government. Furthermore, the chapter focuses on cyberspace and the challenges it poses to sovereignty and the armed forces. The literature review proceeds by discussing the volatility of cyberthreats in respect of military personnel and the armed forces context. Moreover, a review of the literature highlights the cybersecurity efforts made in the SANDF. Furthermore, the chapter discusses the perception of risk when navigating cyberspace, information-sharing behaviour, and the creation of cybersecurity awareness.

In Chapter 3, securitisation as a theoretical framework presents the various views of security. This chapter also offers a brief discussion of what ST entails. Moreover, the chapter engages with the various security threats that have been emerging in the 21st century. The focus then shifts to the development of ST and the basis of how ST interplays with cybersecurity. The role of the securitising actor and the referent object is presented in this chapter, which allows for a more detailed exploration of how technification as a speech act occurs in the securitisation process. Furthermore, the chapter engages with critique of ST by pointing out the perceived pitfalls attached to the theory. The chapter shifts its focus to the military domain by presenting how cybersecurity has entered the military domain.

Chapter 4 addresses the research methodology, and provides an overview of the research design and paradigm that were used in this study. This chapter provides a discussion of the sampling and data-collection procedures that were used for Phase 1 and Phase 2 of the study. Furthermore, the data-analysis procedures used for each of the phases in this research are also discussed comprehensively. The challenges related to the data collection in the study are presented in this chapter, as well as the aspects of validity and reliability, credibility, confirmability, transferability, and dependability. Reflexivity as a tool against preconceived prejudices is also included.

Chapter 5 focuses on the content analysis (CA) of the interviews, and the extraction of themes and sub-themes from the interviews with participants from the SANWC. The main themes presented in this chapter are: (1) *knowledge production and training focusing on cybersecurity awareness*, (2) *challenges of trust with technology and among members,* (3) *the construction of a digital culture among members*, and (4) *the view on cyberthreats is constructed based on experiences in the physical domain*. Each main theme comprises sub-themes that are linked with the purpose of the chapter. The final section of the chapter provides a summary of the themes presented.

Chapter 6 deals with the COQ, and presents the administration and findings derived from the data produced by the SANWC and SAMA participants. The demographic information for both sample population groups, as well as the findings related to the four dimensions of the COQ are presented. The three themes that emerged from the short questions were: (1) *information sharing on best practices requires implementation*, (2) *cautionary behaviour is linked to the navigation of cyberspace*, and (3) *cybersecurity training and education as a way to enhance security measures*.

Chapter 7 contains a discussion of the findings related to Phase 1 and Phase 2 of the study and provides a contextualisation of the key findings that emerged from the data by highlighting the three sample population groups. A discussion of the conceptualisation of cybersecurity awareness among South African military officers and its connection to the primary and three secondary research questions with their various sub-themes forms the core of the chapter. Furthermore, this chapter allows for the findings discussed in Chapters 5 and 6 to be viewed comparatively and includes an analysis of the patterns presented across the three sample population groups.

In Chapter 8, a summary and conclusions drawn during the study form the bulk of the discussion. The chapter confirms the research aim and rationale, as well as the significance of the study, by reviewing the research questions. This chapter also presents a summary of the findings in relation to ST and identifies its limitations, opportunities arising from more recent submissions, and particular contributions made by this study. Thereafter, the chapter provides a review of the indicators found, which comprises the combined findings of Phases 1 and 2. The chapter then revisits the three research questions. Once these have been discussed, the chapter shifts its focus to addressing possible criticisms of the study. The chapter also provides a short discussion of the contributions this research makes and points to the utility of the COQ, supporting policy development, the delivery of cybersecurity in the SANDF, and the prospective scope for academic research.

1.14 Conclusion

With technology advancing at a rapid pace, more users are increasingly becoming connected to affordable devices, which could present opportunities economically and socially, but which could also pose threats and pitfalls. This chapter briefly introduced the role of ST as a way of describing cybersecurity as a threat and the role of cyber in the armed forces context. Cybersecurity as an emerging topic of interest in South Africa lacks understanding and the absence of analysis of the role of military personnel prevails in the cyberspace domain. Here the military and its officer corps are identified as critical role players. Much of the information for understanding the cyber landscape and its security implications is captured in the existing literature, which also assists with demarcating the military connection.

The next chapter focuses on the review of existing literature, which highlights cybersecurity as an emerging threat and how this digital threat is managed in the SANDF. Risk perception and information sharing are also reviewed in Chapter 2.

CHAPTER 2: REVIEW OF LITERATURE ON CYBERSECURITY AS AN EMERGING THREAT

2.1 Introduction

The previous chapter focused on providing a brief introduction of what this study entails by presenting its aims and objectives, as well as a brief account of the methodological approaches used in this research. This chapter serves as the literature review of this study. The central theme in this chapter highlights aspects that concern the development of an operational definition of cybersecurity, which derives from reviewing literature that focuses on the various elements of cybersecurity relevant to this study. The definition itself centres on a comprehensive view of cybersecurity, which is inclusive of behaviour, security practices, and technology. This study proceeded from the view that cybersecurity has three main aspects, namely technological, political, and security. The literature review focuses on key themes that are centred around several aspects: the human element as a focus point in the cybersecurity chain, the complex nature of cybersecurity threats and the impact of these threats on various pockets of society, the role of cyberspace in the armed forces context, and the efforts made by the state to reduce the number of cyberattacks. Furthermore, the literature review also covers risk perception and risk information. Moreover, a brief discussion of cybersecurity awareness creation and information-sharing behaviour is included in this review.

2.2 Chapter overview

This literature review is relevant to the context of the study in focusing on applicable international and South African literature on cybersecurity. The literature review firstly explores the definition of cybersecurity. Once presented, the focus moves to how the human element is located at the centre of the operational definition. Thereafter, the review of the literature discusses the complexity of cyberthreats. The chapter also includes a discussion of the impact of cyberthreats on society. Furthermore, the review pays attention to cyberspace and the challenges it presents for the sovereignty of a country and the armed forces. In addition, the volatility of cyberthreats regarding military personnel in the armed forces context is emphasised. The review then highlights the cybersecurity efforts made by the SANDF and the overall initiatives introduced by the South African government. Moreover, the review also points out the apparent void owing to the limited exposure of South African military officers to the available information and literature on cybersecurity. The digital landscape in South Africa is also discussed. Furthermore, the chapter deals with the perception of risk when navigating cyberspace. Information-sharing behaviour and the creation of cybersecurity awareness are also discussed as important risk indicators in the behaviour of military personnel.

2.3 Defining cybersecurity

Cybersecurity is often used as a general term to denote safety in cyberspace but the definitions are often inconsistent and uninformed owing to the multidimensionality of the concept (Ashraf, 2021; Schatz et al., 2017). The definitions listed in this section indicate how the thematic areas centred on cyber and the human element are linked together. The literature relating to this area contributed to the construction of the operational definition. The search for a definition that was inclusive of the complexity of cyber posed a challenge, especially since most definitions are objectively focused on technology, legislation, or online security. Furthermore, the continuing search for an acceptable definition related to cybersecurity has been a central preoccupation of scholars in the disciplines of international relations (IR), political science, and information and communications technology (ICT).

It was thus essential to conceptualise a definition of cybersecurity that is multidisciplinary (Ramluckan et al., 2020). Looking back to the past, Lewis (2006, p. 1) defines cybersecurity as “the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption”. Lewis’ (2006) definition shows that ICT has received more prominent focus in describing the technical process of safeguarding computer networks. In the last 15 years, this definition has undergone some change as the emphasis moved to a more integrated approach by also taking into consideration other disciplines included in the description of cybersecurity. For example, Mukiibi (2019) positions an argument relating to social context in the description of cybersecurity. In addition, a multidisciplinary approach that combines offensive and defensive measures is necessary to secure cyber assets for both state and non-state actors (Duvenage, 2019). From this perspective, while mention has been made of the extension of the definition, it still does not refer to the human role in cybersecurity. The operational definition that was formulated from information derived from the literature attempted to bridge the gap by integrating both technical and social domains, where the human factor interacts with both physical and digital spaces. From a security studies point of view, Cavelty and Wegner (2020) argue that cybersecurity should transcend the technical terrain and be more flexible in considering other disciplines. Bourbeau et al. (2015) originally mentioned in their book *Security: Dialogue across disciplines* that the construction of security can be described by drawing on disciplines such as psychology, sociology, and IR. How different academic fields view security is an important factor to highlight as descriptions of the concept of "cybersecurity" are influenced by technology, politics, and science (Cavelty & Wegner, 2020).

Dlamini and Modise (2012, p. 4) posit, from a political science approach, that cybersecurity can be defined as a "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that may be utilised for the protection of the cyber space and its users". This definition connects three main aspects, namely the technical (infrastructure), scientific, and political. It nevertheless limits the cybersecurity definition by not including the human factor or aspects related to the changing social environment. Furthermore, Dlamini and Modise's (2012) definition comes across as an attempt to explain the confined restrictions on best practices and guidelines in Africa. Much like other definitions, Dlamini and Modise (2012) refer to the tools necessary for engaging with cybersecurity but they fail to suggest that users have a key role in applying awareness and knowledge to maintain safety in a digital environment. In addition, Mashiane et al. (2019, p. 244) note that cybersecurity is defined as the "technologies, processes, controls and users that are set up to protect systems and systems data". While this definition points to the human element, it does not feature prominently. Instead, the central focus in the definition is the role of protection through the use of technological tools and measures, which emphasise the role of ICT in cybersecurity. Mashiane et al. (2019) nevertheless acknowledge, although not in their definition of cybersecurity, that the human component is an important factor in maintaining cybersecurity.

The definitions recorded up to this point do not fully emphasise the role of the human element in cybersecurity. Mashiane et al. (2019) concur with this notion by emphasising that a large part that is omitted from most definitions of cybersecurity is the "users". It is important to point out that existing definitions that make a societal connection still provide no clear indication of the functions attributed to the human. The focus should therefore shift to the "who" and the "what". More is thus required to introduce the human element to the definition of cybersecurity. For example, the "what" in this case refers to the activities that a user needs to perform to remain secure in cyberspace. Furthermore, the "who" refers to the cybersecurity practices of users and/or specific populations of users and their purpose for engaging in cyberspace.

The aforementioned cybersecurity definitions do not focus on the behavioural nature of humans in the cybersecurity chain. Instead, the definitions of cybersecurity are more closely linked to the technical nature of cyber and the processes followed to secure data in the digital domain (Ramluckan et al., 2020). Expanding on the definition of cybersecurity, what should be taken into consideration are the differences among users as these are able to influence the target audience, who should be included in a comprehensive cybersecurity definition. This is possibly why Van't Wout (2019) argues that training should be presented on the basis of organisational needs and its technology users. While Van't Wout (2019) did not make reference to the conceptualisation of a cybersecurity definition, the argument can be made that context is important, along with the notion that users are unique. A brief search on the human element and its importance to cybersecurity identified literature that considered the notion that cyberthreats and their associated attacks are either caused by human error or deliberate action by the human actor (Ani et al., 2019; Rauf, 2019). The human actor remains important for maintaining cybersecurity and its central role in security is noted in three ways:

1) The first aspect relates to why the human is of central importance, namely that socially engineered attacks may exploit cyber users through psychological manipulation. A cyberattack may therefore present itself in a dual format, by targeting the technical features of a system and attempting to exploit the users' psychological vulnerability (Ani et al., 2019).
2) Users can undermine cybersecurity technology intentionally or unintentionally, which poses a danger to the organisation and their own personal security.

Human behaviour in cyberspace and humans' awareness of digital security should thus be emphasised (Rauf, 2019).

3) The human actor should be cognisant of cyberthreats and potential ways that their online behaviour can be exploited (Ani et al., 2019). Rauf (2019) argues that home users are more likely to be at risk when navigating cyberspace as the quality of security measures is often lacking in comparison to those users who work in organisations and have access to more advanced technological and security solutions.

Barrett et al. (2020) suggest that in order to define cybersecurity, the focus should be purely on the domain of cyberspace. In addition, the National Institute of Standards and Technology (2011, p. 62) defines cybersecurity as "the ability to protect or defend the use of cyberspace from cyberattacks". It is not clear from the definition whether users are considered part of the definition as it mainly emphasises the protection of an invisible space. The argument can be made that users are excluded from this definition, where in fact they should form a definite part of cybersecurity. Pollini et al. (2021) argue that computer security and information security often focus on the technical side of cyber, yet the human factor's cognitive characteristics, motivations, and needs are granted limited priority. The sub-section that follows continues the discussion regarding the operational definition of cybersecurity and brings the human element to the fore.

2.3.1 The human element as the centre of the proposed operational definition

The previous section focused on cybersecurity definitions that can be viewed through various lenses. The definition proposed by the researcher in this dissertation takes note of the changing socio-technological landscape as more users are incorporating the Internet and technology into their daily activities. This proposed new approach acknowledges that there is interaction between technical infrastructure and human behaviour. Table 2.1 presents the rationale behind creating an operational definition that is suitable for taking into consideration the human element and explains why the previous definitions that were presented did not highlight the security awareness, along with training and education, that individuals need to maintain cybersecurity. It must nevertheless be emphasised that several sources indicate the human factor as the weakest link in the cybersecurity chain owing to their vulnerability to being exploited through their behaviour and their cognitive proficiencies (Ani et al., 2019; McMahon, 2020). In making this statement, the researcher acknowledges that the limitations attached to the human factor might have caused definitions of cybersecurity to be directed more towards the technical domain as this is an area that can be controlled.

Table 2.1: Cybersecurity definitions and factors not taken into consideration

Definitions	Factors not considered
Dlamini and Modise (2012, p. 3) define cybersecurity as the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that may be utilised for the protection of the cyber space and its users".	The human factor is mentioned, but it is not the central focus. Technology alone cannot be the sole foundation in maintaining cybersecurity. Instead, there should be a relationship between the technical factors (software and hardware) and the human actor. The aspects of concern are training and the application of best practices. The focus on the human factor should include elements relating to psychological vulnerability and aspects of online security behaviour. The focus of this section was to obtain a clear sense of how cybersecurity definitions consider facets relating to security (technical, guidelines, human factor).
According to Grabner-Kräuter (2018, p. 2), "[c]ybersecurity can refer to the state of being protected against the criminal or unauthorized use of electronic data or the measures taken to achieve this".	This definition departs from the premise that the protection of a nation rests in how critical infrastructure and assets are protected. The omission of the human domain and the balance of the socio-technical environment fails to offer a comprehensive view of maintaining cybersecurity and therefore does not provide a suitable definition that captures the role of the human element.
Mashiane et al. (2019, p. 244) define cybersecurity as "technologies, processes, controls and users that are set up to protect systems and systems data".	This definition agrees that technology is the only way that the user and system data can be protected.
Barrett et al. (2020, p. 20) define cybersecurity as "the ability to protect or defend the use of cyberspace from cyberattacks".	The factors not considered in this definition are the roles of security, training, the interaction between spaces, and the role of the human domain.
The South African NCPF (RSA, 2015b, p. 73) defines cybersecurity as "networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them".	This definition arguably is at the centre of South Africa's attempt to allocate responsibilities to key stakeholders but also emphasises the legal parameters within which cybersecurity can be managed. The definition does not consider the role of the human element at all. The focus is on threats such as intrusions.
Le and Hoang's definition (2016, p. 4) is: "Cybersecurity can be considered systems, tools,	This definition asserts that the crux of cybersecurity should contain elements of

Definitions	Factors not considered
processes, practices, concepts and strategies to prevent and protect the cyberspace from unauthorized interaction by agents with elements of the space to maintain and preserve the confidentiality, integrity, availability, and other properties of the space and its protected resources.”	practices and appropriate tools to safeguard agents and the space itself. The challenge with this definition is that mention is made of the interaction between practices, tools, and performative actions such as confidentiality and integrity. These are words that require some action, yet the human domain is not acknowledged at all. It may be assumed that the human element takes part in the cybersecurity process.

Based on the definitions presented above, it is clear that the human is rarely at the centre of the security process. Cyberthreats too often deliberately target the weaknesses of the human factor by focusing on their behaviour and cognition, which cause them to be vulnerable (Sithole, 2019; Van Schaik et al., 2017). This vulnerability results in security measures not being adhered to, voluntarily or involuntarily, and security operations being compromised (Ani et al., 2019). The researcher therefore noted that an operational definition should consider both technical and social interaction, which is an extension of the definitions captured in Table 2.1. Several scholars are urging the expansion of a cybersecurity definition to be holistic and contemporary (Bachmann & Gunneriusson, 2014; Craigen et al., 2014; Jacob et al., 2020; Ramluckan et al., 2020). Based on this view, Van't Wout (2019) proposes the notion that the exploration of online security behaviour is necessary as more human errors than system errors occur. This statement alludes to the idea that human behaviour and perceptions are of key relevance to understand cybersecurity.

Craigen et al. (2014) suggest that cybersecurity should be more inclusive of other domains and therefore present a comprehensive view of the concept. Craigen et al. (2014) add to this debate by suggesting that to draft a cybersecurity definition that is inclusive of all domains, it should be comprehensive and inclusive of a variety of security aspects, which requires a rigorous process. Cybersecurity is a hybrid form of security as it stretches across and throughout a variety of domains and sectors (Bachmann & Gunneriusson, 2014). This strengthens the argument for broadening the concept of cybersecurity, as the spread of this discipline eventually reaches the point where it ultimately has an impact on human users (Ani et al., 2019). Craigen et al. (2014) suggest that a more contemporary view of the cybersecurity domain is necessary, especially to approach challenges as being multidisciplinary. A more comprehensive approach is essential in exploring cybersecurity in the social context; one that also incorporates the views of other disciplines (Ramluckan et al., 2020). The same applies to a definition that is inclusive of technological changes and the social environment as the notion attached to cybersecurity may be interpreted differently because of the context in which it is studied and applied (Inria, 2019). Moreover, a definition that lends itself to a space that is complex in nature may also contribute to a lack of understanding what cybersecurity and the measures that cultivate security behaviour entail. A definition of cybersecurity must be multifaceted and flexible to be able to adapt to the social environment, as well as to capture the complexities of an evolving technological space (Ramluckan et al., 2020).

Cybersecurity definitions require a holistic view, which demands the acceptance of all domains as it ultimately stretches across various sectors (Jacob et al., 2020). One of the challenges associated with creating a holistic definition of cybersecurity rests in finding an acceptable, all-inclusive view of the concept “security” (Friedman & West, 2010). In the discipline of IR, for example, cyber has been discussed extensively through the lens of politics (Cavelty & Wegner, 2020; Bourbeau et al., 2015). The researcher therefore proposes that an operational definition should be flexible and cognisant of the social element, which is often omitted from conceptualising cybersecurity. The human element functions within the social sphere, with cybersecurity positioned in both the technical and social realms. The researcher argues that cybersecurity is better conceptualised when it includes the human element as the focus point of the security action. The researcher presents his newly crafted operational definition of cybersecurity as follows:

> Cybersecurity is a flexible security process through which individuals are constantly interacting with a technical environment in the social context. Cybersecurity is also the immersive process through which the human factor utilises security software tools in tandem with education, training, guidelines, technical knowledge, and best practices such as awareness training, technical skills, and risk assessment. Cybersecurity also requires the notion of applying knowledge to risk perception and precautionary behaviour, while being fully aware of vulnerabilities in both the physical and cyberspace domain.

The aforementioned operational definition developed by the researcher takes into account the human element and therefore, by implication, the military officer. The operational definition creates functions as an outcome of the literature review. As a result, it focuses on the element of technology and the role of the human, and it goes further by also capturing the aspects relating to context and safety in cybersecurity. This definition incorporates both technical and human interactions, which are absent from other established definitions. Moreover, the operational definition created for this study incorporates the notions of security, the human component, and the social environment. The researcher developed this definition as it helps to bridge the gap in the literature, which fails to acknowledge the human component, which in this case is the military officer. This definition was therefore created to also recognise the military officer (human factor) functioning in the armed forces context. The working definition thus bears relevance to the argument of this research, which is to explore cybersecurity compliance among military officers. Definitions of a variety of disciplines that deal with cybersecurity were considered, although the proposed new operational definition included in this dissertation supports a description that takes into consideration the changes in the social environment and the role of the user in cybersecurity. Owing to this, the next section focuses on the complexity that is associated with cyberthreats in certain contexts and shows that cyberthreats are intrusive and have the ability to cause security-related challenges.

2.4 The complexity of cyberthreats

Cyberspace has had a profound impact on society as it allows for instant communication and facilitates commerce in new ways (Bada & Nurse, 2019b). Along with the impact cyber has had on the interaction between individuals, it also sparked continuous growth in cyberspace. With the expansion of cyberspace, cyberthreats are becoming more diverse in the type and source of actors (Verizon, 2018). Modern society has created both a direct and an indirect dependence on IT, with a strong reliance on immediacy, access, and connections (Craigen et al., 2014). Mbanaso and Dandaura (2015) argue that people have become dependent on the physical and virtual components of cyber, which may have invited unpredicted vulnerabilities that result in data exposure. Fatokun et al. (2019) indicate that the age factor could play a role in the susceptibility of Internet users to cyberattacks. For example, Fatokun et al.

(2019) point out that older Internet users might be more vulnerable to cyberthreats. This perceived vulnerability could be an indication of the amount of time users are exposed to cyberspace at any given time and the lack of familiarity with cyberthreats. It is also argued that younger Internet users might be more familiar with cyberthreats and cyber vulnerabilities (Fatokun et al., 2019). Weiner et al. (2016) highlight that older personnel in organisational settings tend to display a tendency to adopt a sense of hyper-vigilance about their own limitations. This makes the transition between older roles and newer roles in reference to cybersecurity behaviour challenging (Khan et al., 2022). In addition, North and Fiske (2012) posit that older individuals who function in high-pressure organisations may find it difficult to transition into new roles.

Furthermore, cyberspace, and especially the Internet, have been expanding at a rapid rate. Consequently, this has contributed to commercialisation and advancement in the use of personal computers (Egloff, 2015; Geers, 2011). If the confidentiality, availability, and integrity of technological systems are compromised, this may have dramatic consequences, regardless of whether it is the temporary interruption of connectivity or a longer-term disruption caused by a cyberattack (Bada & Nurse, 2019a). Bowden (2019) uses the example of a complex cyberattack in the form of the “Conficker virus”, which had a severe impact on cyberspace users by globally attacking Microsoft operating systems in 2012. The Conficker virus is an example of a longer-term disruption as this specific malware often depends on systems being updated in order for the malicious code to become obsolete (Bowden, 2019).

The advancement of technologies allowed for nation states to facilitate the innovation of new services that enabled the strengthening of communication for modern economies (Kolini & Janczewski, 2015). Veerasamy (2021) argues that during the COVID-19 pandemic in 2020, there was greater dependency on ICT. Threats such as phishing[5], pretexting[6], baiting[7], and quid pro quo[8] are considered forms of social engineering attacks that target users’ emotional states by duping them into sending personal information to hackers (Veerasamy, 2021). Currently, social engineering

[5] Phishing attacks dupe users into disclosing personal information that is linked to their passwords and identification numbers.

[6] Pretexting is a scam where scenarios are fabricated so that users are duped into revealing personal information (Petit, 2022).

[7] Baiting refers to the process where users are lured by prizes or gifts if they provide their password or login details (Petit, 2022).

[8] Quid pro quo is a type of attack similar to baiting but is offered as urgent technical services that the user requires. Attackers often impersonate information technology (IT), hardware, or software representatives and pretend to provide technical assistance to users.

attacks are considered one of the biggest threats to cybersecurity as they can be detected but are very challenging to mitigate (Salahdine & Kaabouch, 2019). Moreover, when considering the response to cybersecurity incidents, the human factor has a key role in identifying security management tools for responding to threats. In addition, the human factor, regardless of the technology being used, must still be aware of the threats and vulnerabilities (technical and human) (Al-Dawod & Stefanska, 2021). Alotaibi et al. (2017) indicate that there are human factors that might influence online security behaviour. Alotaibi et al. (2017) also propose that the relevant factors include technological democracy (the requirement that users should be more free and flexible in using technological devices so as to be more efficient when performing their tasks); cultural factors (the security culture in organisations may influence how security behaviour is practised and how compliant personnel are with security policies); and personality and job satisfaction (an increase in job satisfaction levels has an impact on personnel compliance with information security policy).

Salahdine and Kaabouch (2019) suggest that social engineering attacks can be grouped into three categories. The first includes social-based attacks, where the attacker builds a human relationship with the victim by using a baiting technique. The second category involves technical-based techniques carried out on social media platforms, where users share their personal login and banking details (Salahdine & Kaabouch, 2019). The third category entails a physical attack, where the nefarious actor collects the user’s personal data by searching for documents, where the content is usually related to the personal information of the user/victim (Salahdine & Kaabouch, 2019). The first and second categories of attacks seek to exploit vulnerabilities in the human and target aspects of security awareness. Adding to this discussion, it is worth noting that antivirus software might be selected in accordance with users’ needs and security preferences (Patil & Joshi, 2014). However, the researcher argues that the use of antivirus software might not by itself be enough to mitigate threats such as malware and that the user should be guided by threat characteristics and points of entry, as emphasised by Souppaya and Scarfone (2013). Malware characteristics are changeable and their points of entry in systems vary in complexity according to the malicious code (Souppaya & Scarfone, 2013).

Cyberspace is the amalgamation of technology, virtual reality, networks, and telecommunications. These areas are brought together by the human element and form a space that is said to require attention similar to territorial domains (Mbanaso & Dandaura, 2015). In addition, cyberspace and its security challenges are nearly boundless as there are various examples of how cyberthreats influence a social landscape or damage critical infrastructure. Pieterse (2021) suggests that the WannaCry ransomware attacks that took place during 2017 are an example of malicious software that exploits the vulnerability of server message block protocols. This unique strain of malware leached into and destroyed the operating systems of approximately 200 000 network-enabled computers at the national health hospitals of 150 nations (Bowden, 2019). The implications of these cyberattacks, as witnessed during the 2017 attack, often have offline implications for society and security (Pieterse, 2021). According to Gandhi et al. (2011), members of the public are more likely to respond to the implications or effects of cyberthreats and attacks than actively responding to the potential presence of the attack.

Cyberspace provides a means that ideally permits problem-free communication across nation states, as well as a cost-effective business and political platform. However, it is also an environment in which individuals, businesses, and governments often engage in interactions that are saturated with conflict and where roles are not clear (Mbanaso & Dandaura, 2015). In addition, cyberspace is a complex environment in which individuals (including military officers and civilians) communicate and share information (Bigelow, 2019). There is a need for the armed forces to be involved in cyberspace as this space has been considered an important component in maintaining national security (Bigelow, 2019). Based on the information in this section, it appears that nation states are vulnerable to cyberthreats and, more specifically, there is a level of state immersion in and dependence on cyberspace. This immersion in cyberspace has caused national vulnerabilities to occur (Griffiths, 2017). The next section therefore focuses on the impact of cyberthreats on society.

2.5 The impact of cyberthreats on society

As technology and the complexity of the Internet continue to expand into societies, so too does the nature of cyberthreats and attacks (Stevens, 2020; Zheng & Lewis, 2015). With this expansion in mind, people are changing the way they choose to perform their daily activities, which may have far-reaching consequences in that they may have an impact on governments, businesses, banks, and everyday Internet users (Pieterse, 2021; Zheng & Lewis, 2015). Malicious software is relatively cheap and can be obtained by anyone who has a technological device and access to the appropriate platform to acquire such malicious tools (Whitney, 2021). These software tools can be used to exploit vulnerabilities in computer systems and data systems and are able to destabilise governmental information structures, disrupt banking systems, threaten national defence structures, and interfere with processes to secure users' information (Stevens, 2020; Zheng & Lewis, 2015). Disrupting the flow of data and the capabilities of systems ultimately has an impact on users' digital dependence and behaviour (Stevens, 2020).

The nature and purpose of a cyberthreat influence the narrative attached to the security measures that are used to secure breaches (Kreps & Schneider, 2019). The nature and wording of the term "cybersecurity" imply that there is a conscious attempt to protect a space that may be prone to violation or harm (Grobler et al., 2013). The way the threat and its possible associations are worded may also contribute to confusion among users because of the jargon and technical terms used (Al-Janabi & Al-Shourbaji, 2016). Moreover, the unsupervised nature of the Internet carries many dangers that may leave users in a vulnerable position when their personal data are shared with other sources (Rahman et al., 2020). A major obligation thus rests on users to be aware of the dangers of cyberthreats and the vulnerable position in which they are operating (Chandarman & Van Niekerk, 2017; Mousa, 2019). The researcher also argues that a reciprocal relationship must exist between the security awareness of users and the responsibility of institutions to advance cybersecurity training as routine training. This may assist institutions to have improved results when countering threats (Mashiane et al., 2019; Van't Wout, 2019).

There is a barrage of cyberthreats of which users, organisations, and governments should be cognisant (Hlase, 2018; Lejaka et al., 2019). With computer hardware and software capabilities becoming more affordable and developing at a faster pace, it may be challenging to create and sustain cybersecurity strategies. Creating and remaining updated relating to relevant cyber strategies can seem daunting because of the increase in more affordable computer hardware components and software (Taha & Dahabiyeh, 2020). Taha and Dahabiyeh (2020) suggest that the reliance on technology, such as Internet-enabled devices, may present some security vulnerabilities, especially since certain open-source applications require a constant

Internet connection. Concerns are thus raised regarding information security and the overall security behaviour that users reveal when navigating cyberspace.

Global technological advancement is making it increasingly difficult for nation states to control the safe use of hardware by the citizens within their borders (Grobler et al., 2013). Consequently, this technological development also does not allow for easy control of non-residents outside the borders who are in control of hardware inside another nation state (Grobler et al., 2013). The prevalence of these cyberthreats creates a situation where the national security of a nation state is threatened as these attacks are generally directed at achieving a specific purpose, namely crippling certain sectors of society and acting as catalysts in the distribution of state power (Tkachuk, 2018). However, the state and its institutions are not the only entities that are affected by cyberthreats. National security no longer only revolves around physical threats to the state and its organs of power. The widespread implications of cyberthreats can influence e-commerce (online transactions) and societal instability via social media platforms. Everyday users are affected by cyberattacks and cyberthreats that could destabilise a network supply chain at any point of entry (Reva, 2020; Du Toit et al., 2018). The type and nature of cyberthreats, as well as their target(s), depend on the motivation of the actor (Gazula, 2017) and have national, as well as lower-level, security implications. Collectively, the implications of cyberthreats and cyberattacks often pose challenges across multiple sectors, which can influence the social fabric of society (Irandoost, 2018).

Sutherland (2017) argues that the advancement of cybersecurity is dependent on the concomitant legislation and the speed at which it is implemented. Schneier (2019) confirms that there should be a balance between the pace at which technology evolves and cybersecurity legislation is enacted. Achieving this balance may allow users and their data to be less at risk of cyberthreats (Sutherland, 2017; Schneier, 2019).

Focusing on South Africa, it is apparent that since 2012 some advancement has been made in proposing measures and mechanisms used for the coordination of cybersecurity (Malatji et al., 2021; Sutherland, 2017). Vermeulen (cited in Patrick et al., 2016) argues that most attacks have some political implications; for example, the data breach in 2016, whereby thousands of South African government employees' sensitive contact details and names were posted online by an anonymous hacktivist group (Vermeulen, 2016). This apparent security void red-flags a vacuum in the legislation relating to the protection of personal information. It is important to note that legislation may not necessarily prevent cybercrime from occurring. It does, however, provide a sense of accountability if it is implemented and applied effectively. Furthermore, legislation may assist in the mitigation and prosecution of nefarious actors who commit cybercrime.

Malatji et al. (2021) explored the notion of critical infrastructure and its relationship with the current cybersecurity legislation in South Africa. These researchers note that in the case of South Africa, cybersecurity policies do not necessarily highlight the full extent of the protection that water- and wastewater-critical infrastructure requires. There is thus a need to run cybersecurity tests periodically and administer security audit trails (Malatji et al., 2021). Pollini et al. (2021) posit that it is the organisation’s responsibility to ensure that there are guiding policy documents to ensure that personnel maintain security. However, Pollini et al. (2021) also acknowledge that policies and procedures do not necessarily mean that the human factor will comply with the policies. Furthermore, considering the findings in context, society requires information to function optimally in all its sectors, and the same can be applied to the organisational setting, where operational activities depend heavily on pertinent information (Bester, 2003).

Nefarious actors have increasingly mentioned South Africa on the dark web since 2016 (Business Insider South Africa, 2020). This implies that the country is a target, and that its citizens, businesses, and organisations are at risk. Considering the abovementioned threat, one should focus on the context of cybersecurity in South Africa. Mashiane et al. (2019) posit that highly notable cyberattacks have been observed in South Africa, such as the Liberty Bank data breach that took place in 2018. This data breach resulted in the exposure of millions of users’ data. It is important to note the business element in the case of Liberty Bank as it shows that the state is not the only target of cyberattacks. Pieterse (2021) suggests that the most common cyber incidents in South Africa are where organisations fall victim to data exposure. Cyber activity in the South African context has seen a significant increase, both in a positive and negative sense, and its effects have been highlighted in both the economic and socio-political context (Hlase, 2018). The South African government is relying on ICT platforms to an increasing degree to extend its cybersecurity reach into the economic and socio-political sectors. However, the effects of cyberthreats may have some longer-term implications for the financial and industrial sector, specifically where critical infrastructure is involved (Malatji et al., 2021). The most recent example of a crippling cyberattack was observed in South Africa's state-owned port and rail operator, Transnet, which is a critical infrastructure entity (Toyana, 2021). It was reported that Transnet experienced an "IT disruption" but details regarding the hack were not revealed. It was, however, believed that the effects of this hack halted trade in and out of South Africa's ports for as long as a week (Toyana, 2021). It is worth noting that the Transnet cyberattack had an impact on the maritime industry as several ports were affected by the software malfunction that had occurred. This disruption caused economic challenges as imports and exports were inhibited for a brief period (Reva, 2021). The Transnet cyberattack also had national security implications as it ultimately had an impact on critical maritime infrastructure.

Cyberthreats such as malware, card-not-present or credit card fraud, and online banking fraud were some of the main security challenges experienced during 2019 (Accenture, 2020). Cyberthreats do not just pose a challenge for national security, but also for ordinary users. Ultimately it can be highlighted that, collectively, cyberattacks and threats are disruptive to South African society. Ani et al. (2019) argue that while critical infrastructure and security technology (software and hardware) might be in place, they only contribute minimally to the larger cybersecurity challenge. The security technology used in organisations is only as strong as the human factor (Ani et al., 2019). What this implies is that if an employee is unaware of certain features of cyberthreats, it may leave the organisation's information and systems vulnerable. In addition, despite the security technology in place, users may still be exposed if they are not adequately aware of or skilled in cybersecurity (Ani et al., 2019). The human factor might therefore place a person or organisation at risk of being both a target and victim if there is limited awareness.

According to Veerasamy et al. (2019), there are also other types of threats that organisations and ordinary users are facing in South Africa. These include threats such as malicious emails, ransomware, and theft of mobile devices and laptops. This is supported by Du Toit et al. (2018), who confirm that users typically receive spam, pornographic images, and phishing emails. The military and other state institutions are also not immune to these threats. South Africa experiences approximately 577 malware attacks per hour (Business Insider South Africa, 2020). In addition, ransomware is for sale on the dark web for R1 700, which may pose significant risks for users and national security as the purchase of malicious software is easily achieved. The next section focuses on the legislative cybersecurity efforts by the South African government.

2.6 Legislative cybersecurity efforts by the South African government

The previous section focused on the impact of cyberthreats on society. This section focuses on the cybersecurity efforts made by the South African government. South Africa has a legislative framework that assists with the advancement of governance related to cybersecurity in the country. The regulation and monitoring of cybercrime are a direct result of the increase in Internet-enabled mobile use among inhabitants (Mukiibi, 2019). For this reason, it is vital for the government to expand its development of a legislative framework that shows progression in securing its digital domain and its citizens (Malatji et al., 2021; Sutherland, 2017). In addition to this need, the South African government engaged in the development of a legislative framework consisting of (1) the NCPF (RSA, 2015b), (2) the Promotion of Access to Information Act (PAIA) 2 of 2000 (RSA, 2000), (3) the Protection of Personal Information (POPI) Act 4 of 2013, (RSA, 2013b), (4) the Cybercrimes Act 19 of 2020 (RSA, 2020a), and (5) the Electronic Communications and Transactions Act 25 of 2002 (RSA, 2002a). In the case of South Africa, the government responded to the increase in cyberthreats in 2015 by proposing legal frameworks within which citizens and government entities could operate (Sutherland, 2017). The NCPF (RSA, 2015b) is one of the first national legislative attempts to address the growing concern about cyberthreats (RSA, 2015b; Griffiths, 2017). The NCPF is a framework that does not facilitate in-depth understanding of the various roles and responsibilities of security stakeholders in South Africa (Van der Waag-Cowling, 2017; RSA, 2015b); however, it is a guiding document that facilitates understanding how cybersecurity is expected to be approached by the South African security cluster. Even so, this movement towards understanding cyberspace and its challenges may be considered rather elementary compared to the standards set internationally (Gcaza & Von Solms, 2017). The NCPF is a national policy that contributes to the legislative framework by acting as a guide for how the South African security cluster may interact with stakeholders and address the growing concern about cybersecurity (RSA, 2015b). Sutherland (2017) argues that South Africa has implemented the NCPF, but it is rather complex and modelled on European Union and US policies, with very few contextual aspects that are relevant to South Africa's national circumstances. Although South Africa, along with other nations on the African continent, have plunged headlong into the Fourth Industrial Revolution (4IR), which is geared toward creating new opportunities and connecting civil society to cyberspace, there is a tendency to not provide sufficient security in this domain (Dlamini & Mbambo, 2019; Jansen van Vuuren et al., 2013; Van Niekerk, 2017). Digital technological advancement demands a new way of thinking about cyberspace (Gálik & Tolnaiová, 2019; Mbanaso & Dandaura, 2015).

Cyber space and technology are extending their reach in the daily activities of people (Martin, 2020). Legislation is therefore required to focus on the entities that may manage and distribute personal information (Kandeh et al., 2018). In terms of legal frameworks that link with the South African Constitution, it can argued be that there is South African legislation such as the PAIA 2 of 2000 (RSA, 2000). Section 32(1)(b) of the South African Constitution (RSA, 1996) indicates that everyone has a right to access information. National legislation should therefore be implemented to facilitate exercising this right. The PAIA gives effect to this right, as determined by section 32(2) of the Constitution. In addition, the PAIA (RSA, 2000) and the POPI Act (RSA, 2013b) are different Acts, although they both contribute to the enactment of the constitutional right of access to information (see section 32 of the South African Constitution of 1996). The POPI Act (RSA, 2013b) and the PAIA (RSA, 2000) aim to protect personal information, but they do not have the same purpose. The PAIA (RSA, 2000) highlights the means of accessing information, whereas the POPI Act (RSA, 2013b) refers to the means of protection of personal information. The POPI Act (RSA, 2013b) provides that private and public (government) entities must secure personal information.

Entities that collect and store information are responsible for adhering to the POPI Act (Kandeh et al., 2018). Furthermore, it is acknowledged that there are challenges in implementing the structure required for entities to comply fully with the regulations stated in the POPI Act (Kandeh et al., 2018). For this reason, the POPI Act had to be introduced in order to bring about the regulation of personal information and the possible measures that private and public bodies may utilise to implement security measures. These private and public (government) bodies that are engaging in the circulation, collection, and storage of personal information must adhere to the legislation (RSA, 2013b). The challenge in the implementation of the POPI Act (RSA, 2013b) is in the constant development of technology as the boundaries of the way that information is transmitted, processed, and stored keep changing (Kandeh et al., 2018). In addition, legislation that deals with the regulation and storage of personal data is but a single facet in a state's attempt to ensure national cybersecurity.

The expansion of the legislative framework is clear in the development of the Cybercrimes Act 19 of 2020 (RSA, 2020a), which governs practising security behaviour. The Cybercrimes Act (RSA, 2020a) was first proposed in 2015, when it was named the Cybercrimes and Cybersecurity Bill (Bill 6 of 2017) (RSA, 2016). The aforementioned Bill was introduced for public comment in 2015 (Griffiths, 2017) and was later enacted as the Cybercrimes Act 19 of 2020 (RSA, 2020a). This Act was only passed five years after its first introduction, in 2020, and signed into law by the president of South Africa, which demonstrates the need for greater urgency in passing national legislation.

Van der Waag-Cowling (2017) confirms in her 2017 study that South Africa requires a sense of urgency to pass national legislation attached to cybersecurity strategy. The former South African Minister of Defence indicated that strict budgetary constraints were delaying progress in this regard, as reported in the DoD's annual report (RSA, 2020b). However, the minister's view was contextual and did not provide an indication that national legislation relating to cyber strategy was delayed. According to Van der Waag-Cowling (2019) and Sutherland (2017), the South African government requires some sense of urgency to speed up the drafting of cybersecurity legislation. The fact that South Africa has launched its first ever Cybercrimes Act (RSA, 2020a), however, gives the idea that there is emphasis on establishing a dialogue concerning a potential shift in the response to threats by the designated security cluster and is making an effort to achieve some clarity about clearly defined roles and responsibilities in this area (RSA, 2020b; Van Niekerk & Maharaj, 2013). Nevertheless, the growing trend of cyberattacks in South Africa continues to threaten the maintenance of cybersecurity (Gcaza & Von Solms, 2017; Dinesen & Sæther, 2013).

Advancing the discussion to South Africa's global rank position (59th) concerning cybersecurity efforts, the researcher emphasises the International

Telecommunications Union (ITU, 2021). The Global Cybersecurity Index (GCI)[9] (ITU, 2021) showed that while South Africa is on a developing path with regard to cybersecurity measures, it did, however, find some areas that required attention. Two points of concern were noted; the first being that technical measures needed to be enhanced and secondly that the development of organisational measures relating to cybersecurity needed to be highlighted (ITU, 2021). However, a positive that emerged from the index was that the legal measures regarding cybersecurity were identified as a positive aspect (ITU, 2021). Although South Africa is one of the leaders on the African continent in advancing the cybersecurity agenda, it is still challenged by the delay in providing a national cyber strategy and a cyber warfare strategy (Sutherland, 2017; Van der Waag-Cowling, 2017). According to Sutherland (2017), the GCI does not measure cybersecurity programmes and practical efforts; instead, the GCI focuses on approving national legislative measures and policies. Sutherland (2017, p. 86) suggests that the GCI is problematic as it measures "legislative measures and policies on paper". According to the ITU (2021), the GCI has five measuring factors, which are: (1) legal measures undertaken by the country, (2) technical measures, (3) organisational development, (4) capacity enhancement of cybersecurity, and (5) the employment of cooperative measures. This notion of providing training and education is shared by Van't Wout (2019), who suggests that a blanket approach may not necessarily help to establish awareness; instead, training should be geared towards the needs of people and organisations.

In terms of the operational definition presented in Section 2.3.1, it is evident that training and education are central to describing cybersecurity and placing the human element at the centre. While the operational definition does not indicate the legislative package on cybersecurity, it does acknowledge the role of best practices and guidelines that may ultimately act as the foundation to inform future legislative measures. The political will of the South African government has also come under scrutiny given its slow pace in passing legislation and the significant amount of time the public comment process requires (Sutherland, 2017). In addition, the delayed pace at which legislation is passed does not make allowances for the ever-evolving types and nature of cyberthreats (Du Toit et al., 2018; Sutherland, 2017; Jansen van Vuuren

[9] The GCI is used to track and assess the legislative efforts of countries across the globe in order to highlight key improvements and noticeable challenges (ITU, 2021).

et al., 2013). It should therefore be emphasised that lawmakers who are engaged in implementing strategies to safeguard users against cyberattacks must remain agile and updated with threat information as cyberspace and the tools that are connecting users to it change quickly and continually (Sutherland, 2017). The South African government has been criticised for its failure to implement cybersecurity measures (Sutherland, 2017; Van Niekerk, 2017). On paper, South Africa is doing relatively well as it has signed treaties and approved legislation relating to cyber (Malatji et al., 2021). However, actual implementation and resource allocations do not necessarily serve as a reflection of the political will required for actualising cybersecurity measures (Ramluckan et al., 2020; Sutherland, 2017).

Meanwhile, the demand for more awareness regarding cybersecurity is receiving increased public and government attention in South Africa (Veerasamy, 2021). This increased attention is reflected in the initiatives of the CSIR and the Department of Telecommunications and Postal Services in an effort to highlight the importance of digital security. The aforementioned government-affiliated organisation and government department are lobbying for stricter policies and laws, which ultimately concern governing human behaviour in cyberspace and developing effective cybersecurity capacity (Jansen van Vuuren et al., 2014). This increase in public attention and campaigns for cybersecurity awareness have a variety of reasons, but most notably arise from the increase in cybercrime (Du Toit et al., 2018; Sutherland, 2017; Van Niekerk, 2017).

In summary, this section showed that South Africa has made some progress in introducing legislation and initiatives to address cybersecurity threats. However, the implementation of cybersecurity measures remains a challenge as the government seems to lack the political will to implement them in practice and has failed to allocate appropriate resources to mitigating prospective cyberattacks and threats. This heightens the risk factor and mitigation measures that South Africa, and eventually the SANDF, will have to contend with. The next section focuses on the challenges that cyberspace poses for the element of sovereignty.

2.7 Cyberspace and challenges to sovereignty

The concept of sovereignty, much like cybersecurity, is interpreted very differently across disciplines and contexts (Colomer, 2020). What should be taken into account is that the armed forces are but one of the facets responsible for maintaining national sovereignty. An additional facet is legislation (Colomer, 2020; Cornish, 2018; Tsagourias & Buchan, 2018). Collectively, these facets tend to respond to and underline territory, borders, and space as physical manifestations of sovereignty for jurisdictional purposes. This context makes it important to explore how cyberthreats threaten the cyber sovereignty[10] of a nation.

Sovereignty refers to the authority and control a nation displays in disseminating legislation and enforcing power over its territory and its people (Tsagourias & Buchan, 2018). The definition of sovereignty mentioned above denotes how territory is an important component over which to exercise power and establish control. There are various arguments related to how cyberspace poses challenges to sovereignty (Hong & Goodnight, 2020; Pieterse, 2021; Shen, 2016). For example, Hong and Goodnight (2020) suggest that cyberspace limits how power is displayed domestically, yet this does not challenge the existing authority or legal integrity of a nation. Hong and Goodnight (2020) further suggest that cyberspace and ICT capabilities have become an important component in the race for power and control over territory and society.

Cyberspace cannot exist without the presence of the physical domain (Pieterse, 2021; Shen, 2016). What this implies is that there is a physical stratum to cyberspace that consists of network and computer infrastructure (MacNamara, 2019). Furthermore, network communication is dependent on the physical infrastructure in order to function (MacNamara, 2019). The second layer is found within network communication, which consists of digital activities by users. However, the argument can be made that this layer does not have the same level of dependence as depicted by physical infrastructure.

Kohl (2018) argues that sovereignty is a “sponge” concept, which highlights its ability to manifest in various forms; hence it can be interpreted differently depending on the context. The sovereignty of nation states is challenged by cyberthreats and attacks that target cyber-related vulnerabilities. A nation state may exercise authority by enforcing legislation that is able to protect its nationals and non-nationals from potential cybercrime, threats, and attacks (Tsagourias & Buchan, 2018). Furthermore, the

[10] Leiter (2020, p. 12) posits: “The term cyber sovereignty stems from internet governance and usually means the ability to create and implement rules in cyberspace through state governance.”

information that is disseminated through cyberspace may also be regulated through the way it is shared and the way it is received (Tsagourias & Buchan, 2018).

Owing to the transnational nature of cyberthreats, the power exercised by the state may not be completely effective if there are multiple victims of different nationalities who have been impacted (Tsagourias & Buchan, 2018). In addition, the traditional idea of exercising power over territory is also connected with the notion of power diffusion in cyberspace. This implies that there are stakeholders other than the state who are involved in the monitoring and control of cyberspace. For example, role players in civil society and the private sector all have an important role in securing cyberspace and using security measures to maintain the notion that the Internet is a space in which to exercise individual freedom (MacNamara, 2019).

As cyberspace assumes greater prominence as a domain of power, the struggle ultimately manifests when nation states put greater emphasis on physical power (MacNamara, 2019). Mansell (2016) argues that nation states often rely on the physical stratum, which is infrastructure (Mansell, 2016). However, resource allocation and authority are not sufficient to allow the state to exercise power as cyberspace was not designed as a domain in which the power of control is displayed through state dominance. Instead, what was created to be a space of autonomy and freedom has now shifted completely, in the direction of a place where security and digital sovereignty are considered more significant (MacNamara, 2019; Mansell, 2016). This diversity apparently indicates that the armed forces are one of many components with a role in maintaining sovereignty, along with the governing measures implemented to manage threats in the digital space (Cornish, 2018; Tsagourias & Buchan, 2018). Moreover, the nefarious actors who are constructing and strategically launching cyberattacks may challenge how a nation deals with threats (Pieterse, 2021; Shen, 2016). Cyberthreats and attacks that are executed pose potential dangers to a nation state’s national security, as well as the personal data of its nationals and organisations, along with, for example, a country’s economic competitiveness (Fouad, 2019).

It is also important to consider the role of technological advancement, dependence, and cybersecurity resource allocation for the purpose of maintaining sovereignty. The focus on the development of ICTs in the military shows that technology has become entrenched in operational activities in many armed forces contexts (Sayler, 2020). Cyberspace and technological advancements (hardware and software) go hand in hand and cannot function without each other. Furthermore, the borderless nature of cyberspace poses a threat to border-driven nation states that could potentially fall victim to cyberattacks, which render traditional military measures less effective. In addition, the argument can be made that the potential security threat that cyberattacks present may be escalated in terms of a nation's resources and technological capabilities. This situation often plays out in how a nation responds to threats and the resource allocation that enables the use of cybersecurity technology.

Furthermore, nation states might be dependent on innovative technology that is produced by their counterparts or at least have links to this technology. Such dependence might place the integrity attached to maintaining the cybersecurity of a nation at risk due to the hardware and software not being manufactured on their own terms. Cyberspace thus does not merely constitute a digital threat but can have consequences in the physical domain, where critical infrastructure could fall prey to damage. The narrative concerning cybersecurity in the armed forces context is replete with terms such as cyberterrorism, cyber warfare, and cyberespionage, as well as the cyber arms race, all of which not only present potential military threats but also require a measured military response as part of the response array (Gazula, 2017). The next section focuses on how the armed forces utilise cyberspace and how they could also present a security challenge.

2.8 Cyberspace and the armed forces

Cyberspace is an unseen domain, without any physical boundaries. However, the effects of its use through daily activities and operations can be felt depending on the context in which it is used. For example, a cyberattack that has been launched by Nation State A may have political or socio-economic consequences for Nation State B[11]. Territory in the traditional sense is therefore not considered (Douzet, 2014). An unseen "world war" has been fought for decades with no clear indication of battle boundaries and no foreseeable end in sight. Due to the invisible and hybrid nature of cyberspace, it is ideal for covert attacks (Jupillat, 2015). Aghatise (2006) suggests that the cyber attacker engages in a mental exploitation exercise whereby the vulnerability of the cyber victim is analysed for potential security tools and behaviour that may allow

[11] An example where geopolitics is questioned is the alleged involvement of the Russian government in the political elections that took place in the United States of America (USA) during 2015 (Bing et al., 2021).

for the victim to be left vulnerable in cyberspace. Bada and Nurse (2019a) argue that cyber creates a psychological distance between the user intending to use cyberspace in a non-threatening manner and the nefarious actor who is engaging in cyberthreats.

Furthermore, Bada and Nurse (2019a) emphasise that non-lethal cyberattacks can evoke fear in individuals, which may prompt them to demand stronger regulations and activities, such as surveillance programmes and stricter regulations by the government. Linking this to the armed forces context, it can be argued that the armed forces could potentially play a role in the protection of cyberspace and govern some of the practical aspects relating to enforcing cybersecurity legislation. This view is shared by Welch (2011), who indicates that operations have been carried out by armed forces in cyberspace for some time and claims that six main activities are at play. These six activities are the following: (1) constructing cyberspace by engaging in passive defence activities such as monitoring, (2) launching active defence mechanisms by interaction, (3) operational preparation of the environment, (4) launching cyberattacks, (5) clearing up support capabilities, and (6) identifying challenges associated with operational activities. Shea (2018) and Welch (2011) note that cyber operations that are performed by nation states are nothing new; however, the understanding of cyberspace and security-related aspects require some attention and maturation.

Bardwell et al. (2017) suggest that cyber training is important for the armed forces context, especially since cyber is a fast-emerging domain that threatens aspects such as national security and decision-making systems that are deemed fundamental for the state to exercise power. Gallarotti (2011) argues that a nation state may pursue various “power” strategies in order to achieve its political goals. In addition, the power of the state is often determined by the tangible nature of material assets and capabilities (Nye, 2021). The military forms part of these tangible material capabilities and is used to augment the soft power that may come in the form of legislation and decision making, as well as leadership abilities. Furthermore, the soft-power features are also linked with intangibility, which implies that these capabilities cannot be exercised in the same way as military force.

Cyber capacity and infrastructure expose countries to unseen battles in cyberspace aimed at gaining dominance in cyberspace (Weimann, 2005). Some nations such as the USA, Russia, and China have treated cyberspace as a domain of warfare in both practice and the theoretical sense since the late 1990s (Cavelty &

Wegner, 2020). Georgieva (2020) considers the growth of cyber capabilities by nations and state actors as part of the cyber arms race. The practical display of these cyber powers as being in competition often comes through espionage and intelligence, but also as cyberattacks on adversaries (Georgieva, 2020).

According to Buchanan (2016), cyberspace presents major uncertainty over adversarial capabilities and efforts to safeguard national security and sovereignty. This dynamic is linked with the duality of offensive and defensive measures deployed by the state in order to strengthen and maintain national security in cyberspace (Buchanan, 2016). In addition to the argument that cyberspace encompasses all land, air, sea, and space operations, it is important for the armed forces to exploit the digital domain's potential as they can facilitate protection against emerging cyberthreats (Smith & Palazzo, 2016). Freedom of action is therefore demanded across all traditional domains of warfare such as land, air, sea, and space, which now include cyberspace (Smeets, 2018). Furthermore, the protection of physical and information systems and activities depends on two components: (1) ensuring that freedom of action is maintained by devolving command to other facets in the organisation, and (2) ensuring the protection and maintenance of the armed forces through applying security measures to its members, installations, and resources (Karaman et al., 2016; Kärkkäinen, 2015). Cyber operations thus form a critical part of a nation state's attempt to achieve a tactical, strategic, and operational advantage (Brantly & Smeets, 2020). The researcher also argues that with cyber operations being central to national security, the success of its operations relies on denying its adversaries tactical and strategic freedom.

As nations become increasingly dependent on cyberspace, so too does the need for a military force to have a role in protecting national interests in cyberspace (Nielsen, 2016). This goes back to the human element and eventually the importance of officers as an important cohort in the armed forces, not being weak slots, and thus being a vulnerable layer for cyberthreats to focus on. As the threat migrates towards endangering national interests, the role of the armed forces in cyberspace is an important matter in maintaining national security (Brantly & Smeets, 2020).

When referring to context, how threats target victims may elicit different responses. This argument takes shape in two ways: (1) the responsibilities allocated to the key stakeholders may differ; responses may therefore be dissimilar, and (2) the threats in the armed forces context differ from what is experienced in the civilian sphere. Based on the first point, the argument can be made that one cannot merely transplant cyberthreats that occur in the civilian sphere onto the armed forces as the level of security responses and measures may differ. This can be observed in the profiling of threats and suitable responses, as recommended by Ngcobo (2020). Some of the threats profiled by the SANDF are organised crime groups and state-sponsored cyberattacks (Van der Waag-Cowling, 2017). There are several steps in responding to cyberthreats and attacks: (1) reporting and registration, where an incident number is allocated, (2) verifying the nature of the threat and the classification of the incident, (3) prioritising the incident by referring the case to the required cybersecurity expert, (4) informing the responsible person about what steps to take regarding the reported cyber incident, (5) seeking resolution, and (6) closing the case, all the while learning from the process (Ngcobo, 2020; Parliamentary Monitoring Group [PMG], 2020).

Malatji et al. (2021) showed in their study how cybersecurity roles and responsibilities are allocated according to the functions of entities in security clusters. In addressing the second point above, attention should be paid to the notion that nation states have militarised all forms of cyberattacks by applying the terms “cyber adversary”, “cyber espionage”, and “cyberterrorists”. This brings about the argument that threats in cyberspace are being militarised through the terminology used (Gomez, 2017). Some rhetoric has thus taken on meanings that could be associated with war and the protection of sovereignty, especially since nation states have adopted stronger cybersecurity laws (Ashraf, 2021; Galinec et al., 2017; Schneier, 2013). Military terminology has also migrated into cyber contexts (Nielsen, 2016). An example of this is seen in the term “advanced persistent threat” (APT), which denotes a “sophisticated and specific target attack with the aim of either data theft, disrupting the targeted system, or both” (Jabar & Singh, 2022, p. 1).

When referring to an APT in the armed forces context, it is important to point out the offensive and defensive positions nation states need to assume to ensure comprehensive security in cyberspace. Some of the mandates linked to cybersecurity are more defensive than others, as can be observed in the general cybersecurity legislation (Schneier, 2018; Galinec et al., 2017; Sutherland, 2017). Cyberspace has transitioned into a theatre where nations are vying for dominance and displaying their power, all in the digital space. As technology advances, there appears to be increasing emphasis on using the military as a key factor in cyberspace (Bardwell et al., 2017). The importance a nation places on cybersecurity can be determined by observing the following: connectivity, spending on the defence budget, financial services, ICT and the industrial sector, and legislation (ITU, 2021). Solar (2020) highlights that the USA emphasised its new Command Vision for US Cyber Command, which confirms that a cyberattack should be mitigated before defence systems are placed in a vulnerable position, which may result in the impairment of strategic and tactical operations. A need thus exists to develop a conceptual and doctrinal way of thought concerning military cyber operations and the methods used to deter cyberthreats (Brantly & Smeets, 2020). Viewing the military as a critical tool in cyber defence necessitates highlighting the need to secure sensitive information and to safeguard important assets (Smeets, 2018; Nielsen, 2016). The traditional military function that enters cyberspace may therefore permit the increased assertion to engage in operational activities that are designed to mitigate cyberattacks (Smeets, 2018; Nielsen, 2016).

The armed forces context remains a critical feature in the composition of a nation state’s cyber defence capability. As ICT capabilities are increasingly incorporated into the armed forces context and civil society, secure information is demanded and the armed forces exercise a “peace and safety” role through its infrastructure and human resource component to support cybersecurity. The researcher argues that cybersecurity must act as a bastion in two ways: (1) by ensuring that the power and security of the state is protected, and (2) the extent to which the military is the leading agency in effecting cybersecurity. The next section focuses on the volatility of cyberthreats and placing the armed forces and its human component in a position of increased vulnerability.

2.9 Cyberthreat vulnerability of military organisations and their personnel

Technology and ICT have had a profound effect on every aspect of society in the last decade (Bossler & Berenblum, 2019). This includes military organisations, which have become much more reliant on cyberspace operations (Bardwell et al., 2017). Military personnel remain part of society and therefore part of the cyber connectivity argument. This argument can be linked to the idea that cyberspace has become so entrenched in the daily lives of people that it influences practically all aspects of it (Leenen et al., 2018; Van Niekerk, 2017). In addition, the military as an organisation and its subdivisions use cyberspace and require of its members to be knowledgeable about cybersecurity issues (Leenen & Jansen van Vuuren, 2019). However, the traditional military culture of maintaining security is largely based on the physical stratum (Leenen et al., 2018). This means that security is largely thought of as the outcome of physical force being used to maintain a certain level of peace. Tactics and techniques used in traditional military thinking may not necessarily thrive in a cyberspace environment as this domain is extremely flexible and requires military members to maintain a faster pace in decision making and using their training in maintaining cybersecurity (Leenen et al., 2018). Bardwell et al. (2017) argue that the armed forces are an important target for adversaries in cyberspace. Although cybersecurity is a focal point for private organisations and civilians, cyber warfare is a topic that requires equal attention in the armed forces context as all military organisations do not necessarily promote or possess sufficient awareness training on emerging cyberthreats (Bardwell et al., 2016). Armed forces may become vulnerable when they do not attend to security in both the physical and cyber domains as these two domains intersect. Smith and Palazzo (2016) argue that cyberspace should be given the same consideration as physical space. Exploitation of the cyberspace domain is not limited to mere virtual aspects, as critical physical infrastructure is equally vulnerable.

Cyberthreats are multifaceted and may target anyone, including military officers (Bardwell et al., 2017; Martin, 2020). Ani et al. (2019) suggest that there should be a balance between the human factor and security technologies so that intrusions may be detected more efficiently in organisations. As their world becomes more digitised, the next generation of military officers are anticipated to be more connected to cyber than ever; therefore flagging their importance as potential targets for cyberattacks (Sigholm, 2016). Van Schaik et al. (2017) argue that human factor interaction with computer-based systems allows for increased security behaviour and precautionary decision making. The focus of this study is not the military officer exclusively, but also the strength of the connection between the human (South African military officer) and technological device as both sets of vulnerabilities can cause damage. In terms of the wider view of the literature concerning the military member and cybersecurity threats, the common factors of exploration rest on network security and training in the armed forces (Bardwell et al., 2017; Ďulík & Ďulík, 2019; Kärkkäinen, 2015). From a wide literature perspective, the focus is not necessarily on the rank feature of the military member, but more on members in general. The wider military focus therefore implicitly points out the void as being the military officer, which this study addresses.

Cyberattacks are borderless and not confined to a singular device. Instead, a cyberattack can be viewed as an interconnecting event or series of events that have an impact on a variety of actors. For example, Li and Liu (2021) assert that the consequences of cyberattacks can cause significant damage to the tactical functioning of armed forces, whereby critical data, electronic systems, and information network systems are compromised or altered. Based on this finding, it is evident that cyberattacks might also damage physical equipment and infrastructure, as well as the important human cohort in the armed forces. The rise of cyberspace demands a reframed view of security as the traditional approaches to eradicating threats have become irrelevant in some instances (Mendoza, 2017).

The Bring Your Own Device (BYOD)[12] phenomenon in organisations is becoming a trend among employees (Adedolapo, 2016). Adedolapo (2016) suggests that the use of mobile technology and software tools can enhance productivity and autonomy. According to Benson and McCarthy (2016), technology is becoming more readily available and the military population is not immune to the use of new technologies. The use of personal devices may also assist members of the military with completing their tasks and annual training requirements faster (Benson & McCarthy, 2016). However, these advances may pose unintended security threats for users and organisations. Benson and McCarthy (2016) indicate that by permitting military members to use their personally owned devices and allowing access to privileged or secured networks, the likelihood of information leaks and data breaches become more apparent. In the SANDF, a policy exists on the use of personal devices in the organisation. However, the use of personal devices is strongly discouraged if they are used for private matters or DoD purposes (RSA, 2011a). The security applicable to storing organisational information on personal devices is governed by DoD policy DODI/CMI/00008/2001 (RSA, 2011a). Personal devices, in this regard, are always subject to auditing (RSA, 2011a). Gupta et al. (2019) argue that employees in larger organisations typically use their personal technological devices, such as laptops or mobile devices, as they are more familiar with them and because there is a

[12] "BYOD" is a concept that denotes the practice of utilising personally owned electronic devices such as tablets, smartphones, and laptops for work-related purposes.

significant need for innovation. Nævestad et al. (2018) argue that the support provided by the top management of organisations is often an indicator of the level of compliance with policies by personnel.

Hadlington (2017) refers to the context of cybersecurity awareness in larger organisations when pointing out that resource allocation and financial investment in personnel is a strong predictor of a higher level of awareness. While the private sector in South Africa is able to adopt and advance the BYOD phenomenon (Veljkovic & Budree, 2019; Adedolapo, 2016), the armed forces context cannot afford security breaches, especially as some DoD information is critical to operational activities. Yeboah-Boateng and Boaten (2016) suggest that employees of organisations are not only in favour of using their own devices as this enables them to function without restrictions imposed by network administrators in the organisation but also because they are free from organisational oversight as monitoring of organisational technology usually takes place. However, sensitive information associated with the organisation that is stored on personal devices might be exposed to various threats such as malware and permission that users grant to applications to access their information (Yeboah-Boateng & Boaten, 2016). However, this vulnerability goes both ways as organisational devices might also be susceptible to potential threats. DoD Instruction DODI/CMI/00008/2001 (RSA, 2011a) makes reference to the auditing of personal and organisational devices in order to safeguard against threats and attacks.

Owing to the need to adapt to more alternative communication tools, military personnel might be motivated to use personal devices that are more efficient at accessing personal and organisational data (Rivadeneira Zambrano & Rodríguez Rafael, 2018). However, this is a security risk if the devices that belong to employees are not audited or checked for potential vulnerabilities (Rivadeneira Zambrano & Rodríguez Rafael, 2018). This is therefore a good reason to ensure that military personnel are up to date with threats and vulnerabilities. Organisations facing budgetary constraints are likely to experience challenges in the acquisition of new technological tools for their personnel to use (Boyabatli et al., 2015). Martin (2020) suggests that one of the reasons why military personnel are not satisfied with the inefficiency of formal channels of communication in the organisation is because of the slow pace at which information travels. Unofficial platforms of communication are thus preferred, such as social networking sites to share privileged information (Martin, 2020). However, using social media can have both positive and negative consequences. A possible positive aspect attached to allowing personnel to use social media platforms is that they are able to communicate more efficiently (Jain et al., 2021). In this instance, it is essential to emphasise that the availability of user information on social media platforms might entice adversaries to exploit user data that could be traced back to the organisation (Jain et al., 2021). It is worth noting how this features in the war in Ukraine. Myre (2022) indicates that Ukraine's military intelligence intercepts and targets communication through the use of social media and mobile devices. This interception of communication takes place when official methods of communication break down (Myre, 2022). This enables interception and targeting of data by opposing forces. Moreover, when personnel are uninformed about cyberthreats, it may place the information security of the organisation and their personal information at risk (Murire et al., 2021). The argument can thus be made that awareness training in cybersecurity or information security should be extended to all members of an organisation (Murire et al., 2021). This could be done to increase awareness and training capacity with a view to increasing the human component of cyber as no security tool by itself might be capable of sufficiently protecting a user (Murire et al., 2021). A relationship exists between cyber and technology, and each of these factors requires the other to grow. While technology can be an effective resource for employees in organisations, it is used by humans who come from diverse backgrounds, cultures, experiences, and levels of education. It is therefore of key importance to study how military officers use technology and the procedures they apply when engaging with informatics (Sigholm, 2016).

Keeping the military officer in mind, Ani et al. (2019) and Bardwell et al. (2017) argue that the potential internal and external vulnerabilities in the organisation should be highlighted. Bardwell et al. (2017) emphasise the need for military personnel to be educated in cybersecurity awareness, while at the same time highlighting that the human element in the military should be skilled. Ani et al. (2019) support this notion by pointing out that the human factor should be educated in the vulnerabilities and measures to secure themselves, which deal with bridging the application of knowledge and executing security behaviour. Schwarz (2016) argues that it is not necessary for the personnel of a military organisation to be mobilised concerning offensive and defensive measures, but that specialised personnel should instead be trained to deal with advanced attacks or threats. It is worth noting that the armed forces engage in warfare for a limited period, but the aspect of cybersecurity is a matter that needs to be constantly addressed and maintained. Ani et al. (2019) argue that routine training and awareness education in cybersecurity systems and threats are necessary to build a robust organisation that can cope comprehensively with threats. It is important to note that not all military personnel are directly involved with cybersecurity. However, this does not mean that general training in cybersecurity should not highlight the aspect of human behaviour in cyberspace and potentially facilitate personnel capability of mitigating current and prospective threats (Van't Wout, 2019; Bardwell et al., 2017; Aschmann et al., 2015). In addition, Bardwell et al. (2017) suggest that cybersecurity awareness is central to educating all members of the military about cyberthreats. Mobilisation in this case thus refers to an active pursuit of attaining a level of cybersecurity awareness and equipping all members with basic knowledge to secure data that are critical to the organisation and to maintaining national cybersecurity (Van't Wout, 2019; Leenen et al., 2018). With security behaviour in mind, Bulgurcu et al. (2010) argue that information security awareness is a significant predictor of users practising security behaviour and attitudes. Siart et al. (2016) argue that social status in hierarchical environments might encourage the diffusion of power and alter the perception of other personnel or members of the military with a lower social status. In the military context, this possibly refers to rank.

The development of malicious code and attack vectors that are able to exploit organisational hardware and compromise network security systems is currently taking place (Leenen et al., 2018). The researcher argues that this vulnerability may not only exploit organisational network systems, but also the human element (military members). Trim and Lee (2021) recommend that organisations should focus on their ability to predict and prevent future threats. In military organisations, the information aspect remains pivotal in respect of operations to be carried out and signal messages to be delivered faster. In the digital age, information is power. Obtaining information about possible targets and relaying it to operators in the field are thus critical for a mission's success (Sigholm, 2016). The section that follows extends the discussion of cybersecurity measures by specifically focusing on the role of the SANDF in cybersecurity.

2.10 Cybersecurity in the SANDF

Despite being a powerful entity in South Africa, the SANDF is just as vulnerable to cyberattacks as any other entity or organisation. This view is substantiated by former South African Minister of Defence, Nosiviwe Mapisa-Nqakula, who reiterated in several of her recent annual budget speeches to parliament that cyberthreats are of significant concern for South African society and the SANDF. Several security utterances about cyberthreats have been made by the former Minister of Defence and other authority figures within the South African security cluster. This previous security-related utterance was repeated by the new South African Minister of the Presidency, Mondli Gungubele, in the State Security Department Budget Vote 2022/2023 (RSA, 2022). The first point of focus could be directed at the speech the former Minister of Defence made during the Military Veterans Department Budget Vote 2017/2018, when the minister indicated that the DoD "will provide a comprehensive departmental Cyber Warfare Strategy and Sensor Strategy to the Justice, Crime, Prevention and Security (JCPS) Cluster Ministers for approval. We are seized to the matters of Cyber Security in the country" (RSA, 2018, para. 62).

In the excerpt of the Minister of Defence's speech, very little was mentioned about the aspect of security measures relating to cyberthreats. However, mention was made of the Cyber Warfare Strategy, which is still in the development phase. The researcher found that the SANDF has a mandate to mitigate cybersecurity threats, as noted in the NCPF (RSA, 2015b). The second point, which follows below, from the new minister's speech during the Defence and Military Veterans Department Budget Vote 2021/2022 was as follows:

> We are not immune to fundamentalism and extremism, terrorism, cybercrimes and organised crime. All of these are significantly increasing on the continent and in the region. Defending South Africa, protecting its people and safeguarding our borders and the economy extends to our landward, maritime, airspace as well as our cyber domains (RSA, 2021, para. 36).

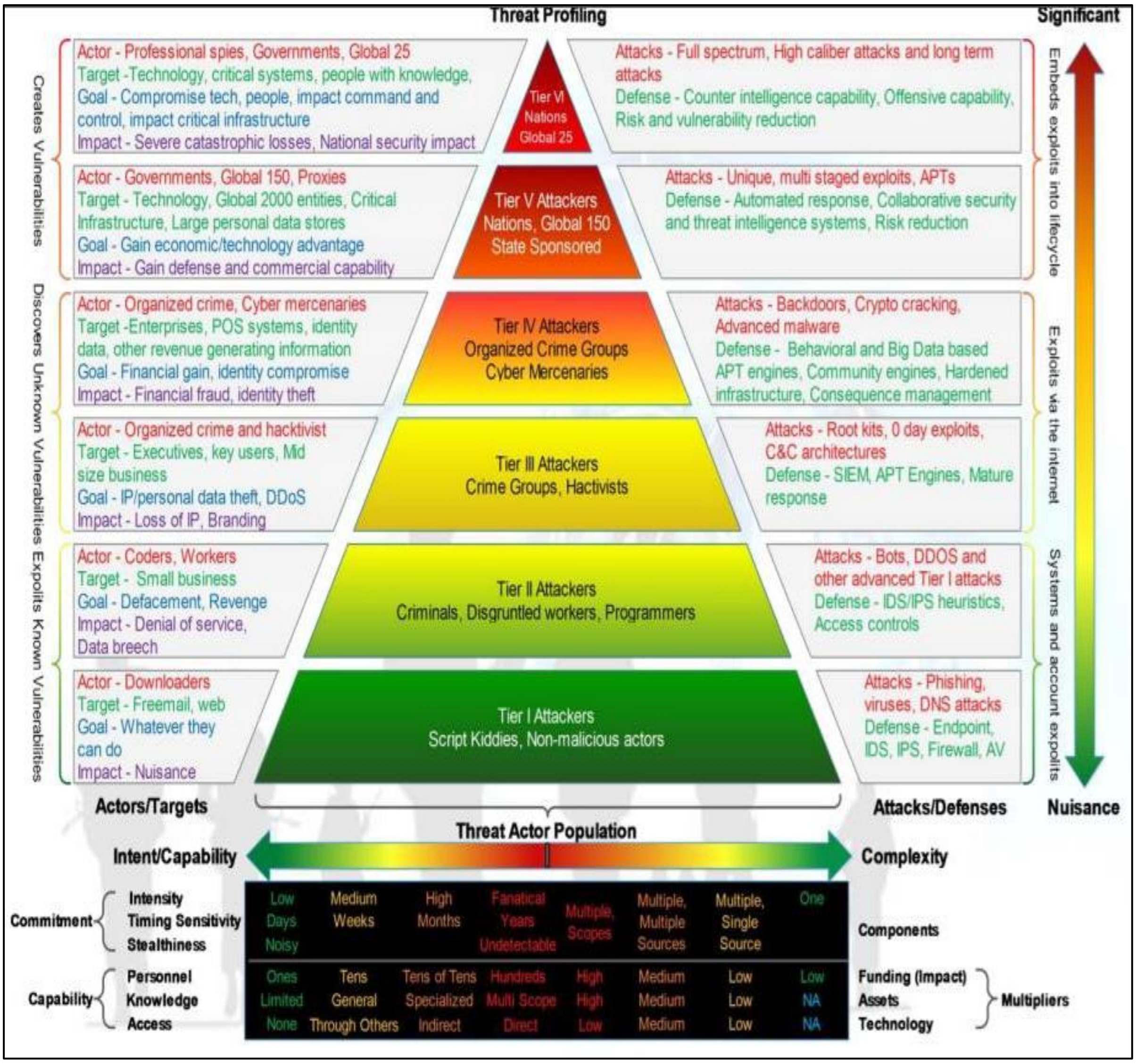
The information supplied by the minister renders it evident that cybercrime has an impact on various sectors in society. Moreover, the excerpt from the minister's speech shows that cyberthreats are challenging notions in which sovereignty presents security concerns for the nation and its interests. The researcher argues that the excerpts confirm that cyber is included in the range of threats that are challenging South Africa, which also include maritime security. Furthermore, what is interesting to note is that cybercrime was seemingly mentioned as falling in the same category as extremism and terrorism. This emphasises the significance of cyberthreats and the challenge it poses for society, and the challenge it presents for the SANDF with regard to ensuring the mitigation of threats. The SANDF realises the importance of cybersecurity, especially since the organisation engages in cyber surveillance in association with law enforcement and intelligence services (Molwantwa, 2019).

The researcher changed the discussion to the role of the SANDF in the mitigation of cyberthreats to the NCPF (RSA, 2015b). The NCPF outlines the role of the SANDF as follows:

> The DOD and MV have the overall responsibility for the coordination, accountability and implementation of cyber defence measures in the Republic as an integral part of its national defence mandate. To this end, the Department will develop policies and strategies pursuant to its core mandate (RSA, 2015b, p. 94).

The aforementioned description of the duties of the DoD makes it evident that a core activity is to maintain cyber defence. A key part of establishing this level of defence is to identify and target specific threats and adversaries that might act against the national interests of the nation (Ngcobo, 2020). Ngcobo (2020) provides a detailed threat profile for identifying threats and malicious actors based on hierarchy, as shown in Figure 2.1.

Figure 2.1: Threat profile of threats and malicious actors


Threat Profiling
Significant
Creates Vulnerabilities
Discovers Unknown Vulnerabilities
Expolits Known Vulnerabilities
Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact
Tier VI Nations Global 25
Attacks - Full spectrum, High caliber attacks and long term attacks
Defense - Counter intelligence capability, Offensive capability, Risk and vulnerability reduction
Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability
Tier V Attackers Nations, Global 150 State Sponsored
Attacks - Unique, multi staged exploits, APTs
Defense - Automated response, Collaborative security and threat intelligence systems, Risk reduction
Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft
Tier IV Attackers Organized Crime Groups Cyber Mercenaries
Attacks - Backdoors, Crypto cracking, Advanced malware
Defense - Behavioral and Big Data based APT engines, Community engines, Hardened infrastructure, Consequence management
Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding
Tier III Attackers Crime Groups, Hactivists
Attacks - Root kits, 0 day exploits, C&C architectures
Defense - SIEM, APT Engines, Mature response
Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech
Tier II Attackers Criminals, Disgruntled workers, Programmers
Attacks - Bots, DDOS and other advanced Tier I attacks
Defense - IDS/IPS heuristics, Access controls
Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance
Tier I Attackers Script Kiddies, Non-malicious actors
Attacks - Phishing, viruses, DNS attacks
Defense - Endpoint, IDS, IPS, Firewall, AV
Embeds exploits into lifecycle
Exploits via the internet
Systems and account exploits
Actors/Targets
Attacks/Defenses
Nuisance
Threat Actor Population
Intent/Capability
Complexity
Commitment
Intensity
Timing Sensitivity
Stealthiness
Low Days Noisy
Medium Weeks
High Months
Fanatical Years Undetectable
Multiple, Scopes
Multiple, Multiple Sources
Multiple, Single Source
One
Components
Capability
Personnel
Knowledge
Access
Ones Limited None
Tens General Through Others
Tens of Tens Specialized Indirect
Hundreds Multi Scope Direct
High High Low
Medium Medium Medium
Low Low Low
Low NA NA
Funding (Impact)
Assets
Technology
Multipliers

Source: Ngcobo (2020)

Figure 2.1 clearly indicates that establishing a threat profile is an important step towards taking strategic and precautionary measures according to the type of threat. By critically engaging with Ncobo's (2020) views in Figure 2.1, it appears that the South African government has classified a multiplicity of threat actors in cyberspace according to their target and attack mechanisms, as can be viewed in Tiers 2 to 4. The figure points out that crime spans Tiers 2 to 4 and distinguishes between the attackers and threats. This points towards South Africa's high crime levels and lower robustness that is also assuming a growing cybersecurity side, while Tiers 1 and 2 are not clearly visibly at play in South Africa. The figure also points out that the level of commitment and capability needed to address certain attacks on the organisation range from significant to nuisance. Tier 4 attackers are classified below the significance level.

Van der Waag-Cowling (2017) suggests that a response to the increasing threats should be to develop advanced digital open-source intelligence and that social media intelligence capability is also required. Dodd et al. (2020) suggest that cyber operations should be considered for South African members of the military, especially as this is a growing area of interest. Garcia (2017) proposes that emphasis needs to be shifted to cyber operations in the South African armed forces context. Leenen et al. (2018) refer to creating a cultural bridge concerning cybersecurity in military contexts. Furthermore, Aschmann et al. (2015) argue that cybersecurity is an important component in establishing cyber sovereignty, while also averring that the creation of an African cyber army would assist with enabling the military to reach its objectives in the protection of cyber and defence against cyberattacks by an enemy. PMG (2020) and Jansen van Vuuren et al. (2014) highlight that the CSIR supports research carried out in the SANDF domain that specifically provides insight into cyber warfare. The NCPF (RSA, 2015b) makes it clear that the role of the Cybersecurity Response Committee is to guide and coordinate efforts to address cybercrime, cyberterrorism, cyber espionage, cyber warfare, and other cyberthreats. However, Van der Waag-Cowling (2017) argues that the NCPF (RSA, 2015b) is part of a fragmented approach by the South African government as the framework relies on information sharing among various stakeholders and requires being properly resourced to mitigate cyberthreats.

While South African literature on cybersecurity advances the dialogue on awareness, online behaviour, and cybersecurity culture, attention is rarely paid to exploring cybersecurity in the South African armed forces context (Garcia, 2017; Aschmann et al., 2017; Van der Waag-Cowling, 2017; Van't Wout, 2017). Furthermore, pertinent issues linked to training and education in cybersecurity are not specifically indicated as a priority in the DoD's annual report (RSA, 2020b). Van der Waag-Cowling (2017) and Aschmann et al. (2015) suggest that training and education are important for enhancing cyber capacity in the armed forces context. Venter et al. (2019) argue that efforts to bring about cybersecurity awareness require routine practices and that the aforementioned efforts alone may not necessarily be enough to create awareness of cybersecurity among South Africans. In elaborating on this view, Van der Waag-Cowling (2019) suggests that the focus should be on finding a balance between cybersecurity training at the tertiary level and professional military training. Furthermore, the researcher of this study makes the statement that if military personnel were to undergo formal training combined with their professional military training, this would further entrench existing knowledge of cybersecurity awareness in the organisation. Venter et al. (2019) assert that computer science education leads to improvement in how users interact with mobile device security and privacy issues and therefore contributes to increased security awareness and better precautionary practices. The literature and discussion in this sub-section go some way to indicating that cybersecurity awareness training inspires a variety of positive behaviours that may have an impact on the organisation's approach to cybersecurity.

The researcher argues that this is an important link to consider for the purpose of this study as at present there is limited focus on the human factor. The researcher indicates that there are two main arguments for why there is an absence of the human factor and a focus on the military officer: (1) the role of the South African military officer is underplayed, especially since it is the human factor that highlights aspects of psychological vulnerability and risky online behaviour (Dlamini & Mbambo, 2019; De Lange, 2012), and (2) there is an absence of existing literature with a focus on military officers in the cyber domain. The relevance of this domain for security in the South African context necessitates additional research in order to fill this vacuum. Progress concerning research that emphasises cybersecurity legislation and efforts to enhance awareness capacity in public-private partnership domains is noted, but the apparent lack of focus on military perceptions remains (Ramluckan et al., 2020; Van't Wout, 2019; Aschmann et al., 2018; Leenen et al., 2018).

Research focusing on the South African military officer is essential as the SANDF will continue to experience challenges that require greater emphasis on human functioning and a core focus on cyber operations (Garcia, 2017). The South African government has created structures to ensure that national cybersecurity is achieved by strategically allocating tasks to major stakeholders who oversee and coordinate efforts to mitigate threats (RSA, 2015b). The Cybersecurity Hub is South Africa's national Computer Security Incident Response Team (CSIRT), which focuses on making cyberspace friendlier in terms of minimising threats and attacks on users in South Africa (RSA, 2015b). The South African government has given the CSIRT the responsibility to ensure that its citizens are able to share information securely and to communicate without any restriction or threat of being harmed. While the State Security Agency has the overall responsibility for managing the CSIRT, it has a strong relationship with the SANDF with regard to sharing critical information relating to cybersecurity threats and possible attacks (Malatji et al., 2021; RSA, 2015b).

The SANDF has been collaborating on cybersecurity with state entities such as the CSIR, Armscor, and the State Information Technology Agency (RSA, 2010). The aforementioned information links up with section 50(3) of the Defence Act 42 of 2002 (RSA, 2002b, p. 46), which provides the following:

> To the extent necessary for security and the protection of information, members of the Defence Force and employees may be subjected to restrictions in communicating any kind of information and, where appropriate, may be subjected to the prohibition of communication.

There are also other policies in the SANDF that highlight matters relating to the security of communication. For example, the instruction in the Policy on the Disclosure of Defence Information[13] (RSA, 2011c) addresses the actors that are allowed to access DoD information and the preservation of confidentiality. In addition, the SANDF also issued a policy on the use of electronic communication[14] (RSA, 2013a), which indicates software and its official use.

While the SANDF is collaborating with other state-affiliated stakeholders, the organisation itself has taken some precautions in creating a policy that allows for the interception and monitoring of all DoD data, transactions, and information communicated externally or internally (RSA, 2010). The South African government has shown good leadership in this regard as it transparently reports the vulnerabilities experienced in systems across the public sector, private sector, and civil society. This was expressed in the 2018 defence budget speech to the National Assembly, where the former Minister of Defence mentioned the presence of and rise in cyberthreats and cybersecurity more than once (RSA, 2018) However, in the South African Budget Vote (RSA, 2021), there was no mention of the critical nature of maintaining cybersecurity, which is echoed by the funding allocated to the SANDF. The Report of the Portfolio Committee on Defence and Military Veterans on Budget Vote 26 showed that cybersecurity in the SANDF has been placed on a secondary agenda owing to the operational demands of the COVID-19 pandemic (PMG, 2022). What this means is

[13] Policy on the Disclosure of Defence Information (POL&PLAN NO/00022/1999).

[14] Policy on Electronic Mail in the Department of Defence (CMIS/00011/2001).

that in the longer-term reality, the human element must be empowered in the SANDF by equipping the members of the corps with the necessary cybersecurity skills and awareness. The researcher argues that the human element in the SANDF might exacerbate this disconnect between noted cybersecurity vulnerabilities and the threats associated with limited spending on putting the right measures in place. It is therefore critical to determine how to ensure that cyber intransigence among military officers, for example, does not make this worse.

Although the South African Defence Review (RSA, 2015a) does not refer to the vulnerability of military personnel in connection with cybersecurity, it does refer to the cyber factor being of concern to the organisation and that it requires attention. The South African Defence Review (RSA, 2015a) indicates that the SANDF is in a state of decline, which means that contextual challenges such as budgetary constraints may further hinder the development of the cybersecurity capability. Owing to this constraint, the military officer may be considered as a vulnerable population group as cybersecurity skills development is not acknowledged as being of importance (Martin, 2020). The lack of skills development and limitations in organisations may therefore imply that this is an actual threat to the human factor.

It is worth noting that the SANDF is in a state of decline, which might pose a challenge for the critical defence infrastructure that is able to counter new and emerging threats (RSA, 2015a). Furthermore, the South African Defence Review (RSA, 2015a) points out some vulnerabilities with regard to building cybersecurity capacity in the SANDF. Cybersecurity education and training remain of fundamental importance in advancing knowledge and awareness in personnel (Aschmann et al., 2015; Van't Wout, 2019). Linking this argument to the SANDF, the human domain should be considered as important as the role of technology alone may not be sufficient to ensure cybersecurity. The human element remains the weakest link, according to the literature on this aspect, and thus requires close attention from defence decision makers (Ani et al., 2019; McMahon, 2020; Van't Wout, 2019).

Military officers are also individual consumers and are not immune to cyberthreats (Karaman et al., 2016). Concerning the digital space in the SANDF, military members have been scrutinised for utilising cyberspace and sharing information without adequate security measures being in place (Martin, 2020). The military is a population that has not received much attention with regard to cybersecurity in the South African context. One of the reasons could be that fewer research studies have been conducted on defence. Overall, collaborative research efforts between civil society and the military in South Africa have declined since 2004 (Janse van Rensburg, 2019). In addition, research and scholarly research on military affairs have little prominence in South African literature. This literature gap is echoed in the topic of cybersecurity in the SANDF. However, the researcher notes that this absence of military literature is not a general trend and is more visible outside of South Africa. Ramluckan et al. (2020) suggest that due to the mandate of the CSIR to perform research for the SANDF, the result is that there is very limited interaction between academic institutions and the DoD.

Social science research in the SANDF has not specifically emphasised the emergence of cybersecurity as central to understanding the changing organisational culture brought about by cybersecurity. This type of research has neither focused explicitly on notions of risk nor precautionary behaviour relating to cyberspace. Emphasis has been placed on training and education as factors that allow for the mitigation of cyberthreats. However, there is an apparent lack of military research on cybersecurity through the lens of social science. Recommendations by Van't Wout (2019) highlight that the human domain remains of concern in studies of cybersecurity as the motives and thought processes involved in navigating cyberspace are most often not considered. Yet, Aschmann et al. (2015) focus on the idea of future militaries and flag the importance of acknowledging the human being as at the centre of cybersecurity.

Alternative forms of research in the SANDF have been conducted, but cybersecurity was not the premise of those studies. For example, research in the SANDF has been geared towards military leadership (Bester & Du Plessis, 2015; 2014), career success (Rawoot et al., 2017), combat readiness, organisational climate (Makhathini & Van Dyk, 2018), and peacekeeping among military psychologists (Bester, 2016; Bruwer, 2016). However, this does not mean that it is wrong for cybersecurity not to be the focus. Instead, it strengthens the argument that cybersecurity is a neglected topic that deserves greater attention as an emerging threat in the South African context (RSA, 2020a; Ramluckan et al., 2020). The section that follows focuses on the perception of risk when navigating cyberspace.

2.11 The perception of risk when navigating cyberspace

The previous section focused on cybersecurity efforts made by the SANDF, especially since there is an increase in cyberthreats that have emerged in the nation state (Patrick, 2021; Pieterse, 2021; Van der Waag-Cowling, 2017). Focus must thus be placed on the military officer as an actor in the cybersecurity process by acknowledging the perception of risk when navigating cyberspace. This section presents one sub-section that focuses on the role of risk perception in identifying information in cyberspace. The role of perception is an important facet in this study as it appears in the research questions, as well as the overarching aim of the study. Furthermore, the role of perceptions was also the reason that the study engaged in a sequential design approach (see Sections 4.3 and 4.4). The world is on a changing path towards a space in which it is decreasing in size as communication globally is increasing, which allows civilians to share information on platforms across a borderless space (Du Toit et al., 2018; Leenen et al., 2018).

More specifically, users might be impacted by the risk posed by cybersecurity threats in the form of surveillance programmes, identity theft, phishing, viruses, spyware, and malware (Van Schaik et al., 2017). The perception of risk enables gauging how users perceive certain risks and identifies possible ways how they may respond to the threats (Du Toit et al., 2018; Larsen & Lund, 2021). Huth et al. (1992) suggest that the likelihood of risk occurring can be observed in the comparison of individual decisions that are based on the same values but that are essentially different. This statement implies that risk suggests the possibility of losing something. In the case of cybersecurity, from a very basic perspective, risk may refer to a loss of feeling secure, a loss of data, or the perception of the loss thereof.

With technological devices becoming more affordable and accessible, the risks are increasing, which may have negative implications online and offline (Jang-Jaccard & Nepal, 2014). Brantly (2021) indicates that the perception of risk in cyberspace is different than in other domains because the construction of risk in cyberspace is influenced by the following factors:

- The capacity to remain anonymous over a long period of time;
- The implications of cyberattacks are not straightforward and require a deeper exploration due to the interconnectedness of cyber and the technology used to advance these links;

- The complexity of cyber capabilities may stretch beyond the intended targets, which makes it very different from the physical threat of destructive power;
- The perception of risk linked to cyber is elevated due to the surge in cyberthreats; and
- The uncertainty of the cyberattacker's capability may also increase the perception of risk, as cyber creates a blacked-out screen, which makes it challenging to identify nefarious actors and their perceived motives.

When referring to cybersecurity and cyberspace, reference should also be made to the aspect of information security that governs the everyday lives and activities of people to an increasing degree.

The researcher argues that the risk perception of cybersecurity may be influenced by the following factors:

- The presence of reliable information regarding risks may influence how users perceive threats (Kahneman, 2011);
- The role of affect in interpreting information may also have an impact on how users perceive risk and ultimately form a perception of an object or event (Skagerlund et al., 2020); and
- Extrospection, which refers to phenomena where the user observes the behaviour of others and applies it to his or her own context (Martin, 2014).

The abovementioned information suggests that the role of perceptions has a variety of factors that may influence how individuals make sense of situations, as well as how this may influence behaviour. It is argued that the factors stated could provide insight into how risk information may inform the perception of cybersecurity as an outcome.

The Internet is being used more frequently and it has become an entrenched part of people's lives (Larsen & Lund, 2021; Schneier, 2015). Jansen and Van Schaik (2016) suggest that some of the precautionary mechanisms that should be enforced are precautionary behaviours related to how users navigate cyberspace and the risk attached to cyberthreats. Precautionary behaviour and risk perception should be connected to each other as functioning terms that co-exist in establishing awareness. In addition, acknowledging prevailing threats is said to be an essential facet in establishing a sense of awareness and developing risk perception behaviour (Van Schaik et al., 2017). The researcher argues that all these aspects are relevant to why the human factor is essential in the cybersecurity process as it is the individual who perceives risk and practises behaviour. Furthermore, the researcher argues that user behaviour in cyberspace and their online security behaviour all assist in the establishment of cybersecurity awareness; therefore making this study sufficiently relevant for exploring the cybersecurity perceptions and online behaviour of South African military officers.

Most individuals engage in some form of activity and daily weighing up of the benefits and risks of that specific activity (Brown, 2014). Larsen and Lund (2021) suggest that individuals use their subjective perception to interpret and evaluate the aspect of risk in their environment. In the case of cybersecurity, Larsen and Lund (2021) argue that risk perception is influenced by previous exposure to a threat and psychological elements that centre on uncertainty. There has also been a steady increase in how users are impacted by cybersecurity threats, especially during the COVID-19 pandemic, when the emphasis was on working remotely (Trim & Lee, 2021). The steady rise of cyberthreats may also pose psychological distress for users, especially if their personal data are at risk. The security systems that are normally in place in organisational settings were unavailable, which left users to rely on their own knowledge of cybersecurity (Trim & Lee, 2021). It should be noted that this state of affairs appears to be a long-term trend as opposed to only being a passing event during 2020, 2021, and beyond.

According to August et al. (2021), during 2020, organisations globally lost more than US$74 billion due to ransomware attacks. The problem that most nations are experiencing is that technology is constantly evolving and that threats such as malware and ransomware are also adapting to the times. It is believed that even though technology is increasing rapidly, the threat is not that organisations will be crippled by cyberattacks and plagued by threats; instead, it is that organisational challenges relate to the training of technical staff, reward-based incentives for maintaining security awareness and online behaviour, and internal and external threats (Herjavec Group, 2019; Ertan et al., 2018).

Technological devices such as mobile devices, including wearable smartwatches and Bluetooth headsets, are all prone to falling victim to cyberthreats and attacks (Herjavec Group, 2019). According to Cilliers (2020), technological devices, especially the mobile kind, are becoming more affordable and are Internet-enabled. The Internet, in association with technologies, ultimately constructs digitisation (Parusheva, 2019). Preventative behaviour through cybersecurity awareness in cyberspace becomes important in a situation where the overall security of systems and data is insufficient (Leenen & Jansen van Vuuren, 2019). By equipping users with a broad understanding of cybersecurity, they will be able to understand the kinetic and hybrid features of cyberthreats (Bardwell et al., 2017). Cybersecurity awareness training and education are an important factor in security efforts to sustain information security (Kortjan, 2013).

Furthermore, Van Schaik et al. (2017) note that a considerable amount of information concerning cyber hazards are published in the media. This can be corroborated by the amount of information reported or disinformation appearing on social media platforms during the COVID-19 pandemic (Bird & Lubisi, 2021). However, the information concerned with newer cyberthreats and challenges to information security may not receive the coverage it so desperately needs. This void in reported information may create distance between the acquisition of new knowledge and awareness in civil society, which may result in society being unable to mitigate cyberthreats. Jansen and Van Schaik (2016), as well as Van Schaik et al. (2017), reiterate that there are two aspects that should be considered when attempting to understand the risks contained in cybersecurity threats: (1) the first aspect is the nature of the cyberthreats and the countermeasures that are produced and disseminated among the population, and (2) the second aspect is threat perception, which deals with the users' engagement with and perceptions of threats. The perception of risks can be considered a crucial component when predicting behaviour (Boss et al., 2015). When dealing with the perception of risk, whether good or bad, a premise exists that the type of security information obtained and aspects linked to self-awareness about the vulnerabilities are important. Risk can be mitigated by highlighting the following elements: (1) the individual being self-aware of their own susceptibility to cyberthreats, (2) identifying the source when risk information is received, and (3) being aware of individual perceptions of professional expert knowledge (Van Schaik et al., 2017).

Garg and Camp (2015) argue that non-expert users of cyberspace need to be aware of the perception that expert knowledge of security systems is sufficient for remaining safe. Van Schaik et al. (2017, p. 7) also note that a predictor of risk perception is the notion of "common risks". A common activity, in this case, is the use of cyberspace. Keeping this in mind, the risk associated with a common activity may be perceived as minimal. Van Schaik et al. (2017, p. 5) refer to this notion as the lack of immediacy to act on potential security risks that emerge from “common activity”, which results in a possibly lower level of perception regarding cybersecurity. The extent to which cybersecurity is maintained depends on its users’ level of awareness, and online behaviour that is in line with best practices (Furman et al., 2012). Cybersecurity is also dependent on users who are educated in and aware of sound practices (Van’t Wout, 2019; Van Schaik et al., 2017; Furman et al., 2012).

Users are often under the impression that third-party organisations are responsible for maintaining online security (Furman et al., 2012). Behaviour is considered an essential component in addressing the need for an educated public to be cognisant of cyberthreats and the vulnerabilities of their systems. Sasse et al. (2007) recommend a framework that assists with user security behaviour. The first component presented in the framework highlights that awareness should be associated with the users’ interests. Secondly, education refers to active participation in considering the users’ knowledge foundation. Lastly, training refers to the systematic process through which users are provided with the proper tools and skills sets to adhere to best practices and render them functionally cognisant of cyberthreats and attacks. In addition to the suggested framework by Sasse (2007), Van Schaik et al. (2017) present practical factors that can be used to mitigate risk as follows: (1) Presenting a refresher course about threats to users who have very little experience with cybersecurity, (2) continuously educating users about the dangers associated with cybersecurity risks and highlighting the potential impact of threats, and (3) emphasising the concept of precautionary behaviour when navigating cyberspace and pointing out the notion of control when using security software as a basis for maintaining cybersecurity. Van’t Wout (2019) concurs with the above points by highlighting that training and education should take place by means of a series of initiatives that should be customised to meet the needs of the organisation and its current interests.

In conclusion, it is imperative to consider elements of awareness, training, and security behaviour as of crucial importance in shaping perceptions of risk. However, the ability to identify and discern between various pieces of security information is an aspect that should be viewed in the same light as receiving training and gaining a level of awareness. This section formed the literature basis for understanding the role of perceptions and risk; more specifically how perceptions can influence behaviour. The following sub-section focuses on the role that perception plays in the identification of risk information.

2.11.1 Perception as a key factor in identifying risk information

The presentation of information is fundamental in establishing a foundation through which an individual can assess preference, which in turn has an impact on the behaviour that is displayed (Chionis & Karanikas, 2018). Exploring the role of perceptions and the notion of risk is essential as it is able to point out how users interpret various objects and events of risk. This view is echoed in the rising cyberthreat rate, which amplifies the importance of the element of perception in cybersecurity. The social context plays a strong role in the creation of perception and, as a result, risk information is perceived differently by people (McDonald et al., 2000). This difference in perception is influenced by the knowledge people have, which they attribute to what they know about the social world (Tsfati & Cohen, 2013). The theory concerning the presentation of risk information may assist with explaining why risk-taking behaviour among individuals manifests differently (Van Schaik et al., 2017).

It is worth noting that positive perceptions that are linked to organisational change associated with information-sharing practices could be ascribed to efficiency in sharing information through practices that are clearly defined as a result of a trusting relationship established between the personnel and the management of the organisation (Ahmad & Huvila, 2019).

Van Schaik et al. (2017) and Schneier (2015) note that the aforementioned approach cannot be applied to the domain of online security and risks pertaining to privacy as empirical data relating to security breaches are considered unreliable. Schneier (2015) indicates that the risks are often under- or overestimated and might be sensationalised in the media. Sapriel (2020) argues that organisations and their stakeholders should communicate aspects of risk and potential threats more transparently. According to Ferrer and Klein (2015), risk perception is reduced when the threat enters an individual’s context and where there is very little control over the perceived impact it may have. On the other hand, Adams (2012) believes that when individuals have perceived control over their behaviour, it is assumed that their view of risk is minimised significantly. According to Rhee et al. (2012), when individuals experience perceived control over probable information, e.g., security breaches that are considered to be increasing, their perceived risk is reduced.

Owing to the emergence of some cyberthreats, people may overstress them. This may occur particularly when different fragments of information concerning contemporary and new threats are shared online. Kahneman (2011) suggests that the aspect of saliency comes into play when referring to the perception of risk information. Saliency in risk information is important when viewing the relationship between the severity of events and how it is accepted by individuals. This means that when information about threats is made available, how the threat information is interpreted by individuals may impact their perception of the risk. However, Prevezianou (2021) argues that low awareness of and a lack of clarity on the threat or incident might result in the management of an organisation underestimating the magnitude of the threat. Dobbie and Brown (2014) suggest that risk perception is a complex construct regulated by behaviour and cognition, which often have an impact on decision making, which causes feelings of fear and guilt, as well as establishing a sense of trust or distrust. As previously emphasised, the mode through which risk information is communicated has the potential to establish awareness and foster knowledge regarding cybersecurity, which may also help to establish the perception whether an individual is applying the necessary precautionary behaviour. Moreover, the element of uncertainty is strongly associated with the aspect of risk (Sjöberg et al., 2004). Furthermore, risk and behaviour, along with the aspect of psychological uncertainty, could arguably be regarded as key factors when individuals respond to certain situations that have consequences (Sjöberg et al., 2004).

In addition, organisational culture might be a strong predictor of how employee perceptions are constructed (Lacey, 2010). Innovation and pioneering are identified as significant features of an organisation that is able to pursue technological and digital transformation as it facilitates an environment in which its employees are capable of fostering behaviour and adopting values that are inherent in a digitised culture (Fichman et al., 2014). Furthermore, the creation of knowledge might also influence perceptions and an employee’s approach to engaging with outsiders and sharing information (Al-Dawod & Stefanska, 2021). Furthermore, when employees are exposed to awareness training, their understanding of why third-party software and applications are placing the organisational information at risk might increase (Al-Dawod & Stefanska, 2021). In summary, risk perception is an important facet relating to how users may respond to cybersecurity and, as a result, undertake certain precautionary behaviour. It is thus important to focus on information sharing as a vital facet concerning the way that individuals receive pertinent security information, which in turn influences how they respond or do not respond to cybersecurity threats.

2.12 The importance of cybersecurity in information sharing

With the dramatic increase in the use of accessible technology and cyberspace, it has been observed that individuals from various sectors in society (government, industry, and society) have become dependent on mobile technologies and the Internet (Cavelty & Wegner, 2020). Users are more reliant on mobile technologies and the affordability of these mobile devices makes them more accessible to users (Mukiibi, 2019; Gazula, 2017). The emergence of new and affordable technology has facilitated access for a wider range of people than were previously able to access the Internet and share information or knowledge – whether private or official in kind. Gazula (2017) argues that this level of affordability may expose more users of cyberspace to potential threats and may even go beyond the individual level and pose security challenges for governments. It is worth noting that there is a variety of information-sharing activities that may be carried out in cyberspace (see Section 1.4). Affordability, greater access, and a variety of information-sharing activities red-flag indicators and defensive measures as essential when addressing security in an organisational setting and acknowledge the critical role of information sharing. The researcher notes that military officers' perception of information sharing is imperative as it frames how cyberthreats are interpreted, as well as how elements of security are understood. Moreover, the researcher highlights that information sharing is key in understanding how pertinent threat data are conveyed in the organisation.

Information sharing refers to the activity where information is exchanged between individuals or entities (Savolainen, 2017). The information shared often has a shared or equal impact on the social world of the parties who engage in the sharing practices (Savolainen, 2017). It is important to note that with the sharing of information on digital platforms, there are potential risks. According to Ball et al. (2015), many users lack the necessary awareness that accompanies online information-sharing practices.

Apart from being reliant on technology and digital platforms that facilitate the process of sharing information, there is also the notion of overconfidence in existing information security practices. Users may erroneously feel that they are efficient in identifying risks and adapting their security behaviour (Ball et al., 2015). Moreover, with increased sharing of information online, users sometimes become overconfident, which may result in unintentional or intentional security breaches (Ball et al., 2015). Al-Dawod and Stefanska (2021) point out that a strong sense of risk awareness might be present among a population that is aware of cybersecurity threats.

Changes in organisations may also result in differences in how information-sharing practices are perceived by employees. Ahmad and Huvila (2019) suggest that a positive perception of information sharing relates to organisational change internally and externally. Efficient and secure information-sharing practices are also linked with trust in the organisation. Alternatively, if organisational changes are perceived negatively, secure information-sharing practices will not be taken seriously (Ahmad & Huvila, 2019). The importance of information sharing links with key aspects such as who is sharing the information, why the information is shared, who should share sensitive information, and what is to be done with the information shared. These are all questions that must be asked in organisations when there is strong emphasis on awareness and maintenance of cybersecurity (Goodwin et al., 2015). The activity of information sharing involves a great deal of trust, which, when done effectively, can improve cyber defence measures by drawing on the knowledge, capabilities, and experience of the larger community. Organisations are also able to engage in information sharing with the broader community to obtain situational awareness and foresight in order to identify specific threat actors, tactics, and their coordinated patterns (Zheng & Lewis, 2015). On the other hand, limitations do exist in information sharing, as has been pointed out, which are bound to limit access to important forms of information, which can result in an increased level of frustration (Alam et al., 2021; Laitinen & Sivunen, 2019).

Moreover, D’Arcy and Greene (2014) indicate that the quality of the information security culture in organisational settings can be linked to how personnel adhere to policy or the suggested security guidelines. It can be argued that an organisational culture may exist even though personnel are not directly aware of safe information-sharing practices. In addition, Nævestad et al. (2018) aver that when organisations adopt a robust information security culture, the possibility that the human factor could cause a cybersecurity breach is considerably less. Ertan et al. (2018) argue that employees’ previous automatic behaviours and habitual behaviours could have an impact on the security culture in the organisation. Information sharing remains an important aspect of maintaining cybersecurity. The section that follows builds on the current section by presenting literature that deals with the information-sharing behaviour of individuals when navigating cyberspace.

2.13 Information-sharing behaviour in cyberspace

The previous section focused on the importance of cybersecurity in information sharing. This section focuses on the behaviour attached to sharing information. As technology and cyberspace develop and expand their reach to include more users, the capabilities of online tools are increasingly centred on online services and platforms that serve to create a space where individuals can interact and share information (Liou et al., 2016). Bălău and Utz (2017) indicate that information sharing is a strategic behaviour and suggest that many organisations invest in this strategic activity by introducing new technology and knowledge management systems to enhance operations. However, knowledge management and safe information sharing often fail in organisations because individuals’ social motivation is lacking and their behaviour shows this (Bălău & Utz, 2017). Murire et al. (2021) suggest that personnel can receive information security awareness training in an effort to educate them on what might happen in the organisation should the integrity of security management be challenged.

The literature follows a general approach to identifying the intricacies of information sharing among systems and people. In recent times, there has been an increasing shift towards understanding information sharing; specifically in viewing it from a behavioural stance (Liou et al., 2016; Bălău & Utz, 2017). The nature of communication has changed over time, as have the modes through which information is shared. Information sharing denotes an activity whereby information is exchanged and received (Liou et al., 2016). Liou et al. (2016) focus on information-sharing behaviour and the need to engage in online sharing activities. Liou et al.’s (2016) findings indicate that members of an online community share information online, based on collective values, identification, and information security, which have an impact on the level of trust and willingness to exchange information (Liou et al., 2016). The need to share information online is considered of key relevance in the construction of behaviour directed towards information sharing (Liou et al., 2016). Information sharing is crucial when it is a goal for the organisation to enhance its organisational knowledge (Zheng, 2009). This is particularly important as it may advance the organisation's ability to compete with other sectors and similar organisations (Soeters & Goldenberg, 2019). Organisational knowledge can be viewed as one of the deciding factors that contribute to the aspect of competition among individuals in an organisation, especially where it is viewed as having perceived power (Marouf, 2015).

Information sharing in the context of the armed forces pertains to key strategic information that assists in military operational activities. While the sharing of pertinent knowledge in the organisation can be related to the organisation's operational functioning, it has the ability to influence participants' perceptions (Marouf, 2015). Marouf (2015) also suggests that the reverse is possible, where personnel who view knowledge and information as power will be hesitant to disseminate it to other members of the organisation. However, trust and the social motivation to share are considered very important in maintaining cybersecurity (Pala & Zhuang, 2019). While official means for sharing information faster exist on social media platforms such as WhatsApp, it should be highlighted that these are not official means of communication[15]. In South Africa, official DoD security policy[16] documents caution South African military officers about information-sharing activities and to be aware of the organisation's measures of determining online activity. The SANDF has official documentation that advises its members on using social media platforms such as WhatsApp, yet this platform is still often used for official communication purposes (Patrick, 2021). The implications for security are linked to the fact that neither the South African government nor any company within its borders owns WhatsApp. However, it has been reported that military members have received communication about their orders and deployment duties via WhatsApp (Du Plessis, 2021). This poses a security challenge to the SANDF as official means of communication fall within the parameters of signals and signed official letters. The use of social media applications such as WhatsApp presents challenges for the traditional forms of military communication and

[15] DoD Instruction DOD/CMIS/R/318/1/P (ed. 4): Policy on the Use of Cellular Telephones in the Department of Defence (RSA, 2011b).

[16] DoD Instruction POL&PLAN NO/00022/1999: Policy on the Disclosure of Defence Information (RSA, 2011c).

the pace at which information is transmitted, which include erosion of the traditional, and therefore secure, communication modes in the SANDF. To counter this dissonance, the South African National Space Agency (SANSA) has designed an application called SANSA-App, which is designed to secure all communications of high-frequency users such as government departments and the SANDF and to assist them with planning their respective channels (SANSA, 2019). While cyberthreats have been of concern to South African society, the impact they may have on society could be detrimental and this threat includes the country's military establishment.

Overall, literature in which the focus is on information-sharing practices in the South African context is not limited (Marivate & Combrinck, 2020; Mashiloane et al., 2018). The emergence of this literature may feed into the greater debate regarding how behaviour is associated with cybersecurity. There are specific reasons why cybersecurity should be considered an important aspect across all domains in society, including military contexts. The following are the specific reasons:

- Cybersecurity is perceived as a sensitive topic when viewing it in line with maintaining national security (Karaman et al., 2016; RSA, 2015b).
- Cybersecurity can be viewed as an expert field of inquiry that requires knowledge to be integrated into the armed forces context in order to establish specialised cyber units (Leenen et al., 2018).
- Cybersecurity legislation is a challenge considering that technology is advancing much quicker than the promulgation of legislation, as can be observed in the NCPF, the Cyber Warfare Policy Framework, and the Cybercrimes Act (Sutherland, 2017).

The technical skills and capacity for a cyber-rich knowledge foundation are still in the process of being developed (Leenen & Jansen van Vuuren, 2019). It is therefore important that research in an armed forces context should continue with regard to cybersecurity as it may not only address some points of vulnerability but may also resolve urgent matters related to information sharing, cybersecurity awareness, security behaviour, cybersecurity capacity, and cyber defence strategies. This section showed the importance of behaviour in maintaining cybersecurity. The next section focuses on the creation of cybersecurity awareness as an input and an output to lower the risk of cyberthreats.

2.14 Cybersecurity awareness creation

Protective online security tools are necessary to prevent the loss of data and to secure network information systems. However, according to Moustafa et al. (2021) and Alotaibi et al. (2017), this may not be the best way to mitigate cybersecurity breaches, and instead a more comprehensive approach to security is required, where the users are actively involved in maintaining cybersecurity through applying security behaviours. Human behaviour in cyberspace has been identified as one of the key reasons why information security becomes vulnerable to threats. As previously identified, the human component is the weakest link in the security chain; emphasis should thus be placed on individual cybersecurity awareness by gauging what users' knowledge, behaviour, and perceptions should be (Zwilling et al., 2020). The focus on cybersecurity awareness at the individual level is significant to understand how individuals may practise cybersecurity behaviour in organisations (Hadlington, 2017).

Duvenage (2019) proposes that there are many methods of cybersecurity training. This can be done by means of face-to-face classroom interaction, online e-learning strategies, cybergames, and simulation activities (Duvenage, 2019). Furthermore, employees in large organisations develop higher levels of cybersecurity awareness due to the financial resources that are in place and policy frameworks that are enforced (Hadlington, 2017). Moreover, when linking cybersecurity awareness to an organisation that is as large as the SANDF, it is vital for these aspects to be in place as the military is responsible for ensuring overall national security. Highlighting levels of cybersecurity awareness is therefore crucial in this regard (Grobler et al., 2013). Bardwell et al. (2017) suggest that to build cybersecurity awareness in an organisation, training in factors relating to cybersecurity might be effective, especially when a basic form of training is presented. Training in cybersecurity in the military context might improve the performance of day-to-day duties when using a computer and the Internet (Bardwell et al., 2017).

Grobler et al. (2013) suggest that cyberthreats have the potential to inflict psychological and informational damage. Exploring cybersecurity awareness among people may therefore allow for an understanding of how awareness, knowledge, and cybersecurity behaviours differ. Grobler et al. (2013) argue that the following should be focus areas to develop awareness: (1) focusing on information related to malware and mitigating factors, (2) ensuring that physical devices and other facets of physical security are secure, (3) policies for governing the navigation of cyberspace, and (4) best practices focusing on how information sharing and communication are performed. Grobler et al. (2013) also argue that a basic cybersecurity awareness programme is required to improve individual security behaviour and skills in cyberspace. Ani et al. (2019) call for awareness education on cybersecurity to enhance individual security in organisations and ultimately to act as an additional element in the security capability of the organisation. Bardwell et al. (2017) suggest that cybersecurity education is pertinent in identifying internal risks related to a lack of knowledge of cyberspace and highlighting computer system vulnerabilities. Providing cybersecurity education to individuals may increase knowledge of security behaviour, which may in turn minimise the risk of the human factor being a point of vulnerability (Ani et al., 2019). This view corresponds with that of Hammarstrand and Fu (2015), who found that participants with a high level of cybersecurity awareness might present good security behaviour, which could be explained by their compliance with security measures. Ramluckan et al. (2020) argue that creating a multidisciplinary approach to cybersecurity in the South African context is problematic because of the rigidity of the National Qualifications Framework and the limited allocation of state resources to cybersecurity. Furthermore, Walaza et al. (2019) point out that ICT awareness in South Africa is not on par with the rest of the world and requires a significant amount of attention. Bardwell et al. (2017) emphasise that condensed and foundational training in cybersecurity may allow personnel with a limited computer science background to understand cyberthreats. Furthermore, this approach may also facilitate cybersecurity awareness challenges and the approaches used to mitigate cyberthreats (Bardwell et al., 2017).

Grobler et al. (2013) suggest that educating personnel may facilitate the advancement of a more secure workforce. Ntsaluba (2017) concurs with the notion of formalised training in the organisational context by focusing on increased Internet activity. The surge in local Internet activity in the past 10 years promoted the view that training related to cybersecurity awareness should be formalised (Ntsaluba, 2017; Pieterse, 2021). Mkhonza and Letsoalo (2017) suggest that large organisations might have difficulty creating interventions that are uniform and far-reaching. Van’t Wout (2019) cautions that a cybersecurity awareness programme in large-scale organisations typically takes on an umbrella or one-size-fits-all approach, which generally does not highlight important security behaviour that needs to be adapted at the same pace as the developing attack space. Van't Wout (2019) suggests that training programmes in cybersecurity should be based on the needs of the organisation. Ghazvini and Shukur (2016) indicate that training programmes should not only be conducted but that personnel should be evaluated pre- and post-programme to determine gaps and strengths and to measure their success. At an individual level, it might be argued that the conceptualisation of cybersecurity awareness might be influenced by factors such as language, assumptions about security, and belief systems (Khando et al., 2021). Janse Van Rensburg (2019) asserts that while the DoD in South Africa does have quality training programmes and training institutions, the challenge arises when military personnel must return to their various units once their training is completed. In addition, the lack of resource allocation and funding results in military personnel not being able to keep abreast with current training needs (Janse van Rensburg, 2019).

Ghazvini and Shukur (2016) posit that routine training in information security awareness might not be effective due to the lack of emphasis on critical thinking. However, e-learning methods have been identified as an effective method whereby users can engage with learning material, especially when a focus on the subject matter is deemed necessary (Ghazvini & Shukur, 2016). Bogdan et al. (2017) hold the view that organisations deliver training to their employees at a low cost by providing them with the necessary skills, which implies that remedying technical issues might be more expensive than to provide training and education to employees. Lehto (2015) argues that cybersecurity awareness is fine and well, but if users do not understand the training material and what awareness means, then the exercise might be futile. Abawajy (2014) points out that cybersecurity awareness may not necessarily be enough to ensure that users are completely secure, even if they have the appropriate cybersecurity protection knowledge to decrease cyberthreats. Cybersecurity awareness and knowledge training related to security tools are required if individuals are to mitigate risks effectively, instead of receiving theoretical knowledge only (Abawajy, 2014). Making such a move relates to practical training methods. One method that focuses on enhancing the user's practical understanding of cybersecurity is the phishing simulator, which aims to develop awareness in users by habitually and practically exposing them to phishing emails that contain suspicious links (Baillon et al., 2019). The phishing simulator provides the user with adequate tools to mitigate the risks (Baillon et al., 2019). It is worth noting that Fatokun et al. (2019) suggest that the more educated Internet users are in cybersecurity, the more likely it is that they are familiar with the threats, which is likely to have an impact on their online security behaviour. Alotaibi et al. (2017) argue that technical issues are not so much the issue regarding cybersecurity, but rather the inability of staff members to comply with policies in organisations. In this vein, Daengsi et al. (2021) argue that prior training and experience may contribute to how users interact with security issues such as phishing emails. In addition, Alotaibi et al. (2017) suggest that when personnel have had inadequate security awareness training, the risks associated with network or system vulnerabilities increase exponentially owing to the increase in the probability of human error occurring.

2.15 Conclusion

This chapter is concluded by stating that the bulk of the literature relating to cybersecurity focuses on governance and technical features in the digital domain. The literature review also highlighted the void that exists with regard to the production of knowledge concerning the perceptions of cybersecurity among South African military officers. This chapter first focused on defining cybersecurity. Thereafter, the human factor was discussed in relation to its role in the description of cybersecurity. The chapter also proposed an operational definition that incorporates both the technical and human factors. Furthermore, a discussion of the complex nature of cyberthreats was included in this chapter. A short discussion was provided of the legislative efforts made by the South African government in respect of cybersecurity. In addition, the discussion provided an in-depth view on the impact cyber might have on society and the potential challenges this poses for a country’s sovereignty. The chapter also provided a brief discussion of the link between cyberspace and the armed forces context, as well as the vulnerability of military organisations and their personnel, with emphasis on their reliance on cyberspace. The focus then shifted to the aspect of risk, which discussed the perception of risk and how individuals could identify potential risk information when navigating cyberspace. A brief discussion of information-sharing behaviour and cybersecurity awareness creation concluded the chapter. The literature presented in this chapter lays the groundwork for Chapter 3. The chapter also pointed towards the aspect that the wider focus on cybersecurity is on the technical features and training in the armed forces context, but not necessarily on the role of the military officer in the ambit of cyber. The common focus of cybersecurity in the case of South Africa rests on the development of awareness, cybersecurity legislation, and training and education. The common denominator in this case is identified as the void in exploring the perceptions of the military officer in the case of cybersecurity. This further highlights the importance of the military officer as a justified element of importance in exploring cybersecurity in the South African context.

The chapter that follows focuses on how cyber is considered an emerging threat landscape and how ST as a framework has expanded to include threats such as cyber.

CHAPTER 3:
SECURITISATION AS A THEORETICAL FRAMEWORK

3.1 Introduction

The previous chapter described the rise of cybersecurity and associated literature relating to the way it is viewed in general and in the military context in particular. This chapter explores the role of a theoretical framework for this study. A theoretical framework serves as a structure that summarises thoughts and concepts that have been tested in published work (Kivunja, 2018). The use of a theoretical framework such as ST served as the foundation to configure or assemble cybersecurity threats and to synthesise the findings of this study. Cybersecurity is a current reality, much debated and exposed to multiple views, and thus needs to be highlighted as a security threat with wide and unexpected repercussions that complicate understanding the phenomenon. The ST as a concept and theoretical departure was briefly introduced in Chapter 1. Different schools of thought are used to explain security issues in the social context, such as the Welsh School and the Paris School of Security Studies. Both schools of thought take on a sociological approach and distances itself from the normative concepts such as the speech act and the role of language in the security process (Floyd, 2007; Stępka, 2022). The ST was proposed by the scholars of the Copenhagen School (CS) to capture the security process when threats were promoted beyond normal political rule, which demanded extraordinary measures to resolve (Huysmans, 1998).

ST has become increasingly relevant in the construction of security threats and responses, but more specifically to explore the nexus of the human element and cybersecurity as a threat (Aydindag, 2021; Bote, 2019; Hansen & Nissenbaum, 2009). Moreover, ST also challenges normative ways of conducting security discourses in society and exploring the background processes of why actors pursue security agendas and why security is announced in certain ways (Stępka, 2022).

3.2 Overview of the chapter

This chapter first presents a discussion of the different views of security. Furthermore, the chapter provides an in-depth discussion of what ST entails. The chapter then focuses on the emergence of new security threats in the 21st century by touching on emerging issues such as threats in cyberspace. In addition, the chapter engages with the increased focus on ST. The focus of the chapter then shifts to ST and its interplay with cybersecurity. Following the latter discussion, the chapter provides a discussion of the role of the securitising actor and the referent object, which would allow for better understanding of the section that follows, which deals with how technification as a speech act occurs in the securitisation process. Moreover, the chapter engages with critique of ST by pointing out the shortcomings of the theoretical framework. The chapter then presents a discussion of how cybersecurity entered the military domain, which also lays the foundation for the subsequent section, which deals with how cyber is approached in the SANDF, but more specifically how securitisation is interpreted in the armed forces context.

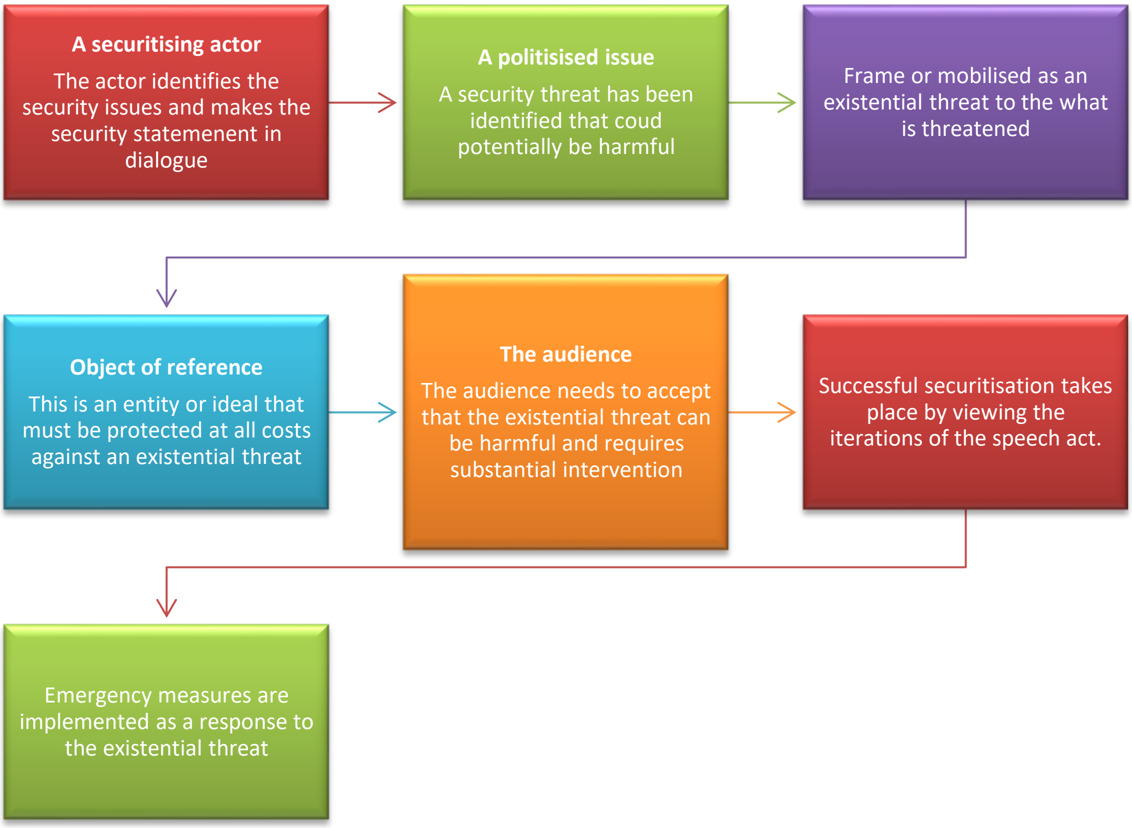
3.3 What is ST?

ST involves a process of intersubjective understanding regarding a security threat and managing it as an existential issue regarding a valued referent object. Framing a threat as existential and responses as extraordinary remains the difficult part, but in the overall ST debate this cannot negate ST in total as an explanatory theoretical construct. After the threat had been indicated, a call is issued in the political community to enable exceptional measures in response (Aydindag, 2021). The ST is a theoretical framework that has primarily been developed in the IR discipline (Kapur & Mabon, 2018). Van Ooijen (2020) notes that Buzan et al. (1998), the developers of this theoretical framework, based it on the work of Austin's (1975) speech act theory, which considers language as performative. Lucke (2016) argues that ST often focuses on aspects linked to war and conflict, especially when the securitisation process involved was deemed successful – when existential threats were resolved by means of extraordinary measures. Dos Santos (2018) asserts that the CS did not focus on a security perspective that it is based on either the objective or the subjective nature of threat perceptions. Instead, the CS focused on the role of decision making as an important factor for the "securitising actor" in the political community (Buzan et al., 1998). Decision making is therefore an important factor in the securitisation process because of the conditions that govern the speech act (Buzan et al., 1998). In addition, ST highlights the role of the state by emphasising how domestic and international issues could threaten those involved in the security process, including civil society and the state (Bote, 2019; Egloff & Cavelty, 2021). Securitisation offers a logical process through which measures are introduced and elevated to deal with existential threats (Eroukhmanoff, 2018). Linking this view to this study, the researcher argues that the linear progression of ST might not be applicable in some contexts. In the context of South Africa, the securitising actor (the state and authorised representative) has declared cyberthreats as threatening national security interests where the human factor is indicated as a potential actor that may place sovereignty at risk (RSA, 2018).

In the social context, the researcher argues that this politician-state-centred view might be countered by new thinking that questions this monopoly on an issue that carries the label of being securitised when the state as an organ of power must proclaim a specific issue to be a realistic threat to its citizens so that adequate measures can be taken to counteract or mitigate the threat. Philipsen (2018) argues that the traditional notion of ST can be challenged by the idea of who may speak of security. Traditionally, ST emphasises that actors in positions of authority are a precondition for speaking of security and possibly proclaiming the significance of the threat. Instead, Philipsen (2018) suggests that speaking of security should be the condition of authority. Egloff and Cavelty (2021) argue that ST gives consideration to the construction of policy linked to security agendas. A threat might therefore be classified as objective and even to a certain extent described as existential, but the true success of the securitisation process is achieved when the existence of threats is established and presented successfully in the political domain (Buzan et al., 1998). In terms of politics, the CS first considered public issues to be politicised, after which they were securitised (Hama, 2017). Based on this view, securitisation is the elevation of political issues beyond normal political practices designed to respond to day-to-day security threats and vulnerabilities (Hama, 2017).

Egloff and Cavelty (2021) assert that ST is grounded in the speech act theory, which purports that the use of language can be a performative act. Security speech acts that contain performative power can reconstruct and change social reality. This may in turn influence how security is described within social and political contexts. Furthermore, the security responses to threats may also be influenced by the security utterances of the actors (Stritzel, 2007). It is of key relevance that the ST process is understood in its sequential format. Figure 3.1 illustrates how the securitisation process may occur according to the CS.

Figure 3.1: Linear securitisation process and response


A securitising actor
The actor identifies the security issues and makes the security statemenent in dialogue
A politisised issue
A security threat has been identified that coud potentially be harmful
Frame or mobilised as an existential threat to the what is threatened
Object of reference
This is an entity or ideal that must be protected at all costs against an existential threat
The audience
The audience needs to accept that the existential threat can be harmful and requires substantial intervention
Successful securitisation takes place by viewing the iterations of the speech act.
Emergency measures are implemented as a response to the existential threat

Source: Researcher (2022)

Figure 3.1 shows that the securitisation process occurs in a series of steps. A tenet central to the theory described in the section above is to ensure that the securitising actor makes securitising moves, through which security utterances are related to the audience. Lucke (2016) argues that in order to gauge how securitising moves are performed, the facilitating conditions that evaluate the end result of the move, in other words the success or failure of the security move, should be considered. The facilitating conditions in this regard act as an important component to analyse the speech act (Lucke, 2016). The analysis of the speech act is evaluated by considering the success of securitisation processes in contexts by focusing on internal and external conditions[17]. Buzan et al. (1998) refer to the speech act but also reiterate that the conditions in which these acts and moves occur could be assessed to monitor whether the security utterances were misaligned or abused in political and social contexts. By connecting Figure 3.1 to this study, the researcher argues that South

[17] The internal conditions refer to the grammar used in the speech act, as well as the security logic conveyed. The external conditions refer to the position of the securitising actor and the context in which the securitisation process takes place (Lucke, 2016).

Africa has not complied with all the required elements in the ST process. It could be argued that the securitising actor identified cyberthreats as posing a threat to the state, the military, and its citizens (step one) (RSA, 2018). In step two, cybersecurity as an outcome to threats and attacks has been identified as a facet that requires development in the South African context (ITU, 2021). Relating to the third facet of the figure, the argument could be made that cyberthreats have not yet been elevated to a point where they are considered existential. Moreover, this study postulates that the human factor is essential in the cybersecurity process. By implication, the human factor is viewed as the audience and at the same time the object of reference. In the context of South Africa, especially in the armed forces context, there has been no focus on the member of the military as a source of vulnerability or involuntary threat actor.

Dos Santos (2018) highlights that the process of ST understands security aspects as a speech act with the ability to influence the securitising actor regarding security issues. Buzan et al. (1998) view features of securitisation as involving an actor and an audience. The securitising actor in this case refers to the role players who have decision-making power or have the ability to influence an audience by engaging in the speech act. In proceeding with this process, the referent object that is confronted by an existential threat must be safeguarded against the threatening circumstance by the execution of extraordinary measures (Dos Santos, 2018; Buzan et al., 1998). Eventually the existential and extraordinary labels become two of the uncertainties, but this is subject to implicit or explicit references to existential threats or whether military action is the only applicable extraordinary measure to follow. When referring to the responses to the COVID-19 pandemic by world leaders, the researcher argues that the insight and scientific input to leaders assisted an efficient response in implementing extraordinary, but non-military, emergency measures. The same can be said for the world leaders who were not inclined to take scientific advice and subsequently delayed making a decision about implementing measures (Forster & Heinzel, 2021). The next section focuses on the interdisciplinary views of security.

3.4 Interdisciplinary views on security

Cyber has developed to the extent that it has become interwoven with other disciplines such as economics, the armed forces, environmental areas, and social areas. As a result, it no longer restricts itself to the technical domain. The notion of security has taken on many meanings to a variety of sectors. The working definition of cybersecurity presented in Chapter 2 indicated that cyber should be viewed from an interdisciplinary perspective as this would allow for a comprehensive take on how security and concomitant behaviour associated with cybersecurity could be integrated into people's lives. The inclusion of cybersecurity in the new conceptualisation of security links to the idea that ST is still developing and allows the inclusion of newer threats such as cyber. The creation of an operational definition extends the later conceptualisations of security as indicated by Philipsen (2018). Furthermore, the operational definition allows for the newer connection to understand cyber as a non-traditional threat. The definition also brings human security to the fore and, in doing so, overcomes the earlier difficulties of limiting ST to politico-military security as existential. Furthermore, sectors such as environment, health, cyber, and economic have their own existential threats. Through this view one may add that threats stemming from these sectors are considered non-traditional as earlier thought on ST only considered threats to the state as existential. Later thought on ST thus allowed for new conceptualisation of security and a more expansive view of non-traditional threats. It is worth noting that cybersecurity threats may also be considered a national security risk; it might therefore be viewed as an existential threat and is deserving of being viewed through the ST lens. The narrative concerning cyber is also diverse and thus necessitates a definition that incorporates a well-rounded description (Bourbeau et al., 2015). The operational definition developed in Chapter 2 is as follows:

> Cybersecurity is a flexible security process through which individuals are constantly interacting with a technical environment and the social context. Cybersecurity is also the immersive process through which the human factor utilises security software tools in tandem with education, training, guidelines, technical knowledge, and best practices such as awareness training, technical skills, and risk assessment. Cybersecurity also requires the notion of applying knowledge to risk perception and precautionary behaviour, while being fully aware of vulnerabilities in both the physical and cyberspace domain.

This definition shows how cybersecurity can be approached from an interdisciplinary perspective and that it is applicable to various social contexts. The definition focuses on the element of security and addresses the aspect of the performative action as it relates to the proactive navigation of cyberspace with the intention of using security tools that are both technical and psychological. It is also necessary for the concept of security to be described in this section as it ultimately feeds into the understanding of ST and its processes. While this part of the section highlights the role of security in the working definition, it is vital for attention to be paid to how the concept of security can be interpreted from the perspective of various disciplines.

The concept of security is interpreted very differently across disciplines such as law, geography, criminology, psychology, sociology, politics, and IR (Bourbeau et al., 2015; O'Brien & Tropp, 2015). Not all disciplines are addressed in this section as the researcher was interested in the disciplines of psychology, sociology, and IR as the argument regarding ST in this study focuses on the human factor. The selected disciplines that expand on security were therefore applicable to this study. Bourbeau et al. (2015), in their book titled *Security: Dialogue across disciplines*, support studying security from the viewpoint of various disciplines. Romaniuk (2018) suggests that security is a concept that is socially constructed, which is generally subjective. This view lends itself to the debate that security as a concept cannot be tied exclusively to notions of politics and issues of national security. Furthermore, Romaniuk (2018) highlights that the CS of Security provides insight into the challenges relating to security that link with aspects associated with society. These aspects of security may originate in various domains such as a nation state, civil society, armed forces, politics, economics, and the environment. Changes in security threats and vulnerabilities within these domains therefore have the potential of having an impact on people and society (Romaniuk, 2018). The researcher argues that with this view went the notion that military officers could be influenced by the aspect of saliency (Van Schaik et al., 2017). Saliency is described as a process through which individuals become attracted to an event in their context; thus impacting their level of experience with and perception of the event (Van Schaik et al., 2017). The researcher furthermore argues that the level of saliency might have an impact on their perception of risk and how threats are accepted and interpreted. Philipsen (2018) notes that the meaning attached to threats might be extended owing to new security actors entering the domain. According to Bronk (2018), cybersecurity is a recognised security challenge in the field of security studies and cyber warfare in the realm of defence studies.

Psychology as a discipline lends itself to the notion of human security and concerns the idea of adjustment after a threatening event. With the notion of cybersecurity as a cross-disciplinary topic, it is advisable for researchers to explore cyber-related issues and their implications in the social environment (Kiboi, 2015; O'Brien & Tropp, 2015). Psychology is also one important field through which the construction of security behaviour can be studied and described. Bourbeau et al. (2015) suggest that the discipline of psychology contributes to the subjective factors that could predict perceptions and highlight feelings of insecurity, as well as the possible repercussions arising from the ways in which feelings of insecurity are displayed through behaviour and attitudes. The diversification of referent objects[18] in the engagement of security is apparent as psychology typically refers to human security[19] and can show how individual perceptions could create insecurity and possibly exacerbate conflict and threats (Bourbeau et al., 2015). Individual perceptions of cyber can provide insight into how security is approached in the digitalised domain. Cyber psychology (a subfield of study in the discipline of psychology) contributes to how members of the armed forces respond to threats and how aspects relating to resilience are maintained (Dando & Tranter, 2016). Furthermore, psychology also positions itself in the security debate by pointing out how communication and intelligence-gathering activities take place on digital platforms, with emphasis on the social cognition and behavioural patterns prevalent in groups (Dando & Tranter, 2016). The researcher thus argues that the exploration of perceptions is in alignment with the focus of this study, namely the human factor. The researcher submits that the object of reference is the human factor due to the vulnerability associated with security breaches (Van Schaik et al., 2017).

In recent times it has become evident that psychology has contributed to the study of cybersecurity. For example, McCormac et al. (2017) highlight that the human aspects of conscientiousness, agreeableness, openness, emotional stability, and risky behaviour are all predictors of how information security awareness is practised. The discipline of psychology contributes to ST by focusing on how technology is incorporated into everyday life and the way security behaviour is practised (Ancis, 2020). Lucke (2016) argues that psychology can provide insight into how individuals construct perceptions regarding security threats. Furthermore, psychology is a valuable fit with ST as it may facilitate understanding how or whether an audience

[18] The referent object used in this case refers to an object that needs to be protected against an existential threat. The term is often associated with national security or the state (Williams, 2007).

[19] See Section 2.3.1 regarding the human element being at the centre of a proposed operational definition.

accepts the extraordinary security measures proposed by actors who have political power (Lucke, 2016).

The discipline of psychology focuses on the human aspect of behaviour in the social context (Eysenck & Keane, 2015). ST, on the other hand, identifies the diffusion of power among actors and the division of roles (Aydindag, 2021). Understanding the role that perceptions play in the construction of threats might be essential to understand how threats are communicated to the audience and the particular mobilisation activities that are used to counter threats. Psychology assists in simplifying the complexity of the ST process (Lucke, 2016). This is done by specifically focusing on the individual actors and the perceived reality of threats. With regard to the latter, the implementation of intrusive security measures by the state during the COVID-19 pandemic illustrates how perceived existential threats are dealt with using extraordinary security measures (Business Tech, 2021). It is worth noting that the COVID-19 pandemic was a non-traditional threat that had an impact on the health security of society and thus also on human security. Dönges and Hofmann (2018) note that a broadening of the notion of how human-centred security is approached is necessary. The researcher therefore argues that the health threat that the COVID-19 pandemic posed transcended not just the state, but also had an impact on all spheres of society, including members of the military. In addition, the researcher notes that it is no longer only military threats that occupy the existential realm (state-centred). This view opens up the idea that cyberthreats may also pose significant risks to human security; thus positioning itself as a security issue with a scope that is broadened to include actors other than the state and a deepened security agenda that includes new threats (Dönges & Hofmann, 2018).

Traditionally, research in the domain of sociology focused on interpretations of collective cultural systems (Stampnitzky & Mattson, 2015). Sociology contributes to the field of security by focusing on interpersonal, economic, and social factors (Stampnitzky & Mattson, 2015). For example, a study conducted by Deeming (2016) indicated how government policies could have an impact on the social and economic sphere in society, which may deepen social divisions and enhance aspects of inequality, as well as insecurity. The sociology field has often shifted focus onto the armed forces context; thus expanding military sociology as a subfield within the discipline of sociology (Heinecken, 2017; Heinecken & Visser, 2008). With regard to the expansion of the discipline of sociology relating to military studies, Mandrup (2009) indicates that the concept of security includes individual needs, which enforces a human-centric view and indicates a departure from a state-centric approach to understanding security. Dönges and Hofmann (2018) note that society is impacted by various threats; it is thus important to broaden the scope and understanding of security and to move away from the state-centred view. Heinecken (2011) concurs with Mandrup (2009) about the move towards understanding the armed forces and the services they render. The researcher thus argues that contemporary military sociology more often than not addresses issues of human security.

Bourbeau et al. (2015) extend this discussion of the dialogue of security by noting that influential studies have been conducted in the IR discipline, which explored the notion of security. These studies include Williams' (2007) research, who focused on words and images that could be used to announce security threats. Bourbeau et al. (2015) suggest that IR analyse security in three ways. The first approach focuses on how a nation state is always considered a referent object. This can be observed in the notion put forward by Buzan (1991), who suggests that the only referent object is the state (see the adjustment of this view in Section 3.9). The second approach is how security is analysed, which assumes the stance of research territory and considers contributions made to ST. The third approach considered by the IR discipline, as stated by Bourbeau et al. (2015, p. 2), is as follows: "Critical approaches to security are incompatible with methods generally associated with positivist epistemology, whereas orthodox or traditional approaches to security cannot work with anything else than a positivist epistemology." What this implies is that ST studies are advancing the agenda of broadening the security debate, and it is a topic currently being approached from diverse perspectives.

Kapur and Mabon (2018) argue that contexts apart from Western views might have a different way of presenting speech acts and portraying securitising actors. A study conducted by Kapur (2018) critiques India's security discourse related to the strategic strikes on Pakistan during September 2016. Kapur (2018) argues that India's securitisation of the so-called Pakistani threat took place in two (speech) acts. The first act involved the illocutionary, which came before the extraordinary measure, which involved the Indian military engaging in a show of force in the Jammu and Kashmir regions (Kapur, 2018). What this implies is that the linear progression of ST may not necessarily be applicable in the political situation that prevailed between India and Pakistan. The second speech act occurred when India engaged in security utterances that involved the words “surgical strikes” (Kapur, 2018). Furthermore, ST highlights that the speech act always occurs before extraordinary measures are used (Buzan et al., 1998). ST therefore dictates that logic in the process is followed, yet this is very different in non-Western contexts (Kapur & Mabon, 2018). Based on the view of ST where the state is the referent object, it can be argued that the securitising actor (often the state) often utilises representatives to engage in speech acts (Buzan et al., 1998). The process of securitisation in the India-Pakistan scenario challenges the notion of the speech act occurring before existential measures are implemented.

The IR discipline and politics are closely linked, with security viewed as the distribution of power among critical actors in an international political system (Cavelty & Wegner, 2020).

Cavelty and Wegner (2020) also view politics as the main driving factor in cybersecurity politics. Bourbeau and Vuori (2015) suggest that the conceptualisation of security may involve gradual and fluctuating processes. This alludes to securitisation moves that may take longer and relate to contexts where threats have greater or lesser urgency. Linking this to, for example, the South African context, the steps of the ST process are still in progress whereby the Minister of Defence and authorised representatives are declaring cyber as a national security threat. Philipsen (2018) indicates that when a speech act is made, it binds itself to certain criteria. Furthermore, the researcher argues that by announcing cyberthreats as a national security threat, it had undergone several iterations; thus also indicating that something new had been added (Philipsen, 2018). New facets might nevertheless be added to the speech acts, which might present themselves in the increased attention that cybersecurity is receiving. This shift in iterative speech acts can be viewed in the DoD Budget Speech Votes of 2017/2018 and 2022/2023 (RSA, 2017a; 2022). The researcher posits that South Africa is in a prolonged process during which speech acts occur regularly. Bourbeau et al. (2015) argue that in order to study security, the focus should be flexible in order to recognise the distribution of power. The next section focuses on the emergence of new security threats in the 21st century.

3.5 The emergence of new security threats in the 21st century

Analysing security in the 21st century can be rather complex; depending on the region of the focus. Security concerns of nation states have become broader and definitely more complex (Cavelty & Wegner, 2020). These threats have developed from a focus on intergroup conflict and the control of societal groups to challenges that could potentially threaten systems that are linked to the global economy, society, and the environment (Pierce et al., 2018). Kavanagh (2019) suggests that as time progresses, new and emerging threats advance. Fouad (2019) argues that the range of "insecure" security objects has been broadened to incorporate individuals, businesses, and even electoral procedures. In addition, some threats such as global warming have remained on the international security agenda (Bueger et al., 2019; Bueger, 2015).

However, dangerous threats have emerged or re-emerged, namely piracy, human and wildlife trafficking, and narcotics smuggling (Larsen, 2020). In viewing piracy as a security threat to the economic stability of nation states, for example, governments and actors in the African Union, the European Union, and the North Atlantic Treaty Organization (NATO) have prioritised maritime security as one of the security objectives to resolve this problem (Bueger, 2015). Before 2008, it was evident that maritime security was a neglected security sector as not many nations were impacted. However, between 2008 and 2011, governments took note of the implications of piracy and maritime terrorism and the effect of this on inter-regional relationships (Bueger, 2015). What this implies is that maritime security has emerged as a significant threat in the 21st century and nation states have elevated the risk of maritime piracy and terrorism as major threats to national security. In addition, in both cases the threat grew in posture and danger, in response to which governments mobilised vast resources to combat their impact (Bueger et al., 2019; Bueger, 2015). It is important to note that the threat profile linked to the risk of maritime insecurity did not occur through government initiative alone as collaborative efforts by international (United Nations [UN]) and non-state (shipping lines) stakeholders assisted with the creation of threat awareness by allocating more resources to measures associated with mitigating risk and raising the threat profile. Bueger (2015) showed how the piracy threat in the domain of maritime security became securitised and inspired an extraordinary international naval response that is underpinned by UN resolutions to mitigate the impact of sea piracy and the danger associated with it.

In the case of cybersecurity, it is important to note that governments and the private sector are in a precarious position. Cybersecurity threats are too challenging for governments and businesses to manage alone. Failure to acknowledge cyberattacks and the scope of the threat they pose to sectors might prove to be a major test when an attempt is made to elevate the threat to a level where it receives sufficient attention (Chandrasekhar & Mee, 2021). The acknowledgement of a threat has consequences for a nation state. This implies that when threats are acknowledged, priority and resources must be provided to address the threat. Therefore, in the long term, societies and economies may flourish as a greater component of society and businesses admit their dependence on cyberspace (Fadia et al., 2020). In linking this to the argument concerning who the referent object is, the researcher adds to the idea that cyberthreats not only pose challenges for various sectors, the human factor also now forms part of the range of "objects" threatened by cyberthreats (Ani et al., 2019).

While maritime security is only one of the newer topics on international and national security agendas, cybersecurity has emerged as one of the latest security threats on these agendas, and has become a significant security topic (Larsen et al., 2022; Larsen & Lund, 2021). Solar (2020) posits that world leaders have acknowledged the complexities and challenges associated with security in cyberspace. In 2018, the UN Secretary-General, António Guterres, noted that cyberspace has become a space where cyber wars are being fought between nation states in a concealed manner (UN, 2018). Mihaela (2020) argues that the world has entered a period of information change, where technological capabilities have advanced opportunities in various domains. However, this emerging domain also sparked new threats, which present the danger of exposure of sensitive corporate data, information security challenges, and electronic challenges relating to phishing scams (Mihaela, 2020). Mihaela (2020) also extends the view of cyberspace as a threat domain by highlighting that the paradigm of security has evolved and introduced new topics for consideration, such as big data, information security, machine learning, and AI. In addition, cyberspace has been added as a late entry to the scope of new and emerging threats in the 21st century as the prevention of cyberattacks on critical infrastructure and important assets in the private and public sectors has increasingly become a national security priority (Wilson, 2015). It could be argued that, collectively, these developments now form a security sector of significance owing to evolving threats. If the sector's vulnerabilities are not addressed, they may have implications at national, corporate, and individual levels. This view positions cyberthreats as an acknowledged security issue and ties in with the section that follows regarding the rise of ST and the process of its development.

3.6 The rise of ST

The previous sections focused on the nature of ST, the various views arising from different disciplines in the study, and an analysis of security. This section expands on the focus area, namely the rise of ST and the developments that it inspired. This section commences with explaining that at the end of the Cold War, a debate was sparked over security in the IR field, which sought to classify how threats were viewed and anticipating what the response would be. To classify these threats, Eroukhmanoff (2018, p. 1) introduced the terms "narrowers" and "wideners" to describe the various positions that scholars took towards ST and the advancement of security agendas. The narrowers of security considered a state-centric approach, where the military and politics were seen as the focus of the security debate (Eroukhmanoff, 2018). The other path in the security debate, namely the wideners, focused on broadening the approach to gain an understanding of security through including other, non-military threats, which had consequences for people rather than the nation state. The researcher argues that cyberthreats not only pose challenges for the military, but also extend their reach by exploiting vulnerabilities in society. Hama (2017) proposes that, in a traditional sense, the state is the only referent object and, from a realist approach, that security cannot be broadened. This view has been challenged by the CS, the Welsh School, and the Human Security School (Hama, 2017). In challenging the idea that the state is the sole referent object, it is clear that a competitive notion concerning how security is approached beyond the centrality of the state is developing.

In a traditional sense, ST was created in a Westernised context and within the discipline of IR. However, in recent times there has been a shift away from understanding normative politics through a Westernised model and a more holistic approach to ST has instead been considered (Kapur & Mabon, 2018). The CS created the ST in the late 1980s to make sense of security challenges from a linguistic perspective. This particular framework allows asking security questions as they are linked with politics (Pram Gad & Lund Peterson, 2011). For example, security questions can be posed as follows: What constitutes a security challenge? What are suitable responses to security challenges? What are the implications of identifying and accepting something as an existential threat?

Acharya and Buzan (2017) have moved away from the aforementioned narrow application of the theory. They suggest that there have been shifts in how the application of ST takes place in non-Westernised contexts to account for security dynamics in which speech acts may not necessarily take place. This positions Acharya and Buzan (2017) among the wideners in the security debate. Buzan and Wæver's (2003) definition (see Section 1.7) makes no mention of military force being used in the hope of controlling the threat. This definition points to the construction of security within a political community. The security of a domain therefore does not always rest on challenges experienced in the military domain (Mutimer, 1997). Hirsch Ballin et al. (2020) argue that since the 1980s there has been greater emphasis on extending the concept of security to include aspects related to humanitarian, economic, and ecological security. Furthermore, the expansion of the security agenda included non-traditional threats that range from climate change to issues related to energy insecurity (Hirsch Ballin et al., 2020). However, this does not mean that the military is unable to address these non-obvious threats. Instead, the armed forces have transitioned from only being reactive to taking on an interventionist role in diffusing threats (Hirsch Ballin et al., 2020). In addition, Buzan and Wæver's (2003) definition does not explicitly address or privilege the use of force in response to the insecurity of a referent object deemed of vital interest to secure.

While the theoretical application of ST has been on a steadily increasing trajectory in interpreting security dynamics in the Western world, in a non-Western sense the theory has emerged slowly (Kapur & Mabon, 2018). This emerging development can be observed in the application of ST in non-Western contexts, where the focus is on the limitations of the speech act, political regimes, and the use of extraordinary measures that follow a speech act (Kapur, 2018). Advancing the ontological and epistemological features of ST in the CS can facilitate how political and social events could be understood more clearly (Mabon, 2018; Fox, 2008). Acharya and Buzan (2017) argue that ST, as understood through the CS, is increasingly being applied to cases in non-Western contexts to comprehend the discourse and the role that political actors play in constructing a security threat.

The CS is renowned for its extensive research and development in the security studies domain. Its original approach to describing security issues in a social landscape has been one of the most influential approaches, where ST is considered to have played an important role in providing insight into threats and their perceived impact (Balzacq, 2011; Hansen & Nissenbaum, 2009). The CS focuses on adding to the field of security studies by assuming a more critical stance relating to events that occur in certain contexts (Romaniuk, 2018). ST forms part of the post-positivist movement that was established in the work of Max Weber (Fox, 2008). In addition, the post-positive movement became part of the post-Cold War scholarship. The CS outgrew the normative political debate that centred on rationalism and realism (Charrett, 2009). It is important to point out that it was during the post-Cold War period that the USA and the Union of Soviet Socialist Republics started to pursue new and innovative technologies to achieve a dominant position (Netolická & Mareš, 2018). This is also the period when desecuritisation and demilitarisation occurred, which means that security issues that were previously accepted were no longer considered as the only priority (Buzan, 2008). In addition, at the core of Max Weber's (as cited in Fox, 2008) idea of post-positivism is that social realities need to be acknowledged and understood in their totality and from the subjective perspective of the individual instead of the outside observer.

ST advanced to include newer security threats emanating from domains such as the maritime and cyberspace domains. This philosophical and practical development is ascribed to the various securitisation approaches described by the second wave of researchers of the topic (Karpavičiūtė, 2017). There are two main categories of researchers that have contributed to the deepening of ST (Karpavičiūtė, 2017). The first category focused on the philosophical and sociological features of ST, as dealt with by Balzacq (2015; 2011), McDonald (2008), and Hansen (2011), along with Stritzel (2007). The conceptualisation drive aimed at reframing ST allowed a different view of the relationship between facets in the security process, namely the securitising actor, speech acts, and the audience in terms of security threats, as well as context (Kapur & Mabon, 2018). Earlier sections in this chapter highlighted that new threats have emerged, which caused a change in how society adapts and responds to security issues, and ST as a process must to an increasing degree account for these shifts.

The second category in the new wave of ST highlights that the practical application of ST to various case studies relates to the legitimacy of threats (Balzacq, 2015). Those who have focused on peace and democracy are also included in the second category (Hayes, 2009). The second wave of ST researchers facilitated the rejuvenation of security and its challenges in the way that security is approached through considering various research designs and approaches (Karpavičiūtė, 2017). Furthermore, this is corroborated by Kapur and Mabon (2018), who mention that an alternative approach to viewing ST and its processes must consider non-Western contexts. Williams (2007), a second-generation ST researcher, highlights that securitisation is not considered a condition, but rather an outcome of the social process, which denotes the social construction of security threats. Security should therefore be viewed from various perspectives in order to frame the construction of meaning related to threats and security (Bourbeau et al., 2015).

Furthermore, Philipsen (2018) and Stritzel (2007) argue that ST and its relevance outside Western countries, especially as the practice of security logic and politics is shifting, are influencing how extraordinary measures are applied in securitisation. Philipsen (2018) denotes that the practice of security and its conditions of success may change over time. The conceptualisation of threats also shifts over time and is influenced by context. Huysmans (2006) contributes to the securitisation debate by suggesting that security speech and the practices associated with security employed by the state and societal elites are obscuring the approach to what is normal and what is exceptional. These scholars form part of the third group of alternative thinkers, who seek to understand securitisation in social contexts (Pram Gad & Lund Petersen, 2011). These authors' views also contextualise the social aspect of cyber in which this study locates itself. While the scholars are commenting from a political science perspective, cyber locates itself across domains and sectors. This enabled the researcher to understand the contextual elements of the securitisation process by noting the possible implications of the activities of the relevant actors and the effect this may have on the referent object.

When debating cybersecurity, Schwarz (2016) suggests that threats are constructed based on the importance attached to them by society and the necessity to initiate emergency solutions to resolve the challenge. The securitisation process comprises three separate stages. The first stage involves the speech act, which involves actors who can construct an existential threat. This existential threat can also come in the form of cyberthreats and cyberattacks, which may challenge the safety of a referent object. Owing to cyber operating on various levels in society, cyberthreats and attacks may pose a challenge to a variety of actors such as the state, business, and individual Internet users (Romaniuk, 2018; Buzan et al., 1998). However, one should note that cyber does not necessarily imply the onset of a threat. In addition, not every cyberthreat is existential in nature, but its constant rise and technological thrusts may cause a strategic effect that can bring threats closer to posing an existential risk. Furthermore, an example of the onset of a cyberthreat could be an offensive activity of strategic information warfare (Lehto & Henselmann, 2020). This is traditionally carried out during times of crisis, when adversarial communication systems are targeted to prevent a threat from escalating. The process of securitisation implies that a threat is elevated as existential and threatening the referent object so that it may either be classified as a mere information security breach of individuals' data or an existential threat to critical national systems in cyberspace. In this manner the threat may also include the security of the power bases of the state (Krickeberg, 2016; Buzan et al., 1998).

The argument can be made that the military is also a referent object. Van Ooijen (2020) argues that a connection exists between cyberspace discourses and war, which ultimately positions the military and the state as referent objects.

Military forces and key infrastructure such as national healthcare systems are at risk of cyberthreats and are often attacked (Edelmann, 2020). The prolonged exposure to a cyberattack may result in a government shutdown and a state of vulnerability in the offensive and defensive capabilities of its armed forces (Edelmann, 2020). When highlighting the acknowledgement of cyberthreats, attention can be paid to the Biden-Putin Summit in Geneva (De Moura & Goldstein, 2021). Biden acknowledged the key impact of cyberthreats on American critical infrastructure and cautioned that Russia's continued cyberattacks on American infrastructure will result in retaliation (De Moura & Goldstein, 2021). The dialogue between these heads of state on cybersecurity is critical in recognising the dangers linked to cyberthreats and the potential implications they may have for national security and the possibility of military responses. In addition, extraordinary responses now include offensive and defensive cyber warfare, as opposed to the previous view of responses confined mostly to kinetic military responses[20]. One may refer to earlier explorations of ST, which questioned whether collapsing critical infrastructure might constitute an existential threat that requires an extraordinary response. Owing to cyberthreats and attacks now being considered rapidly emerging threats, one may suggest that a significant cyberattack or counterattack may constitute an extraordinary response and particularly if under military command or combined with kinetic military strikes. However, in applying the abovementioned statement to the South African context, the researcher highlights the case of the cyberattack on Transnet, which forced the organisation to declare *force majeure* and resulted in extensive financial loss for the country's maritime sector (Smith, 2021). The researcher argues that if viewed in isolation, the Transnet cyberattack did not necessitate the South African government to declare the digital threat as an issue that required elevation beyond normal political debate. However, in the case of Transnet, the cyberattack was most likely criminal in nature and not necessarily state sponsored. A military intervention would therefore have been inappropriate. South Africa nonetheless securitised cyberthreats by formalising legislation to counter cyberattacks, declared it a national security matter, and placed the SANDF at the forefront of ensuring that cybersecurity threats are prevented, contained, and mitigated. In this way, if viewed as an outcome of ST, it thus allowed for traditional security and non-traditional security concerns and responses to be enacted to maintain national cybersecurity.

The researcher argues that a cyberthreat is not by implication existential. This can be observed in the case of South Africa, where the threat is merely introduced, with action characterised by a lack of urgency (Sutherland, 2017). Although legislative frameworks have been employed in South Africa, the existing lack of urgency is corroborated by the measuring factors proposed by the GCI (ITU, 2021). A successful securitisation process that involves the referent object is reliant on the subjective views of the audience concerning the legitimacy of the claims made by the securitising actor (Charrett, 2009). In addition, extraordinary measures are executed to safeguard the referent object against the existential threat articulated during the speech act stage. Lastly, the speech act is accepted and embraced, or rejected, by the audience(s) in the securitisation process (Romaniuk, 2018). Both relate to the success or failure of the

[20] When referring to kinetic military responses, the researcher points out the alleged Israeli airstrikes against a Hamas "cyber facility" (Cimpanu, 2021).

process of securitisation, or even leave the threat in limbo. The section that follows discusses ST and its interplay with cybersecurity.

3.7 ST and its interplay with cybersecurity

Exploring cybersecurity as a construct not only yields a basis of understanding but also enables the view that the term being explored should be considered from a social science perspective to include the human element. In addition, the operational definition used in this study attempts to highlight both the human element and the technical component, which are both linked to cyberspace. Furthermore, digital security in cyberspace is crucial and users' online behaviour and their methods to secure information might contribute to an increase in the susceptibility to cybercrime (Lahcen et al., 2020; Idahosa, 2020). With the development of the Internet as universal infrastructure, it can be considered a powerful tool that may be utilised by all for, among others, politics, espionage, and defence activities (Lahcen et al., 2020; Briggs, 2020; Lewis & Timlin, 2011). The digital space has also opened up a further security domain labelled "cybersecurity" that introduced dangerous threats to society, institutions, and nation states (Briggs, 2020).

Dinesen and Sæther (2013) extend the discussion by noting that ST can explain how securitising actors frame specific issues for an audience. This threat description can be uttered by multiple actors so that the existential threat achieves materiality. What this implies is that the utterances of the threat by actors need to be legitimised and appear tangible enough for the audience to perceive it as existential. Van Ooijen (2020) indicates that the legitimacy of the threat not only depends on the legitimacy of the actors, but also the discourse. Expanding on the aforementioned statement, cyberspace is a domain that is becoming significant in determining which force may win or lose in a time of war in the near future (Heartherly & Melendez, 2019). Herein rests the defence dilemma, as noted by Buzan et al. (1998), which focuses on the dire consequences of nation states losing a war and the lengths to which states would go to avoid military defeat by implementing appropriate security measures. For many countries, defeat in war (even if cyber is augmented) remains an existential threat.

According to Aschmann et al. (2017), a trend prevails among nations to adopt cyber and its asymmetrical features to neutralise an adversary's cyber capabilities. As far back as 2001, cybersecurity had become a real concern for nation states (Geers et al., 2014). Governments realised that cyberthreats may target the political, military, or infrastructural assets of a nation, or even members of the public (Singer & Friedman, 2014). The prevalence of cyberthreats is escalating, and more attention is being paid to the security aspect of cyber (Dinesen & Sæther, 2013; Hinsenveld, 2015). According to Hansen and Nissenbaum (2009), activists who advocate liberation and freedom of information point out the violations of governments where personal information is gathered for mass surveillance, such as in the case of Edward Snowden. On the other hand, authoritarian and even totalitarian governments securitise the flow of information as they regard it as a threat to national security and thus posing a direct challenge to the cyber sovereignty of its domain (Deibert, 2002).

It is possible to link Buzan et al. (1998) and their work to the securitising process that involves the speech act. Lo and Thomas (2018), McDonald (2008), and Buzan et al. (1998) suggest that three conditions facilitate a securitising move. The first security condition entails that acceptable security-related grammar should be used and must link cyberattacks as an existential threat to the state and its people. Pieterse (2021) suggests that cyberattacks are a threat to various spheres in society (social, transport, financial, construction, and ICT). The second condition requires an individual in authority or the state to announce cybersecurity as an existential threat. When linking this to the South African context and the securitisation of cybersecurity, cybersecurity has been communicated as a national security threat by the South African Minister of Defence (RSA, 2022) and as an existential threat and cybersecurity is considered a top priority for the SANDF. To date, no extraordinary measures have been implemented; thus falling beyond the ambit of the traditional military response, which is often seen as the typification of an extraordinary response. Philipsen (2018) argues that in the ST process, the focus should be on performative acts. This therefore indicates that the language used by authoritative actors must match the action through response. In addition, the perceived threat must be shown to challenge the security of the state or the individual (object of reference) (Lo & Thomas, 2018; McDonald, 2008; Buzan et al., 1998). The last condition allows for extraordinary measures to be introduced so that a securitisation move can occur. The state is able to allocate national resources in order for security measures to be implemented to mitigate national threats. In the case of South Africa, there has also recently been an increased allocation of resources and attention to address the growing cyberthreat rate.

Linking this to a similar example, the researcher referred to the COVID-19 pandemic period as a non-traditional threat, when there was an increase in support as the South African government responded by allocating extensive funding for social support grants to lower the impact on South African society and to fund the heavy military deployment required for policing activities during the declared state of national disaster. The example of the COVID-19 pandemic is also indicative of how previously neglected threats entered the realm of existential dangers, which drew extraordinary responses from decision makers. Cybersecurity is closely linked with this shift in understanding, framing, and responding to newer threat sectors. However, ST is not exempt from critique and has been a matter of dispute for years purely because of how threats are contextualised within the parameters of society (Bote, 2019; Dos Santos, 2018; Hansen & Nissenbaum, 2009). This concerns the notion that securitisation as a framework reserves its focus for referent objects and the extraordinary measures that are concomitantly implemented (Watson, 2011). Regardless of the criticism levelled at it, ST has developed into one of the more significant approaches to investigating challenges in security study contexts (Buzan et al., 1998).

The researcher argues that there ae some parallels between how the South African government responds to threats such as the COVID-19 pandemic and highlighting cybersecurity. The researcher argues that the political value attached to certain threats is an indication of the value attached to the responses, as well as the agency attached to the speech act (Philipsen, 2018). The researcher confirms that not all responses to threats are the same. Philipsen (2018) notes that this is based on the context in which securitisation takes place, and how conventional positions of security are challenged by new actors in the security process. In addition, Buzan et al. (1998) never mentioned a security threat such as the COVID-19 pandemic as health security threats hardly featured in the original understanding of the theory. Health issues and cyberthreats were not the core focus of ST when it was first developed by researchers at the CS (Wæver, 1998; 1995). Buzan et al. (1998) nevertheless argue that it is important to broaden the scope of what constitutes a security threat. Philipsen (2018) notes that the speech act in the securitisation process has the ability to shift the meaning of security in contexts. In addition, when considering a broadened view of ST, it is possible to see how new actors enter the ambit of security and attach alternative meanings to threats (Philipsen, 2018). The researcher notes that attaching new meanings to performative acts may impact how new actors deal with threats beyond military responses. Moreover, the researcher argues that with cybersecurity in the South African context, the response may not necessarily indicate successful securitisation, but rather an approach to embracing new actors beyond the political ambit to highlight cybersecurity measures. This may also reflect in how the South African government is currently recommending collaboration between the private sector and government departments (RSA, 2015a).

Returning to cybersecurity, the researcher argues that threat and response do not necessarily have to be at the centre of national security or that using force should be an emergency response. The issue with the securitisation of cybersecurity, besides meeting the requirements of the three logics posited by Hansen and Nissenbaum (2009), is that the narrative linked to security resources and the construction of the security threat are often misaligned. Cyberthreats, although increasing at a rapid pace globally, do not have an impact on everyone, but in cases of a threat such as the COVID-19 pandemic, everyone is at risk. The authoritative actors proclaimed the COVID-19 pandemic a threat by indicating its potential societal and economic impact. However, viewing authority as a precondition for security renders the theory unable to consider how new actors enter the securitisation process and challenge security logics (Philipsen, 2018). The audience in this regard is civil society and these new actors function as important facets in the securitisation process. The audience does not necessarily assess the securitisation process, but contributes to the shifting concept of security (Philipsen, 2018). In terms of cyberthreats, the South African government's response is not in the ambit of extraordinary measures, as observed in the securitisation process during the COVID-19 pandemic. For example, when one peruses the geopolitical consequence of cyberthreats, it is clear that some attacks are engineered to target specific regions or actors (Atrews, 2020; Gonzalez-Manzano et al., 2022). However, the effects of cyberattacks might be progressive owing to their financial implications (Public-Private Analytical Exchange Programme, 2019). Nonetheless, the precondition of securitisation becomes relevant when a general claim is made by the securitising actors, and the audience accepts that the object that is threatened needs to survive at all costs (Aydindag, 2021).

Furthermore, governments are also utilising cyber to enhance security measures but they may experience vulnerabilities in their sectors if appropriate security measures are not already in place to safeguard their interests (Public-Private Analytical Exchange Programme, 2019; Brangetto & Veenendaal, 2016). As cyber has become fundamental for the functioning of society, activities that were once considered accessible in the physical domain have now transitioned to being mostly online (e.g., e-commerce) (Eggers et al., 2018). As with the case of technological capabilities that guard against cyberthreats, they may only be effective up to a certain point in maintaining security (Bada & Nurse, 2019a). Governments have therefore acknowledged that the development of legislation aimed at cybersecurity and the role of security agencies are essential for the security process.

Cyberthreats can cause debilitating harm to the structure of and order in society (Idahosa, 2020). Izuakor (2016, p. 511), for example, suggests that cyberthreats can disrupt critical assets of nation states by targeting digital resources such as "data repositories, information network systems, information technologies and communication links". Moreover, cyberthreats, along with potential physical threats, could strike at a nation state's key critical infrastructure such as buildings, nuclear power plants, and power supplies (Izuakor, 2016). Viewed collectively, cyberthreats thus present dangerous ramifications for a state's power base, which includes its armed forces. The next section discusses the role of the securitising actor and the referent object.

3.8 The role of the securitising actor and the referent object

The state has always been viewed as a referent object with regard to security and, according to Buzan and Wæver (2009), in some ways the nation and its people can also be considered similar to the state. Floyd (2020) highlights that ST is not a once-off event, but rather a political process through which issues are transformed into security threats through a series of steps over time. Furthermore, Floyd (2020) outlines the process of securitisation by stating the securitisation sequence, which commences with the securitising actor engaging in a speech act or making a securitising move. The speech act is geared towards a declaration about a referent object being threatened (Floyd, 2020). This is followed by a focus on the audience, who must accept the securitising move, which then enables the deployment of extraordinary responses required to deal with the perceived threat (Floyd, 2020).

Khan et al. (2020) suggest that cyberthreats posed a threat to three sectors during the COVID-19 pandemic, which combined cyber and health threats, to present an even more dangerous threat to societies, governments, and even the armed forces. These three sectors, which are vulnerable during a pandemic, are healthcare, financial, and government systems. Van Ooijen (2020) argues that the discourse regarding cyberattacks is gradually increasing and while the effects of the attacks can be felt in a physical space, the ultimate consequences are often only experienced by those with expertise in and access to cyber. Bourbeau et al. (2015) acknowledge that the state is by far not the only referent object that is threatened by security issues. As the spectrum of national security is widened to embrace a collective system – one that is inclusive of technical and social systems – more than the state and its political regime could be threatened and often more severely so (Bourbeau et al., 2015).

Hjalmarson (2013) provides for a context in which securitisation can be best understood by stating that the securitising actor is responsible for leading the initiative to securitise an issue or threat, although this actor is also in a position to take these measures on behalf of society. This actor may come in the form of either the state or the nation (Buzan & Wæver, 2009). Furthermore, identifying the referent object is considered the next phase in the securitisation process. The referent object is a key component of the securitisation process and is identified as something that needs to be secured. The securitising actor creates measures or finds suitable security measures in response to the threat(s) to protect the referent object (Eroukhmanoff, 2018; Stritzel, 2007). In addition, the audience, or rather the nation in this case, is considered the target population at which the vulnerability of a specific referent object is directed (Balzacq, 2011). Adding to the discussion, the statement made by Balzacq (2011) points towards the notion that military officers form part of society and that the military as an organisation may also be vulnerable as a power base. Fundamentally, the researcher argues that both are vulnerable to cyberthreats. Eroukhmanoff (2018) substantiates the aforementioned statement by indicating that it is incorrect to believe that threats will impact individuals equally. For example, when referring to the military, the state is the referent object, whereas reference to an individual in the securitisation process means the object of reference is often identity (Eroukhmanoff, 2018). The researcher argues that there are many referent objects that need protection through emergency measures. Thus, although the state might be the referent object, as its national interests and sovereignty must survive at all costs, other referent objects also require consideration.

The researcher believes that there are additional layers of objects of reference that require survival and emergency measures to ensure their survival. With the human factor (South African military officer) as the focus of this study, it is argued that the psychological vulnerabilities of the human must be protected as cyberthreats and attacks are engineered to exploit the behaviour and emotions of human users (Rauf, 2019). The SANDF recognises that cyberthreats are a serious concern for national security (RSA, 2021). This necessitates the exploration of military officers' perceptions of cybersecurity, which plays an important part in determining the organisation's views of cyberthreats and how responses unfold. The researcher argues that the referent object is the SANDF. The reason for this is that the military is an important factor in the security cluster, which maintains national security and carries out strategic operations relating to national security (Van der Waag-Cowling, 2017). Figure 3.2 presents a diagram of the proposed objects of reference that indicate where the human factor locates itself as applicable to South Africa.

The researcher argues that cybersecurity is too often labelled a non-traditional security threat, but is one that has attracted ever-growing attention due to the surge of threats and attacks in the South African context. However, not every type of security challenge attracts attention, but when securitisation occurs of non-traditional security threats and it becomes a fixed threat item on the national security agenda, the securitisation claim might be more acceptable (Philipsen, 2018). The researcher also argues that through this process of progress, by also securitising dangerous non-traditional threats, security aspects may eventually be linked to the individual, the institution, the state, and the international level. The cyberattacks on South African ports underscore the relevance of the national and departmental cybersecurity regimes and bodies that South Africa has put in place (Smith, 2021). In the South African context, the researcher argues that the government has put in place extensive legislative measures and interdepartmental bodies to prevent cyberthreats that may push against national security, as well as the basic rights of the individual given surveillance, tracking of transactions, and linking any monetary movement of transactions in the name of prevention.

Figure 3.2: Objects of reference and their points of vulnerability

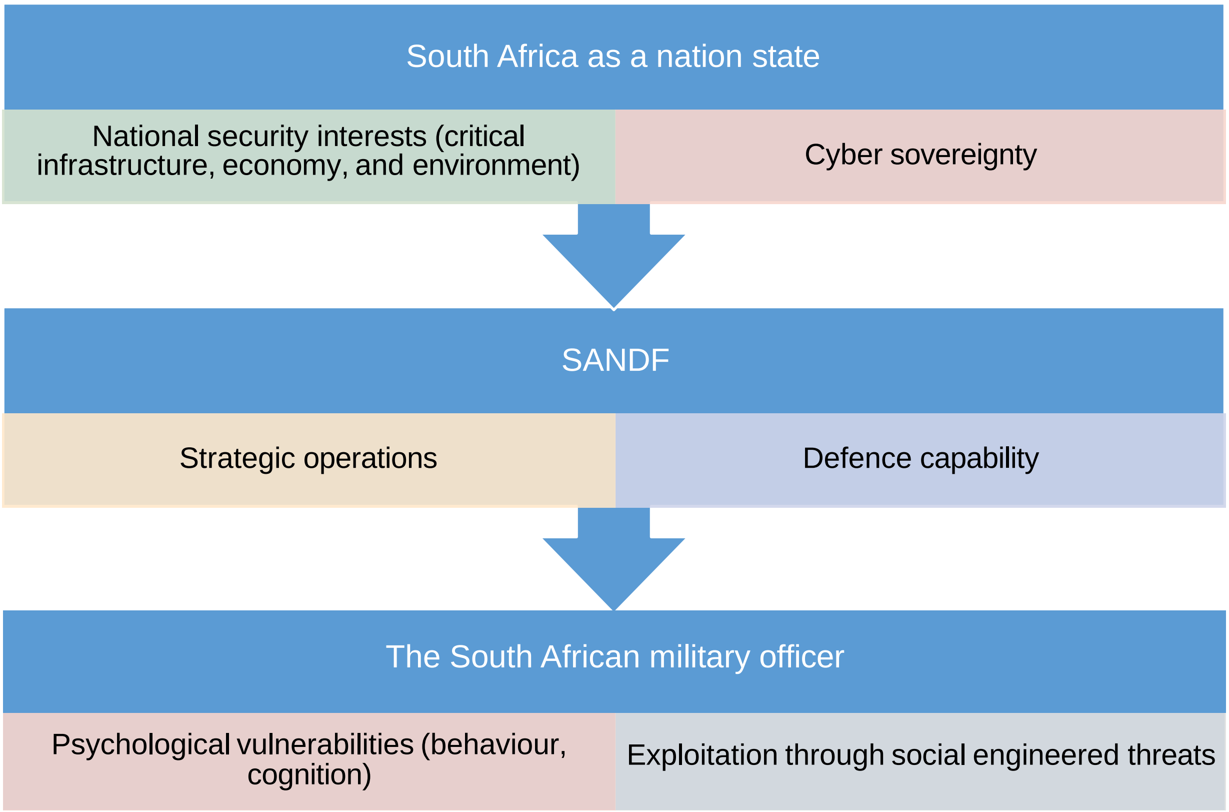

South Africa as a nation state
National security interests (critical infrastructure, economy, and environment)
Cyber sovereignty
SANDF
Strategic operations
Defence capability
The South African military officer
Psychological vulnerabilities (behaviour, cognition)
Exploitation through social engineered threats

Figure 3.2 indicates that ST is a process theory and does not only focus on the outcomes of the security process. It is worth noting that the ST process was mapped out earlier in the chapter (see Section 3.3). Figure 3.2 points out the context-applicable features related to the hierarchical process of the objects of reference. Floyd (2020) suggests that perceptions are of central relevance as they establish the legitimacy of securitisation, although very little is mentioned in the literature about those who execute the securitisation process. It is therefore important to explore the perceptions of the actors that must implement the securitisation process. The implementation of this process would follow after the process that elevated cyberthreats in the overall risk profile of the country and its institutions. Linking this proposed view of the object of reference, the researcher argues that there are three referent objects. The first is the state (which the SANDF needs to protect); the second is the SANDF, where a cyberthreat could potentially pose challenges related to intelligence gathering and maintaining national security; and the third proposed aspect is the military officer, which highlights human vulnerabilities by pointing out aspects of awareness and security behaviour.

The referent object in the case of cybersecurity would be the protection of information and the data of users. However, in some cases the relevant security nuances may indicate that the state is the referent object and that cyberattacks are the threat (Van Ooijen, 2020). Furthermore, the target population should generally be influenced in the aforementioned regard through the implementation of security mechanisms. It should also be noted that as the narrative is created and extraordinary measures are presented to the audience, the potential to divide the nation is an entirely possible phenomenon as some members of civil society may reject or accept the claim that a referent object is being protected. What this implies is that for security mechanisms to be successful, larger groups of society need to experience a sense of protection by the state so that the securitisation process can be considered a success (Balzacq, 2011). In addition, the process up to this point also denotes the importance of the narrative constructed and the acceptance of the existential threat, which may not be a given or obvious to all involved in the security process. Contrary to the aforementioned point, if the object of reference was considered generally good or unthreatened by current and future users of cyber, the narrative and acceptance of the threat might not be essential factors to consider. Furthermore, ST recognises that the state is of central importance, as it requires state-sanctioned decisions and resources to securitise an issue upon acceptance and adoption by the audience (Denning, 1999). The fundamental issue that actors may experience in the securitising process is the absence of absolute confirmation that the audience is receptive, as they only have the view of the decision-making body, where the majority of members would be in agreement with the rulings. Philipsen (2018) argues that new actors may challenge the prevailing conceptualisations and practices of security. Securitisation ultimately downplays the idea that the audience has the power to engage in decision making, while the securitising actor can promote certain agendas and exercise control over the resources that are employed, as well as over the construction of the narrative that the audience or civil society would receive and interpret (Bote, 2019). Moreover, the securitising actor does not have to be politically powerful or even part of this specific domain (Philipsen, 2018).

The researcher argues that the legitimacy of the extraordinary measures imposed depends on the resources available and sanctioned by the state. An example of this would be the securitisation process of cyber in the South African context.

Legitimacy can be established through the presence or the construction of a legitimate danger that is threatening the referent object. In addition, the narrative regarding the existential threat is equally important as it forms part of the securitisation process as this will eventually inform how the audience receives the security utterances regarding a perceived existential threat and why the referent object should be secured. Bote (2019) and Stępka (2022) argue that framing an issue as an existential threat may contribute to a measure of urgency in the responses, as opposed to the slow progress of normal politics. The section that follows discusses the technification of key players in the securitisation process.

3.8.1 Technification as a speech act in the securitisation process

Hansen and Nissenbaum (2009) confirm that technification is a specific type of speech act. Hansen (2011) believes that three types of logic should occur in the ST process for this to be successful and to link all the actors. These types of logic include hyper-securitisation, everyday security practices, and technification. Hyper-securitisation refers to how cybersecurity threats are narrated in assuming that dangerous future digital disasters will occur (Egloff & Cavelty, 2021). However, these hyper-securitisations assume the position that no previous historical events of the same status exist (Hansen & Nissenbaum, 2009). Everyday security practices refer to how securitising actors use specific security nuances to highlight a security threat by identifying the insecurity that civilians are experiencing (Egloff & Cavelty, 2021). The feeling of insecurity on the part of civilians is coupled to the cyber imaginaries / hyper-securitisations by the securitising actor in the cybersecurity sector (Hansen & Nissenbaum, 2009). Individual security practice is thereby cast as both a potential remedy of insecurity (i.e., individuals as “responsible” partners), as well as a driver of insecurity (Hansen & Nissenbaum, 2009). In addition, the practice of individual security is applicable when individuals engage in security practices that facilitate mitigating or accentuating the threat. Furthermore, technification constructs a security threat as something that is dependent on technical knowledge, which ultimately provides the political arena with a neutral agenda (Egloff & Cavelty, 2021). Technification in the ST process refers to influential advisers who may assist the securitising actor to frame a narrative that deals with the survival of the referent object. These advisers may also have specialised expertise, although they might have very little influence over the decision making and execution of security measures. The researcher only discusses the term “technification” as a logic in this section in the chapter as this relates to the context of this study and links to the component of ST that highlights the securitising actor and the construction of the threat information relayed to the audience.

Hansen and Nissenbaum (2009) submit the view that to protect cyber sovereignty, the political challenge should be resolved by introducing technical skills and knowledge (Hansen & Nissenbaum, 2009). According to Schwarz (2016), the technification of cybersecurity enables the process of political approval by the national or international audience. This is true because Buzan et al. (1998) suggest that a key figure linked to the state should announce the threat by identifying the potential impact it might have on the referent object.

Included in the securitisation process is allowing politicians to elevate the status of experts and giving them significant decision-making power (Schwarz, 2016).

Bourdieu (1994) notes that the core power of utterances rests in the hands of those who have been mandated to speak on behalf of a specific group. Dos Santos (2018) submits that the state does not act on its own accord, but instead allows a representative with the appropriate qualities to engage in security utterances. In analysing Dos Santos’ (2018) view, what emerges is that the dynamic of the state in utilising a representative to engage in security utterances refers to hegemonic structures that allow the elite, who have sufficient social capital, to influence the introduction and implementation of security measures. Buzan et al. (1998) emphasise that security measures (policies and actions) are first and foremost planned and implemented by the state. However, the argument can be made that the security measures being used as a response could have been informed by technical experts. Technification thus provides technical experts with epistemic authority to formulate and prioritise the dangers of cyberthreats (Egloff & Cavelty, 2021). Philipsen (2018) provides an alternative argument, namely that actors other than those who have political power are also able to enter the securitisation process by using new logics of security to obtain authority. Philipsen (2018) notes that new securitising actors may also offer an expanded view of security issues by focusing threat characterisation in contexts.

According to Schwarz (2016), critical infrastructure can be viewed as a referent object that needs to be protected; not only against threats stemming from the physical domain, but also those from cyberspace. The networks that are linked to critical infrastructure may also be targeted by malicious software. The narrative concerning protecting users' data and maintaining national cybersecurity, along with recent trends in the upsurge of cyberthreats nationally and globally, allows for influencing or recommending that the audience accepts the securitisation process (Schwarz, 2016). The technification of cyberspace and cybersecurity isolates those who do not have the required skills to execute the measures to facilitate the survival of the state or to ensure individual security (Schwarz, 2016). Nissenbaum (2005) highlights that the over-emphasis on cyber securitisation creates the idea that technical skills for dealing with and the discourse associated with cyberspace as a referent object require expertise. However, ST still rests largely in the political ambit but not exclusively so. Expert actors can therefore provide expertise and undertake consultations with high-ranking members of the state to inform security-related utterances. This can be observed in the South African context, where the National Cybersecurity Advisory Council was introduced to provide advice on security legislation and the technical issues related to cybersecurity (South African Government, 2013). Cybersecurity experts do not necessarily have the deciding power or authority to engage in speech acts or to facilitate the appropriate conditions in which security nuances align with the nature of the threat.

Furthermore, cyberspace can be considered a referent object characterised by technical elements that could be secured exclusively by those who have access to the technical expertise to inform others of related issues on the political agenda (Van Ooijen, 2020; Fouad, 2019). This nexus relies on technification, which ultimately causes the securitisation process to appear politically neutral since it is presented as an extension of technology and not really human agency (Schwarz, 2016). The notion of technification and the narrative relating to maintaining safety underline the process of allowing technical experts to inform the "elite", which contributes to subsequent utterances, but also affects whether effective measures are implemented in response to threats. It should be reiterated that those with less technical expertise will find it more difficult to contest the security issue and the proposed "beyond the normal" responses (Cavelty & Egloff, 2021). The technical expertise that informs the construction of threats and measures may nevertheless depoliticise elements of the securitisation process (Cavelty & Egloff, 2021). Cavelty and Egloff (2021) are in agreement with Philipsen (2018) in noting that those actors with authoritative power who speak on security can be more authoritative if they have more knowledge to speak as an authority on, for example, cybersecurity, as opposed to authority being a precondition for speaking, but with the actor having little knowledge of the topic. The researcher thus argues that the status quo of ST is increasingly challenged by those with superior or technical knowledge. It is important to conclude this section by highlighting that not all attempts at securitisation are bound to be a success, but the uncertainty of emerging threats with a possible existential impact necessitates knowledge and skills of securitisation to determine responses. The section that follows presents a critical review of ST.

3.9 Critique of ST

The CS has developed an innovative approach to explaining the concept of security (Nissenbaum, 2005). Despite the great value that the CS has contributed to the conceptualisation of certain phenomena through the study of securitisation, this school also encountered criticism for failing to highlight certain implications of the securitisation framework (Nissenbaum, 2005). Charrett (2009) contends that society has entered a phase in which security is a basis for obsession. McDonald (2008) contributes to the ongoing critique regarding ST by noting that it can be challenging in two ways: (1) security is constructed narrowly as the focus is on the speech of powerful stakeholders, which results in the exclusion of others, and (2) ST restricts the definition of the context of the act as the focus is only on the moment of intervention (McDonald, 2008; Buzan, 2006). McDonald (2008) suggests that security issues that are constructed over a long period of time may lose the meaning attached to them. When this transpires, the specific issue may inevitably be overlooked. Language is relevant as it conveys meaning that is important in the ambit of ST as the connotation attached to words is valuable for emphasising the importance of images and physical action (Charrett, 2009).

The location of the origin of ST, namely Europe, does not make adequate allowance for existential threats in an African context, nor has it opted to include an Afrocentric view, which may have assisted with developing a theoretical framework that would also be suitable for the African context (Ezeokafor & Kaunert, 2018; Stritzel, 2007; Huysmans, 2006; Williams, 2003). However, several researchers have studied ST outside the confines of the West. In addition, security as a socially constructed phenomenon is highly subjective (Romaniuk, 2018; Wæver, 1995). Nonetheless, Huysmans (2006) and Balzacq (2005) affirm that there are contrasting views in the conceptualisation of threats, which presents challenges for the process of securitisation. The abovementioned authors have contributed extensively to the review of securitisation in the 21st century and made contributions about its relevance relating to non-military issues, where issues relating to cybersecurity have now been acknowledged as emerging threats.

Acharya and Buzan (2017) acknowledge that ST originates from the Western world and neglects the magnitude of change in the social landscape, and fails to embrace histories and cultural contexts and to advocate important ideas that differ from Western theories. Acharya and Buzan (2017) advocate Westernised theories but question the rejection of non-Western norms and contributions by the established framework of securitisation. This implies that African nations, for example, are marginalised and therefore have to adapt their approach to the securitisation of, for example, cyberspace. Furthermore, African nations also need to adapt to local conditions and derive from ST what they can as the debate centres on the adaptation of ST versus accepting Westernised views. Acharya and Buzan (2017) also allude to the notion that non-Western contexts may contribute to the expansion of the theory; thus providing an opportunity to adjust how ST as relating to cybersecurity is carried out in the South African context.

The researcher argues that security as a concept is adaptive in the face of national security and in defence structures. Furthermore, the security measures that are introduced are usually a reaction to internal and external threats (Ahmad & Huvila, 2019; Al-Dawod & Stefanska, 2021; Uchendu et al., 2021). This reaction merits the constant adaptation to change and changing the perceptions of national security (Dearlove, 2010). Philipsen (2018) denotes that what is deduced from a performative view on ST is a framework that presents how iterations about the logic of security is readjusted. Viewing security as an iterative process allows for the perception of security to be analysed as it enters new disciplines. Moreover, Philipsen (2018) suggests that this movement across disciplines facilitates a change in the conceptual notion of security. It can be argued that a performative approach enables the analysis of securitisation to consider practices in the process that do not necessarily “succeed”. However, these practices still have the potential to have an influence on current security debates and practices (Philipsen, 2018). The researcher notes that considering multiple speech acts allows for the exploration of security as it emerges, instead of approaching it as being reliant on societal structures. In addition, it highlights the power practices embedded in speaking security and enables analysis of how some speech acts contain a certain subjectivity, while others contest them (Philipsen, 2018). This is also in line with Lucke's (2016) view of the facilitating conditions of the speech act, which sought to analyse the security grammar of the authority actor, and the position of the actor as relating to the security logic it applies to the securitisation process. In this way, ST provides meaningful insights into the security logic that is used in certain contexts. Philipsen (2018) argues that broadened and newer concepts of security present a challenge to the static nature of ST, by pointing to the iterations that are characteristic of any security expression. This iteration challenge attached to ST can be overcome by not viewing it as a blockage in the theory, but as a potential for change (Philipsen, 2018).

Cybersecurity is considered a hybrid form of security and does not form part of the first wave of philosophical and practical development of ST. Yet, the second generation of researchers using this theory is focusing on incorporating new and emerging threats to society. For example, when perusing the introduction of cyber securitisation, Hansen and Nissenbaum's (2009) work is evidence of an attempt to incorporate new threats into the security discourse (Bote, 2019; Fouad, 2019; Kapur & Mabon, 2018; Lacy & Prince, 2018; Van Ooijen, 2020). In addition, the securitisation narrative linked to cyber should be considered over a longer period for a more effective outcome (Van Ooijen, 2020). Hansen and Nissenbaum (2009) also argue that cyber defies the notion that the state and the military should be the central figures of power in the securitisation process. Van Ooijen (2020) argues that the discourse on cyber and the militarisation of cybersecurity should take place over an extended period of time, when repetitive patterns could emerge. This consideration confirms the idea that the securitisation of cybersecurity is not a straightforward, single-event process but takes place over time (Van Ooijen, 2020). Although many view cyber as a critical threat with serious implications for national security, the response and priority accorded to cybersecurity is a different matter. This can be observed in the initiatives relating to nation states' responses to ongoing cyberthreats (ITU, 2021). The researcher thus argues that context is an important element in how nation states arrive at securitisation and incorporate the military to mitigate risk and protect national security interests.

Cyber within ST is an upcoming concept and challenges existing ideas related to the construction of threats. According to Karpavičiūtė (2017), from the second wave it is clear that scholars may not want to engage with the argument that cyber is an existential threat given that it has existed for many years. This concept has also been named various terms, such as “transnational”, “asymmetrical”, or a “new form” of warfare. Including cybersecurity as a hybrid concept in the theoretical arguments of “threat identification” may facilitate understanding of the existential and non-existential elements of cyberthreats (Karpavičiūtė, 2017). One of the main developments in ST was its alignment with widening security to include sectors outside the state and the military (Buzan & Hansen, 2009). This consequently allowed for cyber to be considered as an emerging form of warfare. Hansen and Nissenbaum (2009) argue strongly that cyber should be included as a new sector in ST as it has the ability to produce disruptive consequences in society and therefore demands attention (Van Ooijen, 2020).

Cybersecurity may not necessarily be securitised rapidly, as the COVID-19 pandemic was, simply because the anticipated mortality level may not be clear. The argument can be made that cyber can be securitised by following a similar process as the one through which the COVID-19 pandemic was securitised – through multiple phases over time. However, Philipsen (2018) focuses on the aspect of response in the securitisation process by noting that not all threats necessitate agency in speech acts owing to differences in context and the political value attached to security issues. Aschmann et al. (2015) maintain that the cybersecurity of a nation is important for ensuring the protection of information and information-based processes of citizens, corporations, and the government and to guard the safety of a nation’s critical infrastructure. A nation must maintain its cyber sovereignty by protecting itself against cyber onslaughts by adversarial nations, as well as from cyberterrorism and cybercrime. The status quo for a nation is to maintain cyber peace, both internally and with its allies. The military has objectives to protect and defend against a cyberattack from an adversarial nation and to launch offensive cyberattacks in times of war. The major threats to economic vitality and national critical infrastructure in cyberspace now offer adversaries the potential to cripple the modern state over time while avoiding engagement in traditional kinetic war (Demchak, 2016). The next section focuses on how cyber is approached in the SANDF with reference to the components of ST.

3.10 Cyber in the SANDF

Cyberspace is an important channel for advancing diplomacy among nations, conducting intelligence operations that involve security agencies, and advancing the capabilities of the military as a force multiplier (Doyle, 2015; Painter, 2018). Furthermore, the promotion of threats beyond normal politics is undertaken by the state and its apparatus, which includes the military (Cavelty, 2013). One therefore cannot downplay the key role of the military in maintaining national cybersecurity[21] in the digital domain. This attribution has wide implications for the SANDF as the entity entrusted with maintaining national cybersecurity for South Africa. Nissenbaum (2005) suggests that the military is a referent object. Hirsch Ballin et al. (2020) note that the concept of security has extended beyond the military addressing external threats to a nation state[22]. While newer threats have emerged in various domains, the connection to cyberspace has become more apparent. Buzan et al. (1998) denote that several sectors are referent objects; one of which is the military domain, and that each of these sectors is pertinent for the survival of the state. However, the military itself is noted as an object that needs to survive and should be protected (Aydindag, 2021). While ST traditionally considers the military as a component in addressing the existential threat, the extension of security beyond issues impacting the state has removed the military from the apex as a response (Hirsch Ballin et al., 2020). The extension of the security agenda therefore allows other actors to enter the securitisation process. This extension may allow cybersecurity to be addressed as a key facet for achieving national security. However, Philipsen (2018) argues that not every iteration requires a change in approach to the conventional method of addressing security, which means that whereas newer threats such as cyber have emerged, it does not necessarily imply that how the military addresses the security issue should change from how it approached previous security threats. In addition, Philipsen (2018) argues that older forms of security practices might be used to address newer security iterations in the

[21] The NCPF (RSA, 2015b, p. 73) defines national cybersecurity as “a broad term encompassing the many aspects of electronic information, data and media services that affect a country's security, economy and wellbeing. Ensuring the security of a country's cyberspace therefore comprises a range of activities at different levels”.

[22] See Sections 3.4 and 3.5 for the expansion of security to include new threats beyond external threats that are geographically based.

securitisation process. When referring to how cybersecurity is elevated to the national security agenda, the researcher argues that the SANDF is but one referent object that needs to be protected so that the nation state's cybersecurity initiative may flourish and for its sovereignty to be protected. Hirsch Ballin et al. (2020) denote that cybersecurity must incorporate all objects of security, namely the state, the authority actors, and the individual. This implies that the object of reference is not just the state, which also extends the argument that threats from the cyber domain might be approached by various actors. This view furthermore opens up the notion that the referent object cannot be isolated to the SANDF, but should extend to including its military personnel.

In the South African context, the former Minister of Defence, in her Budget Vote Speech of 2017/2018, reiterated that the SANDF could not afford to relax its efforts to advance capacity in cybersecurity (RSA, 2017a). In addition, the manner in which the discourse related to cybersecurity is reiterated in the minister's other speeches indicates that cyberattacks are also future orientated. Stevens (2016) refers to cybersecurity utterances in pointing towards the notion of cybersecurity being imaginary. This denotes that cybersecurity is inherently progressive as resources are mobilised to respond to current and prospective threats. This cybersecurity imaginary is nested within social imaginary that ultimately influences how narratives regarding cyberthreats are uttered and responded to (Van Ooijen, 2020). Cyberthreats are thus viewed as a current and future threat that governments, and their military institutions, must contend with. In this regard, its iterations and repetition thereof also play a role in configuring and reconfiguring cybersecurity as a threat to infer meaning and flag cyberthreats as a new security act to challenge the status quo and how decision makers view security threats (Philipsen, 2018). South Africa relies extensively on imported technological tools for the protection of cyberspace. This is an indication that the tools, including hardware and software, may not necessarily be created within the borders of South Africa, which presents potential difficulties for maintaining national cybersecurity and establishing cyber sovereignty. Within the frame of the aforementioned argument, it must be emphasised that using social media platforms to communicate information without complying with organisational directives and policies may place both the organisation and the military officer at risk (Martin, 2020).

The SANDF has not yet devised the means necessary to construct secure platforms for rapid and dynamic communication by its members. This is known because the South African Defence Review (RSA, 2015a) does not refer to the development of in-house methods to engage with cybersecurity, apart from capacity building and strategic planning. The researcher is therefore of the view that in South Africa, the potential for the securitisation of cyber exists along with making a move to achieve the militarisation of cyberspace, which has not yet been fully realised. The researcher explains this statement by noting that the nature of cyberattacks and threats necessitates the state and military to take offensive and defensive action (Gomez, 2017). This action is part of the process of establishing national cyber strategies (Gomez, 2017). The researcher argues that in the case of South Africa, the militarisation of cyberspace has not yet been actualised, despite the cybersecurity discourse at the national level, which considers a cyberattack as falling in the same ambit as terrorism. Gomez (2017) suggests that, on the surface, cyberthreats have apparently not yet significantly crippled the infrastructure of the armed forces, which could explain why the militarisation of cyberspace is portrayed differently across military forces. This implies that the military is more reactionary than proactive in its stance towards cybersecurity (Felix, 2020).

The researcher argues that the “driver of insecurity” has relevance for the sample population of this study, namely military personnel. This manifestation of cyber responses across militaries could potentially be symptomatic of how security is perceived and approached in various nation states. The Minister of Defence and Military Veterans in South Africa has addressed parliamentary officials more than once about the dangers of cyberthreats and possible cost-effective ways in which the military could be an effective role player in South Africa’s cyber defence (RSA, 2018; 2020a). Romaniuk (2018) suggests that for the securitisation process to commence, first an existential threat, which in this case is a cyberthreat, should be motivated. The characteristics of the cyberthreat are communicated to a group of people in the state – people who have some form of political power (Romaniuk, 2018). Taking the former Minister of Defence’s speech on cyberthreats into account alongside the warnings of cyberattacks from experts, business, and academia, it could be emphasised that the speech was directed at parliamentary officials. These senior parliamentary officials have the power to make informed decisions about sanctioning emergency responses. While this key address to parliament could simply indicate the creation of a security narrative related to the armed forces and cyber, it nevertheless strengthens the argument that the range of “insecure” objects has broadened (Fouad, 2019). In ST, the change assessed is not a change in how security is characterised, but a change in which issues are categorised as security issues. Furthermore, it is an extensional change that focuses on how securitising actors expand the security logic to include new areas by moving certain issues from the political realm into the security realm. The broadening of insecure objects means that this category also includes the vulnerability of government, business, and electoral processes and individuals to cyberthreats (Fouad, 2019).

As mentioned in the section that focused on the technification of cybersecurity, technology represents a key component in the expression of power by the state as it promotes “information dominance, political dominance, economic dominance as well as military power” (Bote, 2019, p. 12). While Bote (2019) highlights the expression of power by the state, it is perhaps fundamental to highlight the element relating to power derived from words that conform to specific rules established by the government. In the South African context, the former Minister of Defence emphasised in her budget speech in parliament on 18 May 2018 that cyberthreats aimed at South Africa and the armed forces environment could be detrimental if the budget for cyber defence was not increased (Dentlinger, 2018). It is important to keep in mind that this is a security cluster with responsibility. It could thus assist if there is a standardised narrative that is corroborated by ministers in their political speeches. Furthermore, the Minister of Defence also emphasised in her budget speech that failure to allocate effective budgetary resources to advance the cybersecurity agenda in the organisation might cause a failure to implement the South African Defence Review of 2015 (Dentlinger, 2018; RSA, 2015a). This means that the appropriate dialogue should be employed to advance the topic of cybersecurity in the military context. The Minister of Defence thus emphasised (and did so more than once) a need to modernise the SANDF, yet very limited attention has since been paid to the military’s cyber defence capacity and capability. In addition, the minister’s speech focused on creating awareness of the fiscal challenges related to funding of the SANDF. Furthermore, the Chief Director of the Defence Intelligence Division in the DoD made a presentation to the National Assembly’s Defence Committee on the progress of the Cyber Warfare Policy Framework (PMG, 2020).

Several main points regarding SANDF vulnerabilities to cyberthreats were noted during this meeting:

- A cybersecurity strategy in the DoD is necessary for securing national security interests.
- The DoD has the overall responsibility for coordination of, accountability for, and implementation of cyber defence matters in South Africa.
- A focus on understanding the strategic nature of cyberattacks and threats and the various motives of nefarious actors is essential.
- The development of cybersecurity capacity is required to manage cyberattacks and threats from cyber mercenaries who pose a threat to military infrastructure. To corroborate this, the Chief Director referred to the case where an advertisement was posted on the Deep Web to recruit cyber mercenaries to extract critical information relating to some of the SANDF's top military secrets)[23].
- South Africa is grossly underequipped as the DoD and SANDF have only 100 trained cyber officials who are able to deal with cyberattacks and threats, and, even so, these cyber officials operating in the DoD have not yet been equipped with the skills to deal with higher-tier threats such as government sabotage and espionage.

Based on the aforementioned, it can be noted that dialogue concerning cybersecurity is on the agenda of South Africa's top ministerial and military officials. The dialogue clearly indicates that cybersecurity has risen to a position of prominence on South Africa's political and security agendas. President Ramaphosa, for example, along with senior government officials, voiced displeasure about recent reports that his mobile device was placed on a cyber target list by Rwanda in 2019 (McCain, 2021). The South African president's mobile device is also believed to be targeted by Israeli-developed spyware software named "Pegasus" (Du Plessis, 2021). Collectively, statements and events pushed cybersecurity up in the ranks of the South African national security agenda to a fixed topic of discussion at the political level. This progress implies that

[23] Hosken (2016) reported in 2016 that South Africa's top military secrets were stolen through hacking.

the repetition of the argument helps to focus political attention on a previously underplayed security threat.

The SANDF is still in the securitisation process as policy development takes time but must be implemented (Van Niekerk, 2017). This is echoed by the NCPF (RSA, 2015b), which acknowledges that there is an overlap between government departments whose policies do not comprehensively align to address cybersecurity threats with potential attacks. The nature of cyberthreats has been developing and is ever changing, which demands that the view of ST should be widened, especially since cyberthreats are wider than just the armed forces (Šulović, 2010). It should therefore be highlighted that the call for ST to include threats beyond the initial narrow, political-military confines must be noted and mobilised. From a South African perspective, elements of the ST process are visible in the aforementioned discussion, but it is clearly not complete and it should not to be seen as a given that it would be successfully completed. A major void exists owing to the lack of capacity, which is reinforced by the diffused nature of actor responses that are embedded in a myriad of government departments and agencies.

The South African state should strike a balance between constructing a regulatory framework that mitigates cyber risks owing to the advancement of ITs and avoiding infringement of “the fundamental rights of every South African citizen to privacy, security, dignity, access to information, the right to communication and freedom of expression”, as provided in section 3.1 of the NCPF (RSA, 2015b, p. 14). However, the SANDF has placed its understanding of cybersecurity in the realm of information warfare, which deals with the neutralisation of an enemy’s cyber capabilities (RSA, 2017b). In this case, the SANDF is also responsible for pushing the securitisation debate further down the line and using the advantages presented by the asymmetrical features of cyber to execute its mandate relating to national cybersecurity. The SANDF’s promotion of the securitisation of cyber also implies a strong element of militarisation by playing its allocated role nationally and in the military security context. The assumption can therefore be made that South African security actors are in the process of prioritising cyberthreats and elevating the risk profile thereof (Gomez, 2017; RSA, 2015b). The SANDF assumes the largest burden in managing cyberthreats and it is thus in its own interest to have the required political support for its mandate. This is corroborated when reviewing the role of the military as presented in the NCPF (RSA, 2015b). However, to date it only aligns with some aspects of ST as a process. Later thought on ST suggests that threats are able to move beyond powerful political decision makers that centre on the state being the referent object. Chapter 3 showed that cybersecurity can be securitised, and that South Africa in fact already went through some of the phases to arrive at rather extensive legislation, institutions, a military counter-apex, and for entities other than politicians to play a securitisation role. Securitisation thus serves to pitch cybersecurity as a dangerous threat.

3.11 Conclusion

This chapter discussed several key aspects related to ST. The chapter also discussed the emergence of new security threats in the 21st century and indicated that cyberspace is a threat that has emerged as a latecomer among an array of threats that have been afforded priority. A description of ST was provided, along with a brief indication of the actors and the relevant securitisation process. Thereafter, the chapter discussed the various interdisciplinary views on security. The chapter also offered a critical discussion of the rise in and utility of ST and pointed out key contributions in the various contexts to which this theory is applicable. In addition, the chapter elaborated on the intersection between ST and cybersecurity, which allowed for highlighting aspects relating to the actors and the role of power. The movement towards cyber becoming a securitised domain was also considered in the premise of cyber as a referent object. The chapter also offered a critical review of ST, by pointing out the pitfalls and potential aspects that might hinder development and thus its applicability and utility in newer contexts.

The last two sections of the chapter addressed how cybersecurity entered the SANDF and how cyber is approached within this military domain. The focus on these two sections identified that the SANDF is responsible for the overall coordination of cyber defence efforts to sustain national security (Malatji et al., 2021). Through the lens of ST, the South African situation does not fully comply with the tenets of ST, but speech acts, audiences, and reference groups are visible, although patchy. What is visible is that in the case of South Africa, ST in a non-Western context has some value for the country, the SANDF, and its journey to address cybersecurity as a national security interest. It is important to note that the theoretical aspects of ST, along with the literature (Chapter 2), acted as a guide to the creation of questions for both the interview guide and the COQ. This chapter allowed the researcher to show how ST contributes to this study. Furthermore, this chapter allowed the reader to understand why ST serves as a theoretical departure. The usefulness of this framework assisted the researcher with achieving the research aims and answering the research questions, which focus on the exploration of cybersecurity as a dangerous threat in the military context.

The chapter that follows elaborates on the methodology used in this study, and as such explains the research design, the sampling framework, and the data-collection phases.

CHAPTER 4:
RESEARCH METHODOLOGY

4.1 Introduction

This study focused on the exploration of factors relating to cybersecurity in the SANDF. The overall purpose of the study was to explore the perceptions and views of cybersecurity among officers serving in the SANDF. The previous chapter was dedicated to the role of ST in cyberspace and how this influences how threats are constructed. This chapter engages with the methodology selected for this study. This chapter contains discussions of the research design, sampling population, data-collection tools, and the research procedure followed for the study. In addition, the data-collection techniques and analysis used in the study are explained.

4.2 Research objectives

The rationale for this study was the significant gap that exists with regard to the production of knowledge concerning the perceptions of cybersecurity among South African military officers (Gcaza & Von Solms, 2017; Van't Wout, 2019; Van der Waag-Cowling, 2017, 2013). The overarching aim of this study was to provide an exploration of the perceptions that govern the views of the military officer regarding cybersecurity in the SANDF. The study explored how military officers conceptualised cybersecurity by specifically gauging their awareness and how cybersecurity threats were perceived in the context of the SANDF.

The objectives of the study are captured in three specific research questions, which are as follows:

- How do South African military officers conceptualise cybersecurity awareness?
- How do South African military officers perceive cybersecurity threats within the SANDF?
- What are the perceptions of cybersecurity awareness through the lens of the military officer?

4.2.1 How do South African military officers conceptualise cybersecurity awareness?

The information derived from the responses provided the study with the context relating to the impact of awareness initiatives, past experiences, and online education in shaping capacity for awareness among officers in the South African military environment.

4.2.2 How do South African military officers perceive cybersecurity threats within the SANDF?

The construction of cyberthreats remains of key importance to the awareness of military personnel. It was essential to explore how these threats are constructed at the individual level to establish the context in which these perceptions emerge.

4.2.3 What are the perceptions of cybersecurity awareness through the lens of the military officer?

Viewing the perceptions of cybersecurity through the lens of the South African military officer provided a contextual basis for how cyber is approached in an organisational setting. The exploration of these lenses allowed for a deeper view on how broader contextual issues might have an impact on how cybersecurity awareness practices are carried out by military officers.

4.3 Research paradigm

Social scientists' research-related work has specific existing philosophical underpinnings and these sources often contain one or more paradigms (Kaushik & Walsh, 2019). The use of multiple paradigms is generally determined by the nature and objectives of a study. Babbie (2010) suggests that neither the positivist nor interpretivist paradigm is considered better than the other. The onus rests on the social scientist or researcher to employ the research paradigm that is deemed appropriate for answering the research question(s) (Babbie, 2010). This view feeds into the aim of this study, which is to explore the perceptions of cybersecurity among South African military officers, as the mixing of paradigms answers the research questions stated in Chapter 1 (see Section 1.10). The understanding that positivism as a paradigm is fuelled by hard scientific facts characterised by statistical equations and quantitative philosophies of generalisability does not by any means imply that the interpretivist paradigm is less adequate. Merriam (1985) substantiates this claim by suggesting that research in general should focus on aspects of credibility and whether the research is confirmable.

This study used a mixed-methods approach that was divided into two research phases. The qualitative approach was the primary method in Phase 1 of this study. The primary method of selection was key in obtaining a view on the participant narrative regarding aspects such as information sharing in the organisation, their view on cybersecurity, and how they orientate themselves in cyberspace. Furthermore, this qualitative phase (Phase 1) was of key importance as it informed the item development that took place in Phase 2 of the study. The quantitative approach in Phase 2 involved a self-completion questionnaire. Consequently, the researcher adopted a varied approach by employing more than one paradigm[24] to explore the phenomenon in the participants' natural setting (Merriam, 1985). Paradigm mixing may also assist in understanding the sequential design, which is discussed in the next section.

Interpretivism as a paradigm is more suitable for qualitative research. However, considering interpretivism implies that the researcher was interested in obtaining a deeper understanding of a particular phenomenon. The interpretivist paradigm also allowed the researcher to extract the values and perceptions that are connected to a participant's worldview (Alharahsheh & Pius, 2020). Interpretivism therefore informed Phase 1 of the study. The positivist paradigm aligns itself with the quantitative approach because it is more suitable for quantitative research methodologies. The positivist paradigm refers to those events that can be observed and measured objectively (Vermooten, 2018). This statement confirms that researchers do not interfere with the phenomena that are present in the social reality of the participants in a study. The selected paradigm links with Phase 2 of the study, which involved the development and administering of a questionnaire (see Appendix E for the COQ).

[24] See Section 1.11 on the research design used, where emphasis was placed on the paradigm approaches of interpretivism and positivism.

4.4 Research design

Gray (2009) defines a research design as the general plan for the collection, measurement, and analysis of data. Cohen et al. (2011) define a research design as the strategic, tactical, and practical factors relating to research. Creswell (2014) notes that a research design is a plan that links the research problem to attainable empirical research. The research design thus directed how the researcher set up, constructed, and executed the collection, measurement, and analysis of data during Phases 1 and 2 of the study specifically to address the secondary research questions.

This study utilised an exploratory sequential mixed-methods design, which can be described as a systematic research procedure that is characterised by the collection and analysis of data by combining quantitative and qualitative approaches during the research process. According to Creswell (2007; 2009), this specific research design can be used to provide views on the topic. According to Greene et al. (1989), along with Tashakkori and Teddlie (1998), these opposing paradigms can be used to supplement each other and allow a more detailed, richer analysis. Since a mixed-methods approach employs both quantitative and qualitative methods, it is important to illustrate the differences between these two methodologies, as indicated in Table 4.1.

Table 4.1: The differences between quantitative and qualitative research

Research design	Qualitative research	Quantitative research
Scientific method	The qualitative research method is concerned with the interpretative social science paradigm. Qualitative research provides deep and contextual meaning of participants' views (Babbie & Mouton, 2007). Qualitative researchers are subjectivist in their research approach (Creswell, 2009).	The quantitative research design is based on logical positivism (Babbie & Mouton, 2007). Quantitative researchers are positivist in their approach to research (Creswell, 2009).
Types of data collection	Qualitative research uses direct and non-direct observation techniques. Examples of data-collection techniques include interviews and documentary research (Creswell, 2007).	Quantitative research includes the measurement of data through scale items. Data-collection instruments are utilised and validated through external criteria (Creswell, 2007; Messick, 1995). The data-collection instruments are psychometric instruments and surveys.
Data-analysis techniques	Qualitative data analysis seeks to uncover themes and patterns within the participant-derived information	Data-analysis techniques are based on connections between variables (Janse van Rensburg, 2019). Furthermore, the

Research design	Qualitative research	Quantitative research
	and by focusing on the contextual view of participants (Janse van Rensburg, 2019). Furthermore, data are analysed with the qualitative researcher taking a reflexive and subjective approach (Lichtman, 2014).	overall purpose of conducting quantitative analysis is to test a theory instead of engaging in theory development (Babbie & Mouton, 2007).
Reporting findings	The researcher reports the findings extracted from the views of the participants and relies on the interpretation of narratives (Creswell, 2009).	A statistical manner of reporting the data can be followed when deductions are made from objective points of view.

Sutton and Austin (2015) state that a qualitative approach aims to interpret, decode, translate, and make meaning of certain phenomena. A qualitative research method is an approach that attempts to understand social reality and must be grounded in individuals' lived experiences and understanding of their social reality (Gray, 2009). Fraenkel and Wallen (1996) state that the qualitative approach is a method that attempts to understand and interpret what exists at present in the form of conditions, practices, processes, trends, effects, attitudes, and beliefs as the actors perceive them. This was important for the questionnaire employed during Phase 2 of this research and the responses received from the interviews conducted. In contrast, a quantitative paradigm does not readily allow for rich and open-ended discussions that enable elaborating on, for example, military officers' individual perceptions of cybersecurity (Creswell, 2009, 2007; Kvale, 1996; Moustakas, 1994). From a methodological point of view, the integration of findings allows for the topic under exploration to be engaged comprehensively instead of isolating findings to fit one data-collection approach. Furthermore, a mixed-methods approach assists in triangulating the findings from multiple perspectives. The exploratory sequential mixed-methods design involved the researcher following a certain sequence in the data collection. This allowed each method to inform the subsequent method (Berman, 2017). The exploratory sequential design can be categorised into two phases as the qualitative phase of data collection and analysis is usually considered the primary driving force. This qualitative phase must consequently be followed by a second phase, namely the quantitative phase of data collection and analysis (Berman, 2017; Teddlie & Tashakkori, 2008). These methods, however, only aimed to explore the construct of cybersecurity while also envisaging to achieve triangulation of the results. It should nevertheless be noted that in this study, the first method, which is qualitative, was the main method and therefore predominantly informed the findings of the study. The subsequent method, which was quantitative, was followed to complement the qualitative findings. According to Creswell and Plano Clark (2011), the development of a quantitative instrument or survey is largely dependent on the themes extracted from the qualitative data. The final phase in this exploratory sequential approach was to embark on a phase of integration, whereby the core responsibility rested with the researcher to integrate and connect the data derived from the two separate phases.

Interviews and questionnaires are used in mixed-methods studies to confirm findings irrespective of the different data-collection, data-analysis, and interpretative approaches that are followed (Harris & Brown, 2010). Harris and Brown (2010) posit that when engaging with studies that employ different methods, the variables selected and the construct being studied remain important to ensure alignment. In addition, Harris and Brown (2010) recommend that the researcher should make an effort to align the interview and the questionnaire by utilising questions that are similar in both data-collection techniques. Harris and Brown (2010) believe that this may ensure a high rate of consistency among the participants.

The integration of findings also answers the researcher's "why" question, which speaks to the notion that to explore the perceptions of cybersecurity among military officers, it is necessary to provide a comprehensive view in terms of why military officers perceive cybersecurity threats a certain way, as well as how this may inform security behaviour. The "what" in terms of a methodological point of view is best addressed when referring to Research Question (RQ) 3, which asked: What are the perceptions of cybersecurity awareness through the lens of the military officer? The researcher argues that Phase 1 (interviews) is a suitable approach to answer the research question as it adds to the foundation of understanding the participants' level of awareness. Addressing the "how" question in the study, the researcher emphasises RQ1 and RQ2, which primarily sought to explore the conceptualisation of cybersecurity awareness and the perception of security threats in cyberspace.

The researcher argues that in order to answer these questions, the discourse regarding cybersecurity awareness first needed to be established through the semi-structured interviews offered in Phase 1. Thereafter, the dimensions of the COQ offered in Phase 2 needed to supplement the findings that speak to the thematic components of Phase 1. The "how" aspect of the research questions also speaks to the exploratory nature of the study, which seeks to engage in a topic that is not well established, but rather emerging in South Africa and particularly in the military. The questions constructed for the study were therefore aligned with the purpose of an exploratory sequential design. The next section focuses on the sample selection and criteria used to recruit participants from the SANDC, SANWC, and SAMA.

4.5 Sample selection and criteria

Internet users can be grouped into two categories, namely home users and non-home users. Non-home users are believed to be those individuals who have access to the Internet in their work environment and are generally from the industry or government (Kritzinger & Von Solms, 2010). Non-home users are expected to have some experience and awareness of the potential dangers that are lurking in cyberspace (Kritzinger & Von Solms, 2010). The awareness of cyberthreats is important for South African military officers due to the threat rate increasing where government and private entities are placed at risk (Pieterse, 2021). In addition, users' cybersecurity awareness also accompanies the element of exercising security behaviour. The military officer thus becomes an important human entity in establishing cybersecurity. This study was interested in the perceptions of cybersecurity among South African military officers and it was therefore important to demarcate the concept of "users" in this study's population. The inclusion criteria for participants of this study were as follows:

- Permanent uniformed member of the SANDF;
- Student at either SAMA, the SANWC, or SANDC; and
- Uniformed member who is an officer in the SANDF.

The exclusion criteria for participants of this study were the following:

- Foreign students at any of the identified military institutions; and
- Civilians (this may also include civilians who are employed at the DoD).

With regard to the participants, the sampling for this study was divided according to the two research phases relevant to this study. This section includes a description of users as they relate to each phase of the study. A summary of the two phases and the sampling method used for each of them are indicated in Table 4.2.

Table 4.2: Summary of methodological aspects of Phases 1 and 2

Research design phase	Sample size	Sample design	Method of data collection	Method of data analysis
Qualitative phase (Phase 1)	SANDC = 10	Purposive sampling	Face-to-face, semi-structured interviews	CA
Quantitative phase (Phase 2.1)	SAMA = 113	Cluster sampling	Self-administered questionnaire	Descriptive statistics and thematic analysis
Quantitative phase (Phase 2.2)	SANWC = 70	Cluster sampling	Self-administered questionnaire	Descriptive statistics and thematic analysis

4.5.1 Phase 1: Semi-structured interviews

The sampling method used for Phase 1 was purposive sampling. This specific method can be described as a sampling technique whereby all members of the population have an equal chance of being selected to participate in a study (Ames et al., 2019). This method of sampling and recruiting is homogenous purposive sampling as the researcher actively recruited participants from a select group who all complied with a set of predetermined characteristics (Palinkas et al., 2015). These homogenous characteristics were participants serving in the SANDF and being of senior officer rank. In addition, the participants were also required to be enrolled for a military training course for senior officers at the SANDC.

The sample group that was selected to participate in Phase 1 comprised senior-ranking South African military officers enrolled for a developmental course at the SANDC in 2019. The military officers involved in Phase 1 were regarded as both home and non-home users of the Internet. This implies that the military officers utilised the Internet in their professional and private capacity.

4.5.2 Phase 2: The Cybersecurity Orientation Questionnaire (COQ)

Cluster sampling was used as the sampling technique followed for Phase 2. Cluster sampling was ideal for this phase as the participants were geographically located in different regions. Alvi (2016) denotes that populations of interest are generally divided into smaller sub-groups, which are known as clusters. Dividing the population into smaller groups generally assumes that they are geographically located differently (Alvi, 2016).

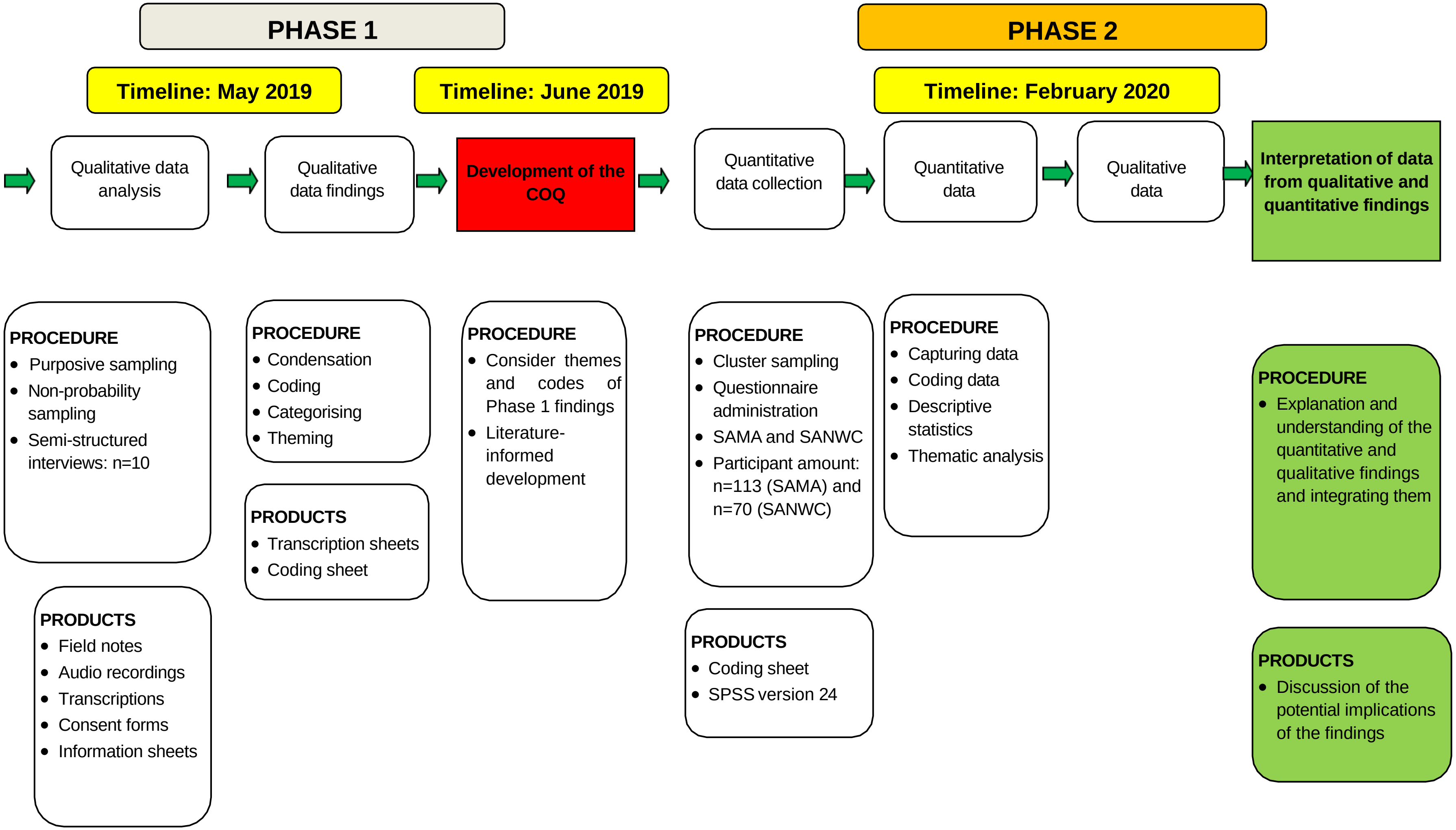
The participants for Phase 2 were selected from two military institutions, namely SAMA and the SANWC. SAMA is located in the Western Cape province and has residential students (junior officers from all arms of service), while SAMA's distance-learning students are located across the different provinces of South Africa. SAMA largely presents undergraduate education programmes. The sample size of the participants recruited at SAMA was 113, which comprised both residential and distance-learning students.

The SANWC is located in the Gauteng province and has only residential students, who comprise senior officers from all arms of service. The SANWC presents training and education programmes to selected officers to qualify them at command and staff level. The sample size of the SANWC participants was 70.

4.6 Data-collection procedure

Figure 4.1 shows how the researcher used a sequential approach in both data-collection phases of the study. Phase 1 was qualitative and involved semi-structured interviews that took place at the SANDC. Phase 2 was quantitative and involved questionnaires that were completed at both SAMA and the SANWC. Before the research for Phases 1 and 2 could commence, permission had to be obtained from the commandants of the SANDC, SANWC, and SAMA, which was granted. In addition, the Ethics Committee of Stellenbosch University (SU), along with Institutional Governance at SU, after reviewing the application, formally approved the researcher's request to commence with the research study and data collection.

Figure 4.1: Research process for Phases 1 and 2



PHASE 1

Timeline: May 2019

Timeline: June 2019

Qualitative data analysis

Qualitative data findings

Development of the COQ

PROCEDURE
- Purposive sampling
- Non-probability sampling
- Semi-structured interviews: n=10

PRODUCTS
- Field notes
- Audio recordings
- Transcriptions
- Consent forms
- Information sheets

PROCEDURE
- Condensation
- Coding
- Categorising
- Theming

PRODUCTS
- Transcription sheets
- Coding sheet

PROCEDURE
- Consider themes and codes of Phase 1 findings
- Literature-informed development

PHASE 2

Timeline: February 2020

Quantitative data collection

Quantitative data

Qualitative data

Interpretation of data from qualitative and quantitative findings

PROCEDURE
- Cluster sampling
- Questionnaire administration
- SAMA and SANWC
- Participant amount: n=113 (SAMA) and n=70 (SANWC)

PRODUCTS
- Coding sheet
- SPSS version 24

PROCEDURE
- Capturing data
- Coding data
- Descriptive statistics
- Thematic analysis

PROCEDURE
- Explanation and understanding of the quantitative and qualitative findings and integrating them

PRODUCTS
- Discussion of the potential implications of the findings

4.6.1 Phase 1: Semi-structured interviews

Once the SANDC had granted permission for the research to be conducted, the researcher presented an information session at the SANDC detailing the purpose and nature of the study by using Microsoft PowerPoint slides. All the students present at the information session, which took place in a lecture hall, received information sheets (see Appendix A) that contained detailed information about the nature, purpose, and objectives of the study. All the information that was relevant to the study was included in the information sheet, such as the contact information of the researcher and the Research Ethics Committee of SU. In addition, a terminology list, which the researcher had developed, was handed to the students, mainly to enable them to familiarise themselves with some of the terms and concepts that might be considered as technical (see Appendix R). Subsequent to the information session, the researcher collected the contact details of the students who had indicated their willingness to participate. The researcher contacted these participants afterwards to establish and agree on an interview time and location that would accommodate their academic schedule (Creswell, 2005).

All interviews were arranged in May 2019 by using a schedule planner. The researcher scheduled interviews outside the students' class time at the SANDC. According to McGrath et al. (2019) and Groenewald (2004), research that focuses on the content and the narrative approach can be regarded as effective when the interviews take place in the participant's natural setting, where the phenomenon is taking place. As a result, the researcher ensured that the interviews took place in a quiet venue located on the grounds of the SANDC, which was appropriate for and conducive to conducting, as well as audio-recording, the interviews as distractions such as background noise were minimal (Creswell, 2005). The interviews were furthermore held on the grounds of the institution for the convenience of the students. Additional information sheets (see Appendix A) were provided to participants on the day of the interview in the event that they had lost the contact details of the researcher and the information pertaining to the study. The participants received a consent form before the interview commenced, in which the researcher reiterated what was expected of the participants, as well as the purpose of the study. Furthermore, the researcher explained to the participants what each section of the interview guide entailed and emphasised their right, as participants, to withdraw from the study at any stage during the interview without incurring any form of penalty. All the participants completed the consent forms before the interviews commenced, in compliance with ethical requirements. The topic under exploration was of a complex and sensitive nature to the organisation; it was therefore crucial to build rapport with the participants, which the researcher did by being polite and treating them with respect. The interview guide functioned as a semi-structured guide (see Appendix D). The researcher also used an audio-recording device, with the permission of the participants, which was essential in the interview and research process, given the necessity to obtain rich and detailed information. The information obtained from the semi-structured interviews was consequently transcribed verbatim, after which it was analysed using qualitative CA.

4.6.2 Phase 2: The COQ

The second phase of the study focused on obtaining quantitative data from the SAMA and SANWC participants. The researcher enquired at SAMA about a suitable time to administer the questionnaire to the participants, particularly when the distance-learning students would also be at SAMA. The researcher arranged for an information session with SAMA's Mess Coordinator to determine a suitable date when the researcher could make a presentation about the nature and purpose of the study to prospective participants. On the day of the information session, at a joint meeting, interested participants received an information sheet indicating the nature and purpose of the study (see Appendix A) and a consent form (see Appendix C) to complete. Owing to the researcher being located in a different province and unable to travel to another province at the date SAMA preferred, arrangements were made with two research assistants from SU, who collected the completed questionnaires. The researcher conducted a formal training session with the research assistants beforehand to ensure that the data collection would be done correctly and that the research assistants were confident in administering the questionnaire to the students. The research assistants also signed a non-disclosure agreement as participant information was regarded as of an especially sensitive nature. All the participants were informed by the information sheet that the research assistants would administer the questionnaire. Since participation in the study was voluntary, only those students who were willing to participate in the study completed an informed consent form and thereafter completed the questionnaire under the supervision of the research assistants. The researcher collected the consent forms and questionnaires from the research assistants and stored them in a safe location.

4.7 Data-collection tools

4.7.1 Phase 1: Semi-structured interviews

Individual interviews were deemed the most appropriate tool to collect data in this phase as cybersecurity is of a sensitive nature and individuals might therefore have been more inclined to share a greater deal of information in a one-on-one interview situation. The researcher was confident that refraining from conducting focus groups would not adversely influence this study and that conducting in-depth semi-structured interviews was the best course of action considering the richness of information that could possibly be elicited.

In-depth semi-structured interviews were conducted by questioning key individuals from a unique population. In-depth semi-structured interviews can be regarded as the primary method for collecting information for this research study. The interview guide was semi-structured as it was composed of a set of predetermined questions about the socio-political implications of cybersecurity. In addition, the use of a semi-structured interview guide ensured that the researcher's freedom to deviate from the predetermined questions was limited, but nevertheless afforded him the opportunity to probe to derive additional information (Dearnley, 2005). The researcher had formulated questions that would clear up any confusion and used them as a means to probe for more information regarding the participants' opinions for the sake of achieving further clarity, and as a means of assessing whether the researcher had arrived at the correct understanding (Mack et al., 2005; Moustakas, 1994) (see Appendix D).

The semi-structured questions in the guide were developed based on this study's aims but were also informed by the literature and other studies that had been conducted in the same field. The interview guide was structured into four sections, namely information-sharing culture, security orientation, views on cybersecurity, and cybersecurity posture in the organisation. Each section of the interview guide was constructed in line with research related to cybersecurity drawn from Elvin and

Johansson (2017), Hadlington (2017), Kritzinger and Von Solms (2010), and Karaman et al. (2016). In addition, the researcher designed the questions to explore the prevailing perceptions of cybersecurity. The questions were developed in such a way that they could accompany the theoretical underpinnings of ST, which refers to the concept of how dangerous and important military personnel regard threats in cyberspace. The semi-structured interview took between 25 and 45 minutes to complete.

4.7.2 Phase 2: The COQ

Phase 2 involved the use of a questionnaire, namely the COQ (version 1.0). Since this study opted to follow a sequential approach, the findings of Phase 1 fed into the construction of some questionnaire items in Phase 2. The main findings of Phase 1 (semi-structured interviews) highlighted four main themes. The first theme focused on *knowledge production and cybersecurity awareness training*. The second theme focused on *challenges related to trust and technology and members of the military*. The third theme focused on *the construction of a digital culture among members*, and the fourth theme focused on the notion of how *the view on cyberthreats is constructed based on experiences in the physical domain*.

Apart from using these four main themes, information derived from the literature by researchers such as Soeters and Goldenberg (2019) and Atkinson et al. (2009) contributed to the development and construction of some questionnaire items. As a result, the COQ captured participant views on information sharing, security orientation, cybersecurity awareness, and cyber culture. These four domains were utilised as sections in the COQ as they represented unique elements that linked with cybersecurity in the social sciences domain. These four domains allowed cybersecurity to be studied in an interdisciplinary manner that went beyond the convention of exploring cybersecurity through a technical lens. Generally, the implications of cyberthreats and attacks have offline implications for the greater number of people in society who are connected to the Internet in some way or other. Keeping this in mind, the COQ was designed to incorporate elements that could be linked to cybersecurity from an interdisciplinary perspective.

The COQ (see Appendix E) is an individual, self-completion questionnaire with the purpose of eliciting cybersecurity behaviours from the participants. The structure of the COQ entailed the following:

- An instruction section to ensure that the participants understood how to answer the questionnaire;
- A biographical section to capture the demographics of the participants;
- Section 1, titled "Information-sharing culture", consisted of 13 statements with a four-point Likert scale of agreement and four short questions;
- Section 2, titled "Security orientation", consisted of eight statements with a four-point Likert scale of agreement and three short questions;
- Section 3, titled "Views on cybersecurity", consisted of 16 statements with a four-point Likert scale of agreement; and
- Section 4, titled "Cybersecurity posture in the organisation", consisted of seven statements with a four-point Likert scale of agreement and two short questions.

Although the COQ has a predominantly military focus, some questions are applicable across different kinds of organisations. The age range of the participants in the COQ was between 18 and 50 years. The COQ took a maximum of 35 minutes to complete.

The nine short questions in the COQ were added to allow the researcher to gain a sense of the respondents' opinions as these short questions asked the participants to provide a short description of their views of information sharing, online behaviour, and how cybersecurity was managed in the workplace. It is important to note that the COQ explores the element of awareness and not the aspect of how knowledgeable respondents are about the practices associated with maintaining cybersecurity. The COQ used only nine short questions to ensure that the respondents did not suffer from "survey fatigue", which usually results in overexposure to items and may reduce the number of responses (MacArthur & Conlon, 2012).

4.7.3 Phase 1 informing the development of COQ items

Phase 1 of the study informed Phase 2, which focused on the construction of the COQ. The codes presented in Section 4.8.1.3 show that using CA yielded a variety of aspects that informed the meaning units and themes in Phase 1 (see Appendix L). Furthermore, the researcher connected codes that focused on awareness initiatives and training to Theme 1: *Knowledge production and training focusing on cybersecurity awareness* (see Appendix S). Based on the information supplied through the codes and analysis of themes, the researcher was able to construct scale items for Dimension 4 of the COQ, which focused on the cybersecurity posture in the organisation. In addition, codes related to trust and vigilance were connected to Theme 2, which focused on *challenges of trust with technology and members.* Once connected, the researcher constructed questions geared towards the view on security challenges in the workplace; the researcher grouped these items under Dimension 3, which was named "The officers' view of cybersecurity". The third aspect to the development of scale items rested with the codes in Phase 1 that focused on the element of digital communication and information security aspects. The third component of the development of the COQ considered the findings of Theme 3: *The construction of a digital culture among members*, which focused on personal device use and a culture of digital security in the organisation. The researcher dubbed the next group of items "Dimension 1", which focused on the information-sharing culture in the organisation. The scale items in Dimension 1 were created to explore the communication strategies in the organisation and how comfortable the participants were to engage in the available methods of sharing information. Furthermore, the final element of the COQ focused on the creation of Dimension 2, which focused on the military officers' security orientation. This dimension was informed by the codes centred on vigilance, prior knowledge on cyber threats, and the notion of digital versus personal security. Moreover, Theme 4, *The view on cyberthreats is constructed based on experiences in the physical domain*, was used to engage in the development of the scale items in Dimension 2. The scale items in Dimension 2 explored the balance between how security is practised in a personal space and how it is applied in an organisational context where the element of security is an organisational demand.

4.7.4 How the elements of ST informed Phases 1 and 2 of the study

This section briefly informs the reader how the elements of ST informed the methodology of this study, particularly by considering the selected design of the study, as well as the sample population. Cybersecurity is not generally associated with ST for reasons outlined earlier, nor is the idea that methodology is associated with factors of the framework that includes elements of the securitisation speech act, securitising actor, and referent object. However, the researcher needed to incorporate elements of the theory in order to address the key questions in the interview guide and the COQ (see Appendix T).

The researcher positioned this study within the later thought on ST, which focused on more flexibility in extending the elements of the theory by including previously excluded or marginalised actors in the security process. The researcher considered military officers as a sample group for three reasons: (1) the military practitioner is an understudied sample group and needs to be explored in the context of cybersecurity awareness, (2) the traditional notion of ST infuses rigidity in the theoretical process and the military is used as a basis for response by the state, but often with little input in the process, and (3) the military officer is both a potential contributing member according to later thought that directed the theory and an actor that does and speaks security.

The speech act in ST refers to the notion that language and grammar are used to convey an issue, which in this case is about the dangers of cyberthreats. As a result, the questions in the interview guide and the COQ were framed around whether the organisation is doing enough regarding identifying and countering cyberthreats. Furthermore, the questions in the interview guide also focused on whether the participants felt that if the organisation were to advance cybersecurity awareness and training, whether they would allocate more attention to cyber.

In terms of the referent object, the questions in the interview guide and the COQ were framed to engage the participants in the conceptualisation of cyber as a threat. This allowed the researcher to gauge how the participants behaved in securing their own data, as well as the data of the organisation. In addition, the researcher considered the military officer as a potential securitising actor as he or she needs to, and does, speak security to align with the view of Philipsen (2018) that speaking security is also to do security. Herein lies how ST also assisted to inform the construction of items in the interview guide and the COQ. As in the South African case, the process of securitisation is the pathway for how the SANDF as the country’s military defence establishment became endowed with national cybersecurity responsibilities. The securitisation process also informs what the SANDF must take care of and these connections became elements of information to also include in the COQ.

ST had a role to play in the methodology of the study, especially in the construction of questions and scale items for the COQ. These items were pertinent for the exploration of cybersecurity in the armed forces context in South Africa.

4.7.5 Reliability of the COQ

This section presents the reliability of the COQ, although the reliability of the COQ was not the aim of the study. However, the internal consistency of the COQ scale items needs to be presented to capture whether the constructs sufficiently measured the cybersecurity constructs.

Table 4.3: Reliability of the COQ for the South African Military Academy (SAMA) and South African National War College (SANWC)

Items	Cronbach's alpha	Total items	Mean	N
COQ items for SAMA	.803	44	123.67	93
COQ items for SANWC	.752	44	124.49	57

The Cronbach's alpha of .803 for the SAMA sample suggests that these items are sufficiently reliable to measure the construct of cybersecurity (Nunnally & Bernstein, 1994). The Cronbach's alpha of .752 for the SANWC sample suggests that the items were sufficiently reliable for research purposes (Nunnally & Bernstein, 1994). It should be noted that listwise deletion occurred when the Cronbach's alpha was generated, which resulted in a reduction of the sample due to missing values. The reliability of the COQ for these two samples indicates that the internal consistency of the COQ is acceptable. This study did not make use of hypotheses as it was an exploratory study and did not require the use of, support, or rejection of hypotheses through the instruments constructed and used (Arendse & Maree, 2019).

4.8 Data analysis

4.8.1 Phase 1 data analysis: Content analysis (CA)

The researcher selected qualitative CA as the data-analysis technique for Phase 1. CA can be described as an analytical technique through which the social researcher examines the participants' views of the world by highlighting the deeper meaning of the content that is produced during the analysis of text and speech. A multitude of definitions are associated with CA. According to Berelson (1952), CA can be described as a research method for the objective, systematic, and quantitative description of the presented content of any communication. On the other hand, Holsti (1968) posits that CA can be described as a technique for making inferences by systematically and objectively identifying some specified characteristics of information. Krippendorff (2004, p. 18) notes that CA can be defined as "a research technique for making replicable and valid inferences from texts to the contexts of their use". Mayring (2002, p. 2) suggests that CA can be viewed as "an approach of empirical, methodological, controlled analysis of texts within their context of communication, following content analytic rules and systematic models, without rash quantification". The researcher notes that there are some common elements in each view of CA. The commonality lies in the notion that text and communication can be interpreted by using a systematic approach. The use of CA in this study allowed the researcher to make inferences based on the participants' qualitative narratives.

Furthermore, this type of analysis seeks to explore written and verbally and visually communicated messages. This analysis method is utilised for the deeper exploration of written hymns, newspaper and magazine articles, along with political speeches in the 19th century (Harwood & Garry, 2003). According to Neuendorf (2002), CA has a very long history of use in areas such as communication, journalism, sociology, and, most notably, psychological research. Zhang and Wildemuth (2005) highlight that qualitative CA extends much further than counting the words or extracting content from text to explore meaning, themes, and patterns. CA permits researchers to obtain an understanding of the social reality of the participants in a subjective manner, yet still maintains scientific procedures. Berg (2001) concurs with this argument by denoting that qualitative CA generally seeks to produce descriptions aligned with the expressions of the participants.

According to Zhang and Wildemuth (2005), qualitative CA is mainly inductive and grounds the exploration of topics and themes, as well as the inferences drawn from them. Zhang and Wildemuth (2005) highlight that this early involvement in the analysis phase assists researchers to move back and forth between concept development and data collection, and directs researchers, in collecting the data, towards those sources that are more valuable in answering some of the research questions that have been introduced (Miles & Huberman, 1994). To the contrary, the quantitative CA approach seeks to examine information by presenting findings in duration and frequency format. Weber (1990) suggests that the best content analytical studies use both qualitative and quantitative approaches, which were used in this study to gain the advantage of both approaches. In addition, Weber (1990) points out that a qualitative CA approach consists of a process that is developed to reduce raw data into categories or themes based on valid inference and interpretation. Zhang and Wildemuth (2005) affirm that this procedure entails inductive reasoning, where themes and categories emerge from the information collected through a researcher's cautious analysis and comparison. Patton (2002) believes that qualitative CA does not need to exclude deductive reasoning and serves as a supplement to the quantitative procedure, which was also implemented in this study.

Substantiating trustworthy interpretations that are made in the social science domain, qualitative CA involves a set of systematic and transparent procedures for processing data (Zhang & Wildemuth, 2005). This study followed the following eight-part process:

1) Preparing the data after interview data had been collected;
2) Defining the unit of analysis, which was expressed in a singular theme or paragraph;
3) Developing categories and a coding scheme;
4) Testing the coding scheme through text from the narratives obtained;
5) Coding the text;
6) Evaluating the code consistency by checking and rechecking for duplication and irregularities;
7) Drawing inferences from the coded data; and
8) Highlighting the findings and methodology used in the research process.

It is important to state that in the eight-part process, the researcher did not make use of any software that deals with sorting and coding data.

4.8.1.1 Application of CA

This section focuses on the practical application of CA by highlighting the shortcomings and positive aspects attached to using the qualitative analysis technique in this study.

The primary research question of this study served to firstly ascertain the primary features of digital awareness of cybersecurity among selected senior South

African military officers and, secondly, to identify the framing of perceptions concerning cybersecurity. The application of CA allowed the researcher to engage with the information retrieved from the participants. At the onset of Phase 1, the researcher engaged with the very first interview and analysed the categories and themes that emerged. This allowed the researcher to identify which questions could be asked differently, while maintaining the same core focus, what items in the interview guide could be elaborated on, and where participants needed clarification.

Preparation of the data before conducting CA required the researcher to ensure that the appropriate sample criteria and sampling approach were used. This was discussed earlier in this chapter (see Section 4.4), where the appropriateness of these techniques was confirmed to be in alignment with this study's objectives and research questions. However, it should be noted that some of the major challenges with CA revolve around the subjective nature of the theory and its validity, as well as that the information used in the study was recorded, which thus excluded other potential participants in the broader population who could have provided other perspectives on the phenomenon being explored. Additional procedures such as the checklist were therefore utilised to track the process. The chief findings of the analysis are based on the researcher's own assumptions, which were captured in an analysis schedule that reported on the meaning units, condensed meaning units, codes, categories, and themes.

Certain challenges emerged from the application of the CA process. One of these concerned the ability to employ inter-coder reliability[25]. This refers to the employment of an additional researcher to assess consistency in the coding process, which was found to be impossible as only the researcher had primary access to the data and analytical tools as ethical clearance required this. To mitigate the risk, the researcher used a reflexive journal[26] to capture any preconceived prejudices and to reflect on the coding and categorisation process, as indicated in the audit trail[27] of the study. Proof of this audit trail can be found in Appendix O. Furthermore, Feng (2014) highlights that reliability is an important aspect of any CA that is performed. The researcher ensured that coding procedures were maintained throughout the analysis

[25] Inter-coder reliability refers to the approach where a numerical measure is taken based on the consensus reached between two or more coders regarding how the same data should be coded (O'Connor & Joffe, 2020).

[26] A reflexive journal refers to a record of examining one's own explicit and implicit assumptions about the qualitative and quantitative phases in a study (Korstjens & Moser, 2018).

[27] An audit trail refers to the description of the research steps taken throughout a research study (Korstjens & Moser, 2018).

process of the study. The primary coding and theming of the interview data were carried out after the researcher had transcribed the first interview. This was done to ensure that the researcher was prepared for the analysis process and the potential views that might emerge from the data (Lacy et al., 2015). The development of a written protocol needed to take place as this allowed the researcher to be consistent when assigning meaning units. As a coding protocol generally involves two or more researchers, which proved impossible in this case, the written protocol ensured the reliability in the study. As the latter was not possible, the researcher had to be especially aware of his own bias when coding the data. Furthermore, the researcher ensured that the meaning units corresponded with the coding schemes. The researcher complied meticulously with all the relevant aspects regarding validity and reliability (Vourvachis & Woodward, 2015). A discussion of validity and reliability was presented in Section 4.9.

As confirmed in previous sections in this chapter, after the first interview, the researcher engaged in the verbatim transcription process, which permitted the identification of meaning units, codes, and themes. This allowed the researcher to gauge what the next interviews could involve and how to pose certain questions to the participants. The researcher followed this route to establish validity and reliability in the data (Dixon, 2008). The transcription process took approximately three weeks. In addition, the coding process took four weeks to complete. One of the key limitations of CA is researchers’ inability to accurately separate the findings from their assumptions and not being able to use an additional coder to minimise bias (Dixon, 2008). The researcher was solely responsible for the transcription and coding procedures employed in the study. As previously stated, it was impossible to use inter-coding and intra-coding given the sensitive nature of the information in the study as no additional individuals received the relevant authority to handle the potentially sensitive data. The researcher therefore used triangulation to confirm whether the information derived from the codes were consistent with the findings derived in Phase 2 of the study, which formed both quantitative and qualitative phases (see Section 4.8.4 for further elaboration).

4.8.1.2 Step 1: Analysing the qualitative data

The first step the researcher took was to organise the information obtained from the transcription sheets and prepare it for the analytical phase of the study. The researcher subsequently engaged with the data obtained from the semi-structured interviews conducted from April to June 2019 and transcribed each of the 10 interviews with participants located at the SANDC. The researcher carefully read each transcription several times to ensure that all the information was accurately noted and transcribed. This process was particularly crucial as the researcher had made annotations on each transcription sheet. The personal annotations gave the researcher a sense of what was to follow in the data and assisted with understanding the context in which the interviews took place. This phase in research typically deals with the meaning unit and is called the decontextualisation process.

The meaning units in the analysis process relate to the actual meaning of the data (see Appendix M). The identified meaning units were allocated participant numbers. The meaning units were then inserted during the decontextualisation process as they were constructed by way of a paragraph or sentence that allowed the researcher to gain a sense of what was reflected in the data (Bengtsson, 2016).

Upon analysing the data, the researcher engaged with the interview transcription sheets for consistencies and similarities between points that the participants from the SANDC had highlighted. The meaning unit may thus be interpreted as a condensed description of what the participants had actually said, presented in the form of a narrative through the transcripts (Gunnarsson, 2018; Graneheim & Lundman, 2004), and served as a precursor to the creation of codes in the data-analysis process (Berg, 2001). This is demonstrated in Table 4.4, in the extract from one of the interviews. In order to understand each code, the researcher constructed them to align with the context of the study. This was done to ensure that the researcher remained consistent throughout data analysis. Once the meaning units had been acknowledged in the analysis process, the researcher used digital colour markers to identify and separate the meaning units to clearly highlight their use or rejection. Where the meaning units did not have explicit links with the objectives of the study, the researcher, as is allowed, rejected them (Bengtsson, 2016). In this particular analysis, the researcher had to remain neutral when extracting information concerning aspects of cybersecurity awareness, lack of information-sharing practices, organisational challenges in terms of accessing new technology, as well as training of South African military officers.

The next step in the process was to condense the meaning units. The researcher performed this task when extracting the data obtained from the qualitative interviews, as presented, for example, in Table 4.4, where one meaning unit is displayed (see Appendix L). The condensed meaning units needed to be reduced, while those selected retained the core meaning of the extended text.

Table 4.4: Meaning unit and condensed meaning units of the data

Meaning unit	Condensed meaning unit
… I do feel that they should share information on what happened on Facebook, for example, and state that they have detected this and that it's wrong, and because of the lack of knowledge about a command like this, uhm, you kind of don't know what's allowed and what's not allowed. And you don't want to start a name-and-shame campaign but, yeah, we don't know" (Participant 2, senior military officer).	Members are unsure what to do in terms of information sharing.

4.8.1.3 Step 2: Coding the qualitative data

The coding process follows after the creation of meaning units, which are compressed descriptions of the participants' actual narratives. Given the small number of participants in Phase 1, the researcher did not use a coding program such as NVivo to sort the data, but rather personally involved himself in the process and applied the inductive approach. This process implies that the researcher first received the data and then inferred from it what possible codes might meet the research aim. Furthermore, the coding sheet (see Appendix M) assisted the researcher in the analysis process. This procedure ensured that the researcher was able to keep track of his own view of the data and how the coding process evolved as the researcher became better acquainted with the data (Bengtsson, 2016). According to Downe-Wambolt (1992), the researcher is required to engage with the coding process for each transcription and make notes, while being aware that the interpretations and the process itself may shift and have an impact on the reliability of the data. Codes were therefore digitally indicated on each transcription sheet in different colours. Table 4.5 is an example of how codes were used in the analysis process.

Table 4.5: Codes used in the analysis process

Codes	
Violations in cyberspace	Trust in technology
Violating organisational trust	Trust in each other
Awareness initiatives	Trust in the organisation
Awareness through education	Policies
Lack of seriousness	Online security culture
Proactive measures	Organisational culture
Training of members	Security awareness
Challenges in accessing knowledge	Unclear awareness information
Mutual trust	Vigilance
Refusal to adapt	Prior knowledge
Different generations	Physical security vs digital security
Online security	Removal of devices
Personal devices	DoD online systems
Unclear awareness procedures	Access to information
Limited understanding	DoD software
Implementation	
Older means of communication	
More fast-paced	
Expanding gap	
Open-source applications	
Information security	
Outdated technology	

The table used colour coding, which represents the various thematic groupings these codes fall under. The colour of the codes in Table 4.5 links with the colour of the themes and meaning units presented in Appendix L. The researcher used the aforementioned process during analysis as this enabled him to identify which codes were based on which description and colour. Each of the codes had a specific meaning, which could be linked with its associated meaning unit. In the process of creating codes, the researcher reviewed each part of the text that comprised the data and the suitability thereof for answering the research questions and objectives. For example, the code "violations in cyberspace" is associated with the category of "awareness construction", as indicated in Tables 4.5 and 4.6 in this section. Viewing this code and its category in isolation would not have revealed sufficient meaning. The analysis process demanded a horizontal view of the analysed data to have as the outcome a consistent stream of meaning attributed to the analysis units. Table 4.5 shows the codes used in the analysis process prior to the researcher engaging in the categorisation phase of the process.

4.8.1.4 Steps 3 and 4: Categorisation and theming

Inductive CA is believed to be appropriate for studies that are developing a theory or are contributing to an existing body of knowledge (Zhang & Wildemuth, 2005). Step 3 involved the development of categories and themes. This step involved answering the crucial questions that related to the "what, where, how, and when" aspects of the data analysis. The researcher ensured that the appropriate codes were categorised and themed according to the relevant factors derived from the text. However, before the researcher began to create categories, the step of condensing meaning units needed to be performed. This entailed reducing the number of words necessary to describe meaning without losing any of the content of the unit (Graneheim & Lundman, 2004). The depth of the meaning units determines the level at which the analysis can be performed. The process of condensation helps when data are based on interviews and CA is to be carried out after transcription. To extract the essence of the data, the coded material can, as has been suggested, be divided into domains or broad groups based on the different focus areas that received attention in the study (Catanzaro, 1988; Patton, 2002). Graneheim and Lundman (2004) prefer the concept "content area" since, in their view, this indicates an explicit area. For example, the material can be divided based on the questions posed when the data were collected or the theoretical assumptions that emerged from the literature (Graneheim & Lundman, 2004). Table 4.6 shows the process the researcher followed in the categorisation of the themes, which formed part of Steps 3 and 4 of the data analysis.

Table 4.6: Categorisation of the SANDC data across all themes

Categories that emerged from the data	Dominant themes
Awareness construction	Theme 1: Knowledge production and training focusing on cybersecurity awareness
Absence of awareness procedures	
Measures to secure information in cyberspace	
Challenges of implementation in the organisation	
Training of members to create cyber awareness	
Distrust in one another	Theme 2: Challenges of trust with technology and members
Distrust in policies	
Distrust in DoD computers	
Practices and guidelines of cyber in the organisation	
Relaxed take on cybersecurity	Theme 3: The construction of a digital culture among members
Behaviour of not caring	
Absence of mutual trust	
Organisational response to cyber	
Cyber culture	
Reliance on technology for operational activities	

Categories that emerged from the data	Dominant themes
Divide in the understanding of cyber	
Method of communication	
Technological demand	
Distrust in one another	Theme 4: The view on cyberthreats is constructed based on experiences in the physical domain
Distrust in DoD computers	
Distrust in policies	
Perception of insecurity	
The balance between viewing threats in a physical and a digital space	
Prior knowledge assists with information security	
Official hardware used for securing information	
Behaviour of information security practices	
Members questioning the trustworthiness of DoD-sanctioned software	

The colour coding of the information supplied in Table 4.6 shows that it can be linked to the meaning units and codes presented in Appendix L and Table 4.5. The use of colour in the presentation of the table is to make the information easier to read. The blue categories were grouped under Theme 1: *Knowledge production and training focusing on cybersecurity awareness.* The colour orange frames the categorisation of Theme 2: *Challenges of trust with technology and members.* The green categories are linked with Theme 3: *The construction of a digital culture among members.* The ivory category frames Theme 4: *The view on cyberthreats is constructed based on experiences in the physical domain.* The categorisation and coding of data are further elaborated on in Appendix L. It is worth noting that the same colour coding was used in Table 4.5 to ensure meaning and consistency.

The categorisation of the themes leads to the organisation of extracted data. This process involves the identification of categories and themes when the extraction of a theme from the data answers the “how” question. According to Bengtsson (2016), the data should be heterogeneous in its categories and homogenous in its themes. Step 4 involved the researcher testing the coding scheme through the participants’ qualitative narratives. The final phase of the analysis required writing up the findings, which included presenting the interpretations. The content and layout of Table 4.7 indicate the way the analysis process was carried out to achieve all the essential parts, but also pertain to how the coding scheme linked up with the meaning units and themes.

Table 4.7: Example of the analysis process

Meaning unit	Condensed meaning unit	Code	Category	Sub-theme	Theme
I do feel that they should share information on what happened on Facebook, for example, and state that they have detected this and that it's wrong, and because of the lack of knowledge about a command like this, uhm, you kind of don't know what's allowed and what's not allowed. And you don't want to start a name-and-shame campaign but, yeah, we don't know (Participant 2, senior military officer).	Members are unsure what to do in terms of information sharing	Trust in the organisation	Distrust in policies	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members

The literature review in Chapter 2 revealed that cybersecurity is an emerging field of study in the South African context. The researcher thus used CA as a way of exploring and contextualising how cybersecurity is approached and viewed among South African military officers. Utilising CA ultimately afforded the researcher the opportunity to participate in the research process by engaging with the content that the participants provided during the interviews and that the researcher found in the concomitant analysis process. CA as a method is flexible when the aim is analysing information. However, this study adopted the CA guidelines that better suited the objectives of the researcher (see Section 4.8.1.1).

Furthermore, utilising inductive qualitative CA as a technique contributed towards the exploration of the participants' perceptions of cybersecurity within the confines of each individual's reality. Hansen and Nissenbaum (as cited in Lacy & Prince, 2018) suggest that ST may facilitate understanding emerging threats in cyberspace as a domain. In addition to ST, the exploration of cybersecurity in specific contexts also allows for a better understanding of how threats are constructed and how they are perceived by South African military officers, which relates to the second objective of this research.

4.8.2 *Phase 2 data analysis: Descriptive and thematic analyses*

The data analysis relating to Phase 2 involved analysing the data that accrued from the completion of the COQ. The COQ data consisted of Likert scale items and short questions, which required two data-analysis techniques. As a result, the researcher analysed the Likert scale items descriptively and used thematic analysis for the short questions.

4.8.2.1 Descriptive data analysis

Descriptive data analysis may take place as a stand-alone analytical technique. In this study this technique lent itself to Phase 2 of the study, specifically the Likert scale items in the COQ. Quantitative description analysis, as employed in this study, sought to identify patterns in the data across sample populations (Loeb et al., 2017). It is important to note that the analysis was not appropriate for generalising the findings beyond the parameters of the sample population groups as descriptive analysis merely ascribes the responses received to the scale items included in the COQ. Descriptive analysis links well with the research questions and aims of this research study. In addition, descriptive statistics were regarded as appropriate for assisting with communicating the findings and performed by using SPSS version 24 (Chaumba, 2013; IBM Corporation, 2016).

The first step in the descriptive data analysis was to present the biographical data, which comprised categorical variables such as ethnicity, gender, arms of service, and rank in the SANDF. As part of the descriptive analysis process, the researcher analysed the Likert scale items, by employing the frequency distributions and cumulative percentages of these items (Chow, 2002). Moreover, the Likert scale data for the COQ were analysed and presented as percentages and listed in respect of each Likert scale item in the COQ. This allowed the researcher to present an overall view of how the military officers in the sample responded to the Likert scale items and, more specifically, the dimensions of the COQ.

4.8.2.2 Thematic analysis

The short questions from the COQ were thematically analysed because the researcher wanted to establish the participants' core views. Thematic analysis was appropriate for this study as it is identified as a foundational approach for a qualitative researcher who is embarking on uncovering meaning in social contexts, which is still to follow (Braun & Clarke, 2006). Thematic analysis can be described as a method to identify, analyse, and report themes that emerge from the data and allows for the organisation and description of the data, which can consequently be interpreted as findings with deeper meaning (Braun & Clarke, 2006). Boyatzis (1998) suggests that thematic analysis enables the researcher to extract the meaning of the findings through applying it thematically to understand the topic under consideration. Thematic analysis is considered a method rather than a methodology, is more flexible in nature, and cannot be fixed to an epistemological or a theoretical framework (Clarke & Braun, 2013; Braun & Clarke, 2006).

The short questions in the COQ, which were thematically analysed, are captured in Table 4.8. The results of the short questions' analysis contribute towards understanding the context in which military officers answered the scale items in the COQ. The researcher therefore determined that thematic analysis would be useful for this study as it allowed the researcher to make connections between the content of the scale items and that of the short questions (Alhojailan, 2012). It followed that Braun and Clarke's (2006) six-step process would be appropriate to analyse the short questions in Phase 2 of the study. These six steps are: (1) become familiar with the data, (2) produce initial codes, (3) search for themes, (4) review themes, (5) define the themes, and (6) write up the results by indicating the themes. A detailed demonstration of the codes and themes of the short questions is presented in Chapter 6. Furthermore, an exposition of the production of the codes is available in Appendix N.

Table 4.8: Short questions in the COQ

Question 14: What would you consider to be sensitive information?
Question 15: How would you describe the culture of cybersecurity within your workplace?
Question 16: Do you share work information with colleagues on a regular basis? And why?
Question 17: How do you feel about sharing sensitive information with your colleagues?
Question 26: What do you think of cybersecurity?
Question 27: How would you describe your behaviour on the Internet?
Question 28: How do you feel about your behaviour when using Internet websites?
Question 52: Does cybersecurity affect how you interact with others in your workplace?
Question 53: What do you feel is the best way to manage cybersecurity in your workplace?

4.8.3 Integration of Phase 1 and Phase 2 results

The construct that was measured in this study was cybersecurity awareness. Given the complexity of the factors associated with cybersecurity awareness, it was crucial to include various features that are associated with this domain to achieve clarity and understanding. The findings obtained through the sequential data-collection process allowed for the data derived from both the semi-structured interviews and the COQ not to be viewed in isolation. Instead, they enabled the researcher to make the connections that a single approach would not have facilitated. It is, as previously stated, important to note that ST, along with supporting literature in the field of cybersecurity, was used to guide the construction of questions for both the interview guide and the COQ (see Appendix S).

Once the interview data had been analysed, the researcher engaged in the interpretation process, which enabled presentation of the four dominant themes. The themes were categorised in table format, which allowed the researcher to view them comparatively with the main findings that emerged from the questionnaire. Once this process had been completed, the researcher was able to consider the findings in relation to the research objectives of the study. Each research phase allowed the researcher to gauge the patterns that emerged from the data (Bowen et al., 2017). The findings derived from the qualitative phase motivated the researcher to introduce contextual reasons for the participants' views of cybersecurity.

It is important to point out that all the responses to the COQ questions were combined. These findings (from nine short questions) were used to substantiate the responses to the scale items included in the four dimensions of the COQ. The large number of responses in the COQ necessitated the short questions to be grouped and analysed thematically. The short questions contributed to the interpretation process as they enabled the researcher to determine whether the findings across two methodological approaches were in line with "what" participants were revealing; in other words, whether they were true. The relevance of this is that the short questions, along with the Likert scale items of the COQ, supported the original reason for selecting the mixed-methods design.

4.8.4 Triangulation of Phase 1 and Phase 2 results

In an earlier section of this dissertation, the researcher emphasised the triangulation of the findings (Foxcroft & Roodt, 2007). Farmer et al. (2006, p. 377) describe triangulation as “a methodological approach that contributes to the validity of research results when multiple methods, sources, theories and/or investigators are employed”. Guion (2002, p. 1) suggests five triangulation techniques, namely (1) methodological triangulation, (2) data triangulation, (3) theoretical triangulation, (4) environmental triangulation, and (5) investigator triangulation. The researcher utilised data triangulation as an approach to increase internal validity (Farmer et al., 2006). Data triangulation was introduced to validate the research findings through two streams of data sources, which include in-depth semi-structured interview transcriptions and a questionnaire. The researcher employed triangulation in Chapter 7, where the integration of the findings is discussed.

4.9 Validity and reliability

Social science research demands that researchers understand the complexity of the context but, more importantly, gain an understanding of concepts relating to validity, reliability, and objectivity (Mohammad, 2014). Reliability and validity act as quality assurance checks in the research process and assist researchers with adhering to sound practices, as highlighted in the qualitative and quantitative paradigms of the study. The terms “validity” and “reliability” are described and used differently by qualitative and quantitative researchers (Shenton, 2004; Guba, 1981). Credibility in qualitative research denotes whether the findings derived from the research are an accurate reflection of the interpretations of participants’ views (Korstjens & Moser, 2018). From a quantitative perspective, credibility can be translated as internal validity (Guba, 1981). Internal validity refers to the conclusions drawn from findings proven to be accurate (Patino & Ferreira, 2018). In this regard, the researcher used the COQ, which assisted with providing a comprehensive view of the respondents’ perceptions. The aim, throughout the research process, was to avoid influencing the respondents’ views and to create a space in which they were able to speak openly; therefore warranting reliability and validity during the research process (Babbie & Mouton, 2007). Similar to the aforementioned point, the researcher ensured that the credibility of the topic under exploration was maintained in such a manner that the results could be deemed trustworthy, and that integrity was sustained (Babbie & Mouton, 2007).

Guba (1981) highlights that there are four trustworthiness concerns that all researchers should address in their respective studies and posits that these guidelines can be used to evaluate the methodological rigour of a research study. These guidelines relate to credibility, confirmability, transferability, and dependability (Anney, 2014).

4.9.1 Credibility

Credibility refers to the value of truth in the research process and highlights the associations between participants' perceptions of the situation under exploration (Collier-Reed et al., 2009). In addition, credibility also refers to the researcher's own viewpoints regarding the process that he or she underwent during the research. When undertaking research, it is essential for the researcher to be aware at all times of existing subjective motives or bias as it is imperative to acknowledge these when data are collected and interpreted (Zygmont, 2014).

Prejudices that are created by cultural and religious systems were not considered in this study, but their existence was given due consideration when the participants were interviewed. The researcher utilised reflexivity procedures to improve the credibility of the findings obtained in the qualitative phase of this research. Spencer and Ritchie (2012) suggest that credibility is linked to the preservation of the inferences drawn from the data and the methodological rigour of the process through which findings are reached. Zygmont (2014) denotes that credibility can be achieved in qualitative research by providing for the following: quotations for preserving statements, peer-review procedures, member validation, and following comparison methods. Mohammad (2014) captures this aspect of credibility by revealing the usefulness of utilising participant quotations and reflections throughout the research process and confirming the value of truth. The respondents' views were included in this dissertation by presenting them in extracted quotation format. The researcher also engaged with credibility by using triangulation to show corroboration between the findings derived from the interview and the questionnaire (Shenton, 2004).

4.9.2 Confirmability

Baxter and Eyles (1997) posit that confirmability as a concept in the post-positivist paradigm refers to the extent to which the findings of a study can be established or substantiated by other researchers in the social sciences domain. Several strategies can be utilised to establish confirmability in research findings. These strategies comprise an audit trail, triangulation, and using a reflexive journal (Anney, 2014). For this study, the researcher used a reflexive journal to augment the confirmability of the research findings in Phases 1 and 2 (see Section 4.10 on reflexivity). Furthermore, the researcher also employed both the audit trail and triangulation methods as Phase 2 of the research was a quantitative method of inquiry (see Section 4.8.4 on triangulation).

4.9.3 Transferability

Transferability in qualitative studies refers to the generalisability of the research findings and replicating or transferring them to different contexts, including new participants (Bitsch, 2005; Tobin & Begley, 2004). Transferability of this study's findings was attained by employing purposive sampling as a strategy in providing a detailed description of the research setting and the research procedure followed (Anney, 2014). Phase 1 of this research utilised purposive sampling to improve the transferability of the findings obtained in the qualitative phase. Transferability also refers to the researcher describing the context in which the research takes place, and to providing a sense of the behaviour and perspectives of the participants (Korstjens & Moser, 2018). Providing an in-depth description of the context in which this study was conducted allowed for the participants' experiences to be rendered meaningful to the reader (Korstjens & Moser, 2018). Furthermore, the transferability of the findings ultimately means the reader should be able to judge whether the findings and methods applied in this context can be replicated and found to be appropriate in their own context. The context in which this study was undertaken was described in Section 4.5.

Furthermore, the researcher recruited military officers as respondents who were able to provide a military perspective of issues that were connected to the phenomenon being explored, as well as the study's research questions. The second phase utilised cluster sampling as participants were selected based on their availability and owing to the sampling characteristics; one of them being part of a homogeneous group. Phase 2 involved administering the COQ to sample populations at two senior academic training institutions, namely SAMA and the SANWC. This chapter also produced a detailed procedure including the methods and research process adhered to, as well as the context of the respondents. This approach may in future assist scholars to review the suitability of the research conducted in this specific military context and provide insight into how this research could be made transferrable to a different context with other potential participants (Anney, 2014).

4.9.4 Dependability

The dependability of qualitative studies means the extent to which the findings of the study are deemed reliable (Anney, 2014). Lincoln and Guba (1985) note that for dependability to be established in a research study, the researcher should always keep in mind the credibility of any procedures that are used. In addition, Guba (1981) highlights that dependability can be translated into reliability in quantitative research. Furthermore, dependability is described as “the stability of findings over time” (Bitsch, 2005, p. 86). Tobin and Begley (2004) suggest that dependability includes participants reviewing the results along with the interpretations and recommendations of the study. This is to ensure that they agree with what had been mentioned based on the data derived from the participants during the research process. According to Vermooten (2018) and Anney (2014), the dependability of the research findings can be ascertained by employing the following strategies: an audit trail, a code-recode strategy, stepwise replication, triangulation, and peer examination.

In this study, the researcher utilised the following methods to improve dependability: an audit trail, peer examination, and triangulation. An audit trail was produced for each step in the qualitative and quantitative phases of the research. The audit trail consisted of a reflexive journal that accounted for the researcher’s reflections on the methodology and interviews, and included preconceived prejudices. Evidence of the audit trail is available in Appendix O. The researcher used several conference platforms that related either to a psychology or military context. The purpose was mainly to deliberate with colleagues who were unfamiliar with the topic, but who were considered experts in research methodology, research procedures, and preliminary findings. Owing to this being a mixed-methods research study, the objective was to increase confirmation of the findings by using two or more methods (Heale & Forbes, 2013). The findings of the semi-structured interviews were thus positioned as the main data-collection technique. The findings of the COQ were comparatively applied with those of the interviews, which were conducted in Phase 1 of the study. In addition, the findings of the COQ were based on data derived from the selected samples at two training institutions, namely SAMA and the SANWC, with the findings of the study achieved by using the procedural steps displayed in Figure 4.1.

4.10 Reflexivity

Reflexivity was applied in this study as a tool to guard against preconceived prejudices. Reflexivity as a qualitative concept was considered crucial to the researcher in this study as he was the primary instrument conducting the qualitative inquiry (Watt, 2007; Patton, 2002). Furthermore, the selection, collection, and interpretation of data were influenced by the researcher, who inevitably influenced the direction of the findings as participants' responses are always exposed to the interpretation of the researcher (Finlay, 2002; Holland, 1999). It is thus necessary for researchers to evaluate the impact of intersubjective elements on the data-collection and -analysis processes in order to increase the measure of integrity in qualitative research (Dobronravova, 2009; Finlay, 2002). Moreover, it was necessary for the researcher to declare and be open about his attitudes and views regarding the topic being explored, namely cybersecurity, and how this is viewed in a military context. The element of reflexivity is crucial to succeed in presenting the reader with an unbiased view of the topic and to facilitate understanding (Dobronravova, 2009). It is worth noting that the researcher is a civilian and unfamiliar with the SANDF.

As the researcher commenced with this study and underwent a process of acquiring additional knowledge through engaging in scholarly activities, his perceptions regarding military organisations changed after extensively consulting literature associated with international military organisations. To prevent contamination in the research process, the researcher engaged in self-reflective activities by exploring his reactions and experiences. By engaging in such practices, the researcher was able to recognise and deal with preconceptions that might have influenced his capability to be unprejudiced and to be non-judgemental in his actions, observations, and thoughts while conducting the research. Furthermore, the researcher made several references to the notion that military officers were not completely isolated from society, yet it should be emphasised that the researcher himself, in his personal experience, fell victim to the perspective that members of the military were also influenced by the media's agenda and the public's perceptions of the SANDF. Hence, the imperative of a reflexive journal grew as the process the researcher underwent during the writing of this dissertation could be considered one of dialogue and introspection, as captured in the journal. This reflexivity may be regarded as crucial for the research process as the researcher became very aware of his subjectivity, especially when interacting with the participants during the interviews.

Palaganas et al. (2017) recommend that the relationship between the researcher and the participant should always be made clear during the reflexive process. The reflexive journal is a measure through which researchers can be continuously made aware of their values and preconceived judgements to mitigate their impact on the research practice and process (Pillow, 2003). One challenge that arose between the researcher and the social realities of the participants was characterised by the different views of security measures that were prevalent, which were presented as the norm in most cases. The researcher was therefore confronted with social constructs that were not of his own making, as Parahoo (2006) notes in his study. The researcher had to continuously reflect on his preconceived ideas about the topic of the study and give due consideration to the nature of the SANDF. The next section focuses on the ethical considerations followed in this study.

4.11 Ethical considerations

The researcher endorsed and adhered to conducting himself in line with the ethical requirements outlined by SU, as well as the ethical guidelines of the Health Professions Council of South Africa. This study involved the participation of active military officers who were serving in the SANDF. Participating in this study did not infringe on the dignity, rights, safety, or wellbeing of any officers of the military. Despite the low ethical risk associated with participating in this study, the researcher carefully considered any potential ethical risks associated with members of the military participating in either the interviews or responding to the self-administered questionnaires.

The qualitative and quantitative phases of the research commenced once Defence Intelligence, along with the SANDC, SANWC, and SAMA, had authorised it and the ethical approval of the Research Ethics Committee: Human Research

(Humanities) of SU had been received. The process of participating in the interviews and responding to the questionnaire for the purposes of this study was voluntary. The researcher made use of consent forms that outlined the conditions of participation in this study (see Appendices A and B). The researcher acted ethically in presenting the consent form and explaining all the relevant information pertaining to this study. Participating military officers were informed of their right to withdraw their consent to be involved at any time during the research process without being exposed to any consequences or penalties. It is noteworthy to mention that participation in the face-to-face interviews did not require military officers to engage in any follow-up interviews. The researcher engaged in semi-structured interviews in order to fully capture the contextual realities of the participants. Each of the semi-structured interviews lasted on average between 25 and 45 minutes. This length of the interviews allowed the researcher to engage with the research participants and grapple with the information received. The confidentiality of the participants' information was assured and ensured. The participants were allocated a pseudonym to ensure anonymity and confidentiality. Only the researcher had access to the information, and all identifying information, for example the names and contact details of participants, was stored separately from all other information, also in a secure location. In addition, no identifiable information was linked to either the interviews or questionnaires. No falsification of findings took place in the analysis and reporting procedure of Phases 1 and 2. Additionally, the researcher did not engage in plagiarism activity, especially in the construction of items in the data-collection tools and literature presented. Furthermore, all the information collected from participants was encrypted and password protected. After a period of 15 years, the data and records obtained from the participants will be destroyed professionally.

4.12 Conclusion

The aim of this chapter was to provide a discussion of the methodology used for this study. In this chapter, several key aspects were covered, including the research objectives, as well as the rationale and aim of the research. Thereafter, the focus was directed to the research paradigm, which presented the reasons why this study utilised a mixed-methods research design. Following this, the research design was also elaborated on to add to the in-depth discussion of the selected qualitative and quantitative approaches. The chapter also described aspects linked to the sample criteria and the selection of participants.

Data-collection tools were also discussed extensively and the motivation to use the semi-structured interview and a questionnaire was justified by not only pointing to the objectives, but also the research design that was selected. The focus of the chapter then moved to the data-analysis method that was used in this study, which highlighted CA and the steps used for rigour in Phase 1. The researcher also discussed the data-analysis procedure for Phase 2, which involved descriptive analysis and thematic analysis. The integration of the results for Phases 1 and 2 were discussed, with a subsequent focus on triangulation. Moreover, the chapter highlighted aspects related to validity and reliability, and included important criteria for credibility, confirmability, transferability, and dependability, as well as reflexivity.

The methodological considerations in this chapter form the basis of the context of Chapter 5, in which the findings of Phase 1, as produced by the data-collection process, are presented.

CHAPTER 5:
PHASE 1: CONTENT ANALYSIS (CA)

5.1 Introduction

This chapter focuses on the findings of the interview data extracted from senior members of the military located at the SANDC. Chapter 5 serves as the starting point in answering the secondary research questions, which act as a gateway to understanding cybersecurity from the view of the South African military officer. This chapter explains the CA of the semi-structured interviews. It is important to note that the qualitative phase of the study presented in this chapter (1) informed the development of the COQ, and (2) acted as the foundation on which the COQ data were triangulated with the interview findings.

The objectives of the study, as outlined by three specific secondary research questions, guided the qualitative CA process. The questions are as follows:

1) How do South African military officers conceptualise cybersecurity awareness?
2) How do South African military officers perceive cybersecurity threats within the SANDF?
3) What are the perceptions of cybersecurity awareness through the lens of the military officer?

The meaning units, codes, and categories of the CA performed were discussed in Chapter 4. Chapter 5 contains the presentation of the main themes and sub-themes that the researcher identified through the CA process. The next section contains the demographic information of the participants located at the SANDC.

5.2 Demographic information of participants at the South African National Defence College (SANDC)

Table 5.1 shows the demographic information of the participants at the SANDC according to gender, province, rank, race, and arms of service.

Table 5.1: Demographic information

Participant no.	Gender	Province	Rank	Race	Arms of service
1	Male	Western Cape	General	Coloured	South African Air Force (SAAF)
2	Female	Gauteng	Colonel	White	SAAF
3	Male	Gauteng	Colonel	White	South African (SA) Army
4	Female	Gauteng	Colonel	Indian	SA Army
5	Male	Gauteng	Colonel	White	South African Military Health Service (SAMHS)
6	Male	Limpopo	Captain	Black	South African Navy (SAN)
7	Female	Gauteng	Colonel	Black	SAMHS
8	Female	Gauteng	Colonel	White	SAAF
9	Male	Gauteng	Colonel	Black	SA Army
10	Male	Gauteng	Colonel	Coloured	SA Army

Based on the information in Table 5.1, it is evident that six males and four females participated in the interviews. With regard to the branches, three participants were members of the SAAF, and four participants were from the SA Army. Furthermore, there were only two participants from the SAMHS and one participant from the SAN. It is imperative to note that the included racial categories were part of the Population Registration Act 30 of 1950, which is currently still being used in South Africa.

5.3 Outline of themes

The themes are represented by either a sentence or through more detailed sections, as previously noted. The researcher, once he considered a theme as important, after it had been identified as adding value to the study, recorded the participant's narrative and the page number on which the meaning unit was located. The researcher merged any overlapping or duplicate themes that were highlighted during the analysis process. Following this, the researcher identified any themes that were not part of the coding scheme. Furthermore, the researcher made inferences from the most dominant categories derived from the texts relating to the perceptions of South African military officers. Table 5.2 displays the extracted themes and sub-themes that emerged from the CA process.

Table 5.2: The four main themes and sub-themes of the study

Themes	Sub-themes
1. Knowledge production and training focusing on cybersecurity awareness	Awareness and knowledge of cyberspace and its associated dangers.
	The establishment of cybersecurity awareness among military members.
2. Challenges of trust with technology and members	Vigilance among members of the organisation owing to differences in how cyberspace is approached.
	The uncertainty of cybersecurity best practices and protocols in the organisation.
3. The construction of a digital culture among members	Culture of digital security among officers.
	Personal devices are considered more efficient to store organisational information.
	Cyber increases the skills gap between more senior and junior military officers.
	The demand for faster and more efficient communication is becoming normalised practice.
4. Cyberthreats are constructed based on experiences in the physical domain	Information security as a practice.
	Perception as an important aspect to military members.

Relating to the discussion of the sub-themes that emerged from the data, the researcher created the context of the main theme as it denoted that awareness among military officers could not be viewed from an isolated stand, namely one that focuses on military officers' knowledge of cyber awareness. Instead, questions were posed during the interview that alluded to the concept of cybersecurity awareness by judging this topic from a contextual point of view. In analysing the participants' narratives, deeper issues related to awareness were raised, which focused mostly on organisational challenges concerning how cybersecurity awareness was viewed and not necessarily what it meant as a construct.

5.4 Theme 1: Knowledge production and training focusing on cybersecurity awareness

This main theme, *Knowledge production and training focusing on cybersecurity awareness*, focused on interviewed members of the military who shared the viewpoint that education on cyber awareness should be regarded as crucial by organisations and senior management. The main theme was accorded this priority given the emphasis on knowledge and awareness of cybersecurity. It was thus appropriate for the two sub-themes: *Awareness and knowledge of cyberspace and its associated dangers* and *The establishment of cybersecurity awareness among military members*, to be included under this main theme as they shared similar characteristics and fit the description of knowledge production and training in cybersecurity.

The analysis process, which entailed coding and categorising, as well as identifying thematic features in the data, clearly revealed that most members believed awareness training and knowledge on the topic of the main theme should form part of military training at all levels. However, some participants indicated that not all members should receive education and training in cybersecurity as it could pose a threat to the organisation if the knowledge was imparted to lower-ranking members. The participants conveyed the belief that NCOs might use this knowledge to their private advantage as they had not attended additional training on security, which senior officers had attended. On the other hand, it should be considered that this viewpoint was only shared by two of the senior military officers interviewed, while the majority believed that cybersecurity training should start from the foundation phases, which implied that training should commence at the basic level.

5.4.1 Sub-theme 1.1: Awareness and knowledge of cyberspace and its associated dangers

Sohrabi and Von Solms (2016) denote that a specific experience is owing to the accumulation of knowledge, which leads to acquaintance with, as well as comprehension of, specific events. In the context of this sub-theme, awareness and knowledge related to cyberspace refer to familiarity with the Internet and the information that could be linked to security threats, skills, and the capacity to prevent, manage, and alleviate the risk of sensitive information being vulnerable to exposure (Ashenden, 2008). Awareness and knowledge of cyberspace and its dangers emerged as a sub-theme as eight of 10 participants indicated that they were aware that their organisation focused on cybersecurity. On the contrary, while eight participants acknowledged that the organisation was aware of cybersecurity, five of the eight participants indicated that the organisation was not doing enough to promote education and training in cybersecurity.

For the purpose of this sub-theme, the focus was on senior military officers at the SANDC who had highlighted their awareness of the threats that exist in cyberspace, and who also indicated that they were equally cognisant of the practices that went hand in hand with remaining active in cyberspace. This outlook was, for example, corroborated by Participant 2, who argued:

> *"I think the organisation should enforce a policy more if there is one and to check and make a presentation during war*[28] *period once a month to say, like, that there were seven violations on Facebook and counter-M should look at this to create that awareness on rules and order within cyberspace"* (Participant 2, senior military officer).

Upon analysing the extracted text produced by Participant 2 in the interview, it became evident that the military officer referred to violations in cyberspace and highlighted the proposal that the organisation should be more active concerning the enforcement of policy, which links with creating awareness of cyberthreats. Participant 2's narrative was indicative of experiences that might have been noted on social media platforms such as Facebook. Social communication platforms such as WhatsApp and Facebook were the main concept identified in the narratives during analysis. The belief that the organisation should instil levels of awareness should nevertheless not be the only consideration in this sub-theme. How awareness was perceived and made practical should also be regarded as appropriate for consideration in this sub-theme, as can be seen from Participant 1's narrative:

> *"Like I said, being a human and pushing the military away from the normal human being, uhm, which is from a personal capacity, uhm, I don't think that I take it that seriously, but in my work environment I take it very seriously and I know the consequence[s] and implications. But from a personal view, people or hackers can build a personal profile of you and put it out there and that's why I don't belong to Facebook or have a Facebook profile, but I am on WhatsApp as it is more commonly used. So you can see my profile, but it doesn't say anything more on me. One thing that I do use is LinkedIn, which is what I use for jobs and linking with other professionals in my field and sharing information and creating a network. I also see a lot of my other colleagues on LinkedIn. That is of national security value in the sense that this information can be used either against or for. And you can use cyberattacks to get this information, which*

[28] Participant 2 referred to "war period" being held once a month. This terminology refers to a roll-call period, where discussions regarding administrative or operational activities are conveyed to military members.

> *is another form of warfare in my opinion, and if you are not aware of it, you may see your downfall"* (Participant 1, senior military officer).

The above narrative by Participant 1 pointed out the notion that awareness of digital threats may be linked with precautionary behaviour. Van Schaik et al. (2017) argue that the perception of risk is a good predictor of information security behaviour. Participant 1 showed that awareness was vital in securing personal information on social media platforms such as WhatsApp and Facebook. Building on this perception, it is also of key relevance to highlight that knowledge-based systems are generally constructed on the basis of the experience the users had accumulated in their specific context (Rice & Kitchel, 2016). Participant 1 revealed that they were aware of the dangers, which might pose a risk, in relation to personal information that could be used against them. Furthermore, this participant also explained that there were certain exceptions to being secure online as engagement on professional platforms such as LinkedIn was utilised for sharing information. However, the participant also acknowledged that information shared online might compromise the individual if hackers built a profile of them to extort information for some gain or alternatively for purposes of blackmail. Moreover, the participant also highlighted strictly avoiding social communication platforms where data were actively being mined, but also where it was easier for individual profiles to be constructed in association with individual preferences.

However, at the same time it could be emphasised that Participant 1 acknowledged the existence of a difference in the way cyberspace and security were viewed as there was a separation between professional duties and personal capacity. This separation in how awareness was perceived and enacted could be linked to the ramifications of cyberthreats for the organisation as it could have a detrimental outcome for the interests of national security. In addition, the sub-theme *Awareness and knowledge of cyberspace and its associated dangers* relates to the orientation of military officers towards cyberspace. This is a concept that focuses entirely on how the user is able to construct and apply security in a digital environment.

Orientation in a specific context is deemed necessary to consider, especially when the objective is to comprehend a specific object or event (Antonsen & Lundestad, 2019). The focus in this regard was therefore on those participants who were aware of cyberthreats in the military context, either having had prior exposure to training or who were in a position at work that demanded awareness and the necessity to be updated about relevant threats in cyberspace. Galletta and Polak (2003) note that employee behaviour in cyberspace is influenced by technological devices in the organisation. The individual who has such a device is therefore a central part of the cybersecurity process. Previous knowledge and exposure, as has been reiterated, might influence the interpretation of and approach to managing any issue that arises (Rice & Kitchel, 2016). As highlighted earlier, not all members of the military are aware of the dangers lurking in cyberspace and the concomitant implications in the physical domain. The aspect of awareness and knowledge in the cyber domain is considered as critical for the application of online behaviour (Bada et al., 2015). In confirming the aforementioned, Participants 3 and 6's narratives are presented, in sequence, as follows:

> *"The way we structured our security cluster and how we interact with other stakeholders, uhm, all I can say is that people always wake up after the incident. We are reactive as South Africans and we are supposed to be proactive. We are reactive in everything and that's the reason why some of us don't see cyberthreats as a threat. The military should control cyberspace and should be on top"* (Participant 3, senior military officer).

> *"No, I am not security conscious because we are not taught, because the department is not strict on us or telling us to follow the guidelines or even bringing in awareness on that factor"* (Participant 6, senior military officer).

Participant 3's narrative extract showed some indication that planning of defensive measures relating to cyberspace is not balanced from a national point of view and that security organisations are reactive and not necessarily proactive in their approach to cybersecurity awareness. It is important to note that this view cannot be generalised to the broader view of cyber capacity in the SANDF. Moreover, Participant 3 also connected their argument to the interpretation of threats. Bada et al. (2015) and Van Schaik et al. (2017) suggest that the issue of salience arises as this refers to the notion that behaviour online is shaped to a large degree by the measure of relevance of and the meaning attached to threats. The researcher pointed out previously that ST also played a role in the aspect of meaning attached to threats, whether existential or not. This point can be identified as referring to the knowledge component of this sub-theme.

Participant 6 revealed that not all military officers were aware of or possessed knowledge of threats in the digital domain. Participant 6's narrative can be interpreted as pointing to security awareness in the organisation and the responsibility for gaining the relevant knowledge resting with the SANDF, and that the organisation should promote education in cybersecurity. The point that emerged from this participant's narrative affirmed the idea that knowledge of a specific issue is pertinent to practising security behaviour.

Sub-theme 1.1 presented participant narratives regarding cybersecurity awareness in the organisation and the role of knowledge and awareness in displaying security behaviour. The next sub-theme relates to cybersecurity awareness among members of the military.

5.4.2 Sub-theme 1.2: The establishment of cybersecurity awareness among military members

The sub-theme *The establishment of cybersecurity awareness among military members* builds on the previous sub-theme, which focused on knowledge and training in the organisation, but more specifically so at an individual level. This sub-theme shifted the focus to aspects of training and education and what members of the military expect from the organisation. It is important to note that the questionnaire posed a question focusing on the expectation of military members regarding cybersecurity in the organisation. A focus on training and education linked to cybersecurity awareness featured prominently in the coding process. Through the analysis process, it became evident that military members were conscious of training at a basic level, which referred to the notion that content in this regard should be integrated into course material for all members who were undergoing mandatory cybersecurity awareness training.

At this stage, it became important to shift the focus yet again to the awareness responses of Participants 2 and 3 as the narratives drew on knowledge that cyber was an emerging domain that would require attention as technology has been advancing at a rapid pace:

> *"It should be an intervention where one should have training on a monthly basis and deliver education as technology is moving quickly"* (Participant 2, senior military officer).

> *"All people in the DoD should be trained, the skills should not be zoned to a specific group of people, and these skills cannot be zoned. If applied to all, the organisation and its people will have a positive outlook. You need to empower people so that [they] can foresee that if the current measures are in place [it] won't solve the problems and to provide feedback and just wait for specialists or that it will only be in the hands of specialists and Defence Intelligence"* (Participant 3, senior military officer).

The excerpt from the transcribed text of Participant 2 indicates that training should be a regular intervention. Routine awareness activities on cybersecurity are argued by Van't Wout (2019) to be a suitable solution when addressing the overall digital security in organisations. The excerpt from the transcribed text of Participant 3 indicated that information focusing on cybersecurity should be supplied to all military members so that the area of specialisation can be broadened to include most of the personnel in the organisation. Expanding on this narrative, it should be emphasised that training people in certain areas might alleviate some of the risks in online behaviour that have been expressed (Lahcen et al., 2020; Winkler, 2017). This view was shared by Participant 6, who also noted that creating a cybersecurity awareness programme or implementing certain awareness components in the courses that members of the military attend when embarking on a military career, when undergoing basic training in the SANDF, should be mandatory:

> *"This should come through basic training, so that we can be taught this subject at every course you come in contact with. The topic of cybersecurity should be considered a must at every course you are attending and should continue throughout your training as an officer"* (Participant 6, senior military officer).

Participant 6's narrative also confirms ensuring regular exposure to cybersecurity awareness information through the means of training. However, the participant did not specify whether that was applicable to all the members of the organisation, as reference was made to the officer rank only.

Continuing on from the view that training should be offered throughout the career of the military officer, Participant 4 made reference to the training material and the importance of communication in the process of establishing cybersecurity awareness among members of the organisation. Participant 4 placed this in context by suggesting the following:

> *"... uhm ... what we should add is to change the training material and not to just talk about documents but to make young officers and non-commissioned officers aware of the consequences and trends of what currently is happening in cyberspace and [the] security domain, you know?"* (Participant 4, senior military officer).

In the excerpt above, Participant 4 indicated that it can be highlighted that basic military training could be regarded as the starting point for skills related to cybersecurity, which should also be shared. Skills being shared among members in the organisation relating to awareness and security might produce benefits as they would be able to reduce the costs of technical challenges arising from the absence of awareness. Cyberthreats are able to become real and exploit users' data and have an impact on the integrity of systems and networks. Training members in preventative mechanisms and behaviour can thus reduce the risk attached to possible threats and attacks (Bada & Sasse, 2019).

This sub-theme dealt with the aspect of awareness in an organisation and the expectations of members of the military in respect of cybersecurity training. It was evident that eight of the 10 participants felt that cybersecurity education was an important component to subscribe to in the SANDF. The next main theme focuses on how technology is integrated into the organisation and as a consequence might have an impact on trust among its members.

5.5 Theme 2: Challenges of trust with technology and members

Theme 1 addressed how cybersecurity education and the possible use of technology can be integrated throughout the organisation. Furthermore, social media platforms and the Internet were viewed as a beneficial space where members can extract and share information. Theme 2 deals with the lack of trust some of the participants have in the organisation. Trust was considered a major requirement for the participants concerning their passion and respect for the organisation. This theme contains two sub-themes that are connected with the aspect of vigilance among members of the organisation, and the uncertainty associated with best practices related to cybersecurity protocols.

From an organisational perspective, trust can be viewed as imperative to achieve effectiveness in communication (Uslaner, 2002). Furthermore, efficacious collaboration among all members of an organisation and management is crucial in the establishment of trust (Pucetaite et al., 2010). In expanding on this point, it may be noted that the presence of healthy, trusting relationships in organisational contexts may increase aspects such as commitment and performance (Singh & Srivastava, 2016). It should, however, be stressed that technology is able to obstruct the social relations formed among colleagues and possibly impede the trust that had been formed. When behaviour is not uniform and is displayed differently in an organisational setting, then the likelihood of distrust may be experienced owing to a significant difference in views.

The fundamental argument that this theme raises through the display of qualitative narratives was that although the interpretations of best practices and management of Internet usage differed, it was able to instil both a sense of vigilance and uncertainty among members of an organisation. Technology in the workplace can thus be both disruptive and beneficial (Cascio & Montealegre, 2016). The findings displayed under the second theme address Sub-theme 2.1: *Vigilance among members of the organisation owing to differences in how cyberspace is approached*, and Sub-theme 2.2: *The uncertainty of cybersecurity best practices and protocols in the organisation*, which reveals the differences in implementing guidelines and how members interpret the limits in practising cybersecurity.

5.5.1 Sub-theme 2.1: Vigilance among members of the organisation owing to differences in how cyberspace is approached

The findings related to the notion of vigilance indicate that the members of the military who were interviewed shared strong views. The derived coding and meaning units showed that members were not inclined to trust the DoD resources supplied to them and would rather use their own technological devices to feel secure. Moreover, aspects of vigilance not only rested with DoD resources, but also in the manner in which information was disclosed to external sources such as the media. In addition, senior military officers interviewed at the SANDC revealed that there were signs of distrust in the organisation’s policies. The challenges emerged from how some members might use DoD resources such as computers, which was considered to be an aspect that required attention from all members of the military and the senior branches of the organisation. It should be noted that, under this theme, six of the 10 participants reported being aware of how their colleagues approached the topic of cyberspace in the organisation. Participant 3, a senior military officer, suggested that junior members might abuse the resources offered to them in the organisational context. This argument fed into the debate that trust might be compromised when military members did not comply with procedures and guidelines. Participant 3 stated:

> *"You see, the measures can be there, but the problem is that the constant monitoring of people will be like 'I don't trust you, DoD members'. The guidelines can be there and the boundaries can be employed so that people can develop. But if the organisation creates guidelines and boundaries and still dictate to its members how it should be used, then the organisation will not grow, because you have no faith in its members and there will be no innovation in the organisation. If the organisation is allowing its members to go to this end and that end ... as long as objectives are met. And that is where you allow the space for people to grow. If it's too restrictive, then officers will think they cannot be trusted, but if you employ the laws and guidelines and allow people to adapt to it, then the organisation and people will grow"* (Participant 3, senior military officer).

Participant 3's excerpt denotes that trust is not present in the organisation, especially concerning the guidelines pertaining to the use of the Internet in the workplace. Participant 3 alluded to the idea that the organisation does not trust its employees to effectively apply the proposed guidelines and rules. It is worth noting that mistrust can be a symptom of other issues that are experienced in an organisation (Camblor & Alcover, 2019; Sitkin & Roth, 1993). Participant 3 pointed out that there was very limited room for growth and innovation owing to restrictive guidelines and mistrust in the organisation. The researcher argues that the restrictive guidelines are positioned to achieve an improved approach to establishing information security and facilitating safe online security behaviour. However, guidelines are also employed to provide oversight over matters related to the early detection of threats and establishing effective cybersecurity behaviour, as well as information sharing. Participant 3's narrative, however, provided a starting point for employee engagement to address issues of mistrust relating to technology use. According to Camblor and Alcover (2019), the engagement of employees in an environment where the sharing of ideas, values, and behaviour is established as a foundation for colleagues may lead to a reduction in incompetence and an increase in cooperation. Participant 3 noted that there was a lack of growth owing to the restrictive nature of how guidelines were employed. It has been confirmed that the DoD has a clear policy relating to the sharing and distribution of information in an instruction titled "Policy, process and procedures on information and communications systems security in the Department of Defence"[29]. The DODI/CM1/00008/2001 (RSA, 2011a) clearly indicates guidelines for using mobile devices in the work environment, but also stipulates the procedures for the storage of organisational information and the security expectations for communicating sensitive information.

In elaborating on this sub-theme, it was clear that differences might exist in how policies are interpreted and complied within an organisation. Participant 5 perceived the process of information sharing as unclear and not "visible". Participant 5 suggested that cybersecurity violations that occur in the organisation should be disclosed. Furthermore, Participant 5 also recommended that those military members who violated the organisation's trust and procedures should be brought to the attention of the authorities. The consequence of violating organisational trust is presented in the following transcribed excerpts of Participants 5 and 10:

> *"I would make it more visible, if people are being caught out for violating certain cybersecurity procedures, it's usually kept quiet, I think we should make it visible and expose those that are violating the organisation's trust and procedures. If military personnel can see those that have loose lips that can sink ships, then surely this will scare them"* (Participant 5, senior military officer).

> *"They should not do it, they should not use a military computer to browse on the Internet because, remember now, as I said, it's easy to hack a computer, especially on the Internet, so they should not do it. And if you do access the Internet, it should be on a computer that has no military information. You should not use any of your details when it comes to logging on to a website because people can draw a profile of you. And they can start to link you with other things so we must be careful how we browse the Internet, but not with a computer that has military information"* (Participant 10, senior military officer).

[29] DODI/CM1/00008/2001, Edition 4, is authorised and issued for implementation in the DoD (RSA, 2011a).

As mentioned in the introduction to the sub-theme *Vigilance among members of the organisation owing to differences in how cyberspace is approached*, the trust factor was not just confined to the exploitation and abuse of organisational resources but might also potentially cause a clash between members regarding how security is approached. Participant 10 also raised the element of trust among colleagues, by stating that state resources should not be abused to browse unauthorised content on the Internet. This vigilance among members could be owing to the implementation of guidelines and directives for information security and the use of organisational resources. Participants 5 and 10's narratives can be interpreted as referring to trust and security. The heart of the issue, as pointed out by these participants, is limited information security. Ritala et al. (2015) note that the process of trust can be influenced positively if there is reciprocity in knowledge sharing among members, although the alternative, where no reward of reciprocation exists, may be considered as a situation that is conducive to information leakage.

Sub-theme 2.1 showed how the participants grappled with existing directives and policies that govern security in the organisation. It was noted that the interpretation of these existing policies presents challenges related to trust and the use of technology. The next sub-theme addresses aspects of uncertainty concerning best practices related to cybersecurity protocols in the organisation.

5.5.2 Sub-theme 2.2: The uncertainty of cybersecurity best practices and protocols in the organisation

This sub-theme emphasises the interpretation of policies and their implementation. When an organisation implements awareness initiatives directed at increasing awareness of information security, greater application of best practices among employees should occur as the risks would already had to have been identified and acknowledged as understood (Al-Mohannadi et al., 2018). A case in point is that some policies and directives might not be reaching all the members of the organisation, as highlighted by Participants 1 and 2, which might result in policies and protocols not being known or understood clearly. It must be noted that eight of the 10 military officers located at the SANDC highlighted that they were not sure of the cybersecurity best practices that were promoted in the organisation. Furthermore, it emerged that a significant amount of time was spent adapting to new policies introduced by senior management. In addition, communication about the regulations concerning information sharing and the security attached to this was an important component in creating a basis for security awareness among members of the organisation. The next two extracts, which appear in sequence, laid an important foundation relating to the availability of information, as well as the understanding of information contained in security policies, which might cause uncertainty or confusion:

> *"… uhm ... and I must admit we have been doing ... as there is a clear absence of communication in the DoD. Uhm, we have systems in place, but [they have] not been adjusted through the times, you understand. This is quick news, quick information, quick sharing, whereas in the old days you had to write a signal, where you first have to prepare the content and go through the editing process and go onto the system by sending out the signal. Uhm, and, yes, we have official phones, but we don't have [an] official network like SETA that will protect us from sharing information …"* (Participant 1, senior military officer).

> *"We have, like, open presentations to everyone in the building about cyberthreats and so on. I am aware of threats, but I have not seen a policy. I think I know what the right thing is to do ..."* (Participant 2, senior military officer).

As noted in Participant 2's narrative, the basis of a policy is that there should be a foundation of knowledge on which the directives and policies are based. Furthermore, the weak link in the cybersecurity chain appears to be the human element. Participant 2 mentioned that there were presentations on cybersecurity threats at the units. However, in terms of the policies directed at achieving cybersecurity, it was acknowledged that a lack of awareness exists. Moreover, Participant 2 suggested that there was a knowledge gap in education relating to cybersecurity and that the organisation could not introduce a directive or policy if the basis of the matter was not understood or why cyber was not regarded as a threat. Researchers have posited that employees are the face of organisations and are at the frontline of protecting the network's security (Al-Mohannadi et al., 2018). For this reason, awareness training should be able to rectify the prevalence of negligence among staff and reduce possible non-deliberate security breaches (RSA, 2011a).

As derived from the interview, Participant 1 perceived the sharing of pertinent information related to cybersecurity as limited in the organisation. Furthermore, Participant 1 suggested that there was disjointedness in the implementation of information sharing as the so-called “new” way of sharing information should be faster and more efficient, as the “old” way emphasised editing and proofreading before circulating a document, but that the current way was not necessarily faster and more efficient. However, DoD directive DODI/CMI/00011/2001 highlights that communication should be easy and confidential (RSA, 2011a). However, the policy does not mention that the communication mode, which is electronic, should be fast and efficient. It should nevertheless be noted that the sending and receiving of information through the use of email is still considered to be a formal means of communication and bringing information to those who have an interest in it (RSA, 2013a). It is worth noting that awareness of best practices goes both ways. The first part of the sub-theme indicated that there was a lack of communication or no communication at all about a security-related policy. Some participants nevertheless highlighted that there was a level of awareness of a policy on cybersecurity and the protection of DoD information. Uncertainty of best practices captured in policy directives related to cybersecurity in the organisation emerged from Participants 4 and 5’s narratives:

> *“Yes, I am aware of such a policy. Uhm, I feel it’s good because there is a big problem with the amount of military personnel using social media and what they post on there as there’s no restriction. There is no watchdog. However, there is an instruction”* (Participant 4, senior military officer).

> *“Yeah, that’s a sensitive issue because I heard there’s a policy out on it. I am of the opinion that you can do that to all soldiers because we are all in this business, but with posing with your uniforms on social media I do not have a problem because I am of the opinion that I am not putting sensitive information about weapons or armoury or things like that online. The fact that I am a soldier, they, the hackers, will in any way pick it up that I am one without my uniform if they hack into a system. The fact that I have a uniform may give an impression that there [are] more things linked to me, so that’s my opinion”* (Participant 5, senior officer).

Participants 4 and 5 were in agreement that there is a policy on best practices related to cybersecurity. However, it appeared that the measures to implement the policies and practices are lacking. A lack of clarity exists about the policies linked to cyberspace-related practices and the threats that might emerge in this space. Participant 4 suggested that military personnel using social media could pose a security risk to the organisation. DoD Instruction DODI/CMI/00008/2001 indicates that there are clear guidelines concerning the processes that military personnel are expected to action when an intentional or unintentional security breach occurs (RSA, 2011a). Participant 5 furthermore appeared to be uncertain about whether posting a military uniform on social media was allowed or not, but acknowledged that doing so could possibly imply some danger to the individual browser or poster of information or photographs.

5.6 Theme 3: The construction of a digital culture among members

This theme contained various perspectives among military officers as to whether there was indeed a culture in the organisation of promoting cybersecurity among its officers. The majority of the participants viewed culture as an important contributing factor when creating an initiative and spreading awareness concerning a topic that is mostly regarded as untouched or unspoken of. It is relevant to note that most of the military officers interviewed admitted to being sceptical about the existence of a digital culture in the organisation. The concept of culture represents ideals, values, morals, and behaviour in a certain environment (Papazoglou, 2019) and may collectively point to the receptiveness of an organisation to embodying a digitalised culture that personifies cybersecurity awareness and behaviour in line with best practices.

Establishing a culture of digitisation remains a necessity when viewing this topic through a 4IR lens. Organisations are confronted with the reality of automation and streamlining of communication. Culture plays an important role in the formation of a digitised environment (Goran et al., 2017). Within the dynamic of culture, the role of behaviour cannot be omitted as it comes with a set of customs, belief systems, and practices. According to Goran et al. (2017), organisations that do not move fast enough to integrate technology will eventually experience challenges arising in relation to the functioning of their activities. Technology places major pressure on organisations in striving to create a culture of digitisation. Moreover, organisations that have traditionally emphasised the physical environment might experience challenges with the integration of technology (Rishi et al., 2008). This third main theme depicts the findings of the study through four sub-themes, namely *Culture of digital security among officers*, *Personal devices are considered more efficient to store organisational information, Cyber increases the skills gap between more senior and junior military officers*, and *The demand for faster and more efficient communication is becoming normalised practice*.

5.6.1 Sub-theme 3.1: Culture of digital security among officers

The findings discussed in this sub-theme demonstrate that the majority of officers viewed the cultivation of a cybersecurity culture as limited. Moreover, six of the 10 participants indicated that the culture of cybersecurity was limited, despite admitting to the need for driving the establishment of a knowledge and awareness system. Cyber awareness emerged as being significant during the coding and categorisation phases of the analysis process. Furthermore, the notion of culture being linked to awareness was evident from Participants 6 and 10's narratives. These narratives identified that a sense of urgency relating to cybersecurity awareness might be regarded as a challenge in the organisation. In addition, urgency as a challenge was revealed specifically during the coding process as the narratives indicated that there was a need for the organisation to improve and accelerate addressing cybersecurity.

The relevant narratives of the participants in this respect are captured in the following extracts:

> *"There is no awareness culture in the DoD about cybersecurity. I would rate it as a 4 out of 10, which is at its worst, because the majority of officers save DoD information on their personal USB [universal serial bus] sticks or email it to their personal accounts and don't worry about whether their emails are hacked"* (Participant 6, senior military officer).

> *"I believe that we don't yet have a culture of cybersecurity in the DoD and awareness in terms of security. I think that is basically in my intelligence environment and it should not be just an idea; it should form part of your lifestyle. Because, remember, now we are in the Fourth Industrial Revolution now, and this revolution, we don't refer to industrial machines, we refer to technology and if you look at technology ... most people are nowadays connected to the Internet. I mean, 80 to 85% of the country are connected to the Internet. I would say that we should be more cybersecurity conscious and make it a lifestyle. That is why, you see, criminals can easily access your bank account. Look at how people can clone your card. I mean, we think it's robbery but actually it's [a] cybersecurity [matter]"* (Participant 10, senior military officer).

Participant 6's narrative implied that there was a need to increase cybersecurity awareness in the organisation and that a potential vulnerability exists that requires attention. This sentiment was corroborated by Participant 10, who concurred that a cybersecurity awareness culture was limited in the organisation. The description by the two participants demonstrated that the components involved in forming awareness comprises various elements. Participant 6 suggested, as interpreted by the researcher, that organisational information should not be stored on personal storage devices such as USB flash drives. DoD Instruction DODI/CMI/00008/2001 directive highlights that no personal storage device may be used to store organisational information (RSA, 2011a). Participant 10, on the other hand, suggested that in order for a digital culture to be constructed, there should be a presence of awareness and a deliberate effort to practise security behaviour as a lifestyle. The explanation included events that were occurring in the 4IR and mentioned the increase in technology that allows the criminal element to exploit user data. It emerged that emphasis of cybersecurity consciousness was required as a matter of urgency. Furthermore, in order for a digital culture to be constructed, there should be a willingness to understand and implement measures to achieve an increase in awareness, while security-aware online behaviour may be able to mitigate risk (Al-Mohannadi et al., 2019; Bada et al., 2015).

Participants 3 and 5 showed through their narratives that they believed a lack of willingness exists to enforce policies and practices that would enable a digital culture in the organisation. Participant 3 noted that some members of the organisation were wary of constant monitoring. Managing some employees more closely than others would delay the construction of an organisational culture that is uniform in its approach to and management of cybersecurity. Participants 3 and 5's narratives are as follows:

> *"You see, the measures can be there, but the problem is that the constant monitoring of people will be, like, 'I don't trust you, DoD members'. The guidelines can be there and the boundaries can be employed so that people can develop. But if the organisation creates guidelines and boundaries and still dictate to its members how it should be used, then the organisation will not grow, because you have no faith in its members and there will be no innovation in the organisation. If the organisation is allowing its members to go to this end and that end as long as objectives are met ... that is where you allow*

> *the space for people to grow. If it's too restrictive, then officers will think they cannot be trusted, but if you employ the laws and guidelines and allow people to adapt to it, then the organisation and people will grow"* (Participant 3, senior military officer).

> *"I think the information security in the organisation is bad and I don't believe that there is a culture around it. I think if you don't make an example, it will continue to go the same way"* (Participant 5, senior officer).

Participant 3's narrative indicates that in order for a digital culture to emerge, there should also be space for members to grow and be innovative in their approach to safety and adhering to guidelines. This was contributed by a senior officer who provided the narrative from personal experience. The researcher interpreted this as meaning it was likely that, owing to the younger members being more efficient when it came to incorporating and using digital technologies, this form of monitoring could be a challenge, especially when older methods of securing information are regarded as the official means to do so.

This sub-theme made reference to the features of a digital culture in an organisation. The participants noted that aspects relating to the construction of a digital culture in the organisation remained a challenge. As many as eight of the 10 participants agreed that a digital culture focusing on cybersecurity required more attention from management. Based on the coding process of this study, the researcher recorded that members were dissatisfied with the existing digital culture in the organisation.

5.6.2 Sub-theme 3.2: Personal devices are considered more efficient to store organisational information

In this sub-theme, the emphasis is on the use of personal devices that were more efficient than the devices provided by the organisation. It should be emphasised that using a portable device may increase the chances of physical loss (Walters, 2012). This sub-theme built on the narratives supplied in Sub-theme 3.1 and contributed to the context of understanding the construction of a digital culture that was receptive to technology and the change it might be able to bring about. It is worth noting that six of the 10 participants argued that personal devices were more efficient to use in the office than the devices supplied by the organisation. The use of the computer devices supplied by the organisation was distrusted by the interviewed participants as some believed that the devices were not secure and plagued with viruses, which might cause a loss of information and damage to a military officer's storage device. Participant 1 highlighted the following regarding computer devices used by the organisation:

> *"But to make sure that there is a computer standing alone somewhere in the building to access emails and have access to the Internet remains important, yet the computers in the DoD are so full of viruses there ... in the Internet ... there at, uhm, LIW [that] the MSDs used ... and if you unplug your memory stick there, you should first run it through your laptop's virus protection software. The virus protection program on the work computer is not regularly updated, namely McAfee. I use a different virus protection program, which I purchased out of my own pocket. During December it cost me about R1 000 to save my butt"* (Participant 1, senior military officer).

> *"Right now there is no best way as we communicate sensitive information through WhatsApp for the purpose of our day-to-day military activities. We have been cautioned ... uhm ... we want this type of information to be in the public domain. But there is no other way as the old methods of doing things; the old methods of using the filing system and using the fax machine. We are all in a new era now and it doesn't work as we need to get information to others much quicker"* (Participant 2, senior military officer).

The evidence derived from Participant 1 shifted the focus to the perception that organisational computers are not trusted as they often have viruses. Moreover, this participant also took extraordinary measures by purchasing antivirus software that was more secure than the DoD-supplied software for the devices allocated for use by members. It should be noted that DoD Instruction DODI/CMI/00008/2001 condemns the use of external software that is uploaded on DoD devices as this contravenes the protection of DoD-sanctioned software and hardware used for securing information in an efficient manner (RSA, 2011a). In this extract the participant furthermore implied experiencing a lack of trust, and therefore used personal devices as efficient storage methods as the organisation's computers were plagued with viruses. This could potentially also be viewed as a lack of confidence in the organisation. Participant 2 argued that the current methods are outdated and that personnel require more responsive and efficient means of transmitting DoD information. Adding to Participant 2's view, it was highlighted that there was a need to communicate DoD information through social media platforms, which are much faster in transmitting information. Based on this view, it is clear that personal devices might be used as a mode through which information is relayed.

Furthermore, the aspect of viruses on organisational computers suggested that performing regular maintenance is a challenge, which also contradicted the notion that computers receive servicing and updating on a regular basis. This situation might be referred to as the BYOD phenomenon in organisations as participants use their own devices in order to complete certain tasks (Yeboah-Boateng & Boaten, 2016). Thomson (2012) and Gökçe and Dogerlioglu (2019) believe that employees bring their personal devices, which possibly have new capabilities, to work with as they are considered more efficient than those of the organisation. In addition, newer devices are able to allow employees to feel more comfortable and be more productive (Mitrovic et al., 2014). Participant 3 shared the sentiment that the organisation could not supply everyone with laptops or desktop computers given the economic challenges connected to doing so. In the narrative, Participant 3 argued:

> *"You know, at this stage I believe that they are critical because that is the easiest way of sharing information, eh. For example, if you look at the resources that we have in the DoD, we are unable to secure a laptop for each and every individual. But now we can't say no more USBs to everyone [who] has got a laptop to store information. With the economic conditions we find ourselves in, it's going to be hard for us to reach that goal. Now, as a compromise, a guy can come and say, I've got a laptop at home; I can take this information and work at home, and you want to deliver on a specific timeline and in that situation you are compelled to allow this individual to take the information home and complete the task"* (Participant 3, senior military officer).

In interpreting Participant 3's narrative, it became clear that challenges exist with the procurement and supply of computer devices to every DoD member. This situation evidently poses a major challenge for the organisation as tasks are required to be completed timeously. In reference to the argument in Chapters 1 and 2, it is relevant to confirm that military members are not isolated from civil society as they share some similar values and qualities (Heinecken et al., 2005). They are thus equally exposed to threats and vulnerabilities, including cyberthreats. This argument may be coupled with the notion that society embraces technology and, in addition, more of the individual's daily activities require the use of technology. Viewing the extract from Participant 3's narrative in context, it should be stated that the organisation might indeed experience challenges if it does not prohibit its members from utilising personal storage devices or devices that might be used to support the completion of tasks more efficiently. The researcher thus argues that the greater the importance attached to cybersecurity awareness training, the more aligned it could be to an organisational culture that embraces technology. Participant 9's perspective might not necessarily be helpful from the viewpoint of securing information in the organisation effectively. The extract nevertheless exposed how information has been treated with a complete absence of security.

> *"Just my memory stick, but what I have done in the past is, and I think it was a habit, I started doing and saving my work on the H drive, which is backed up, but now, if you don't have a copy of your work on your C drive, and the H drive is down, then you can't work. So in the past I have been able to work because I primarily work on my C drive because what do you do now, and I think this is illegal but it saved my bum a few time[s], but I make copies of my work and save it on my hard drive and then I leave a copy of that at home and that also enable me, when a general contacts me, to provide him with the documents at odd hours because of access to the military servers or drives, or when the systems are down, I have a copy. It has its positive side, but has a risk. Can you imagine they break into my house and they steal that information? There are a lot of copies of ID[s] and number[s] for applications, sensitive information, and CVs. Okay, but luckily I don't have it anymore, because I'm not in charge of it anymore"* (Participant 9, senior military officer).

Participant 9's statement made it clear that personal devices are used as a means to store sensitive organisational information. The motivation for doing so was explained by Participant 9 as that the storage mechanisms of the organisation could not be depended on. Instead, the participant noted that physical means of making copies of sensitive data and storing data on personal storage devices were more dependable.

Furthermore, the participant acknowledged that he did not store information on his personal devices anymore due to not being in a leadership position that demanded managing sensitive information. The next section focuses on the role of cyberspace, and the skills gap between senior and junior officers.

5.6.3 Sub-theme 3.3: Cyber increases the skills gap between more senior and junior military officers

Technology and its availability are increasing; it is therefore becoming very firmly rooted in people's lives. Consequently, it is important to acknowledge differences in the form of behaviour as different approaches to wellbeing, innovation, and organisational citizenship might arise among the workforce (Becton et al., 2014). This sub-theme focused on the role of technology and how it may have widened the skills gap between members of the organisation. The previous sub-theme, *Personal devices are considered more efficient to store organisational information*, made reference to the use of technology by military members and their preference for more efficient devices and storage tools to facilitate doing their work. In addition, six of the 10 military officers interviewed at the SANDC suggested that cyber increased the gap between senior and junior officers. The reason for this perceived skills gap could be due to the groups' varied outlook on the construction of security and the use of cyberspace. It is relevant to note that the amount of exposure to cybersecurity knowledge allows an individual to incorporate complex security behaviour in their everyday functioning (Zwilling et al., 2020). The remaining four participants were of the view that the organisation uses cyberspace but made no reference to seniority in relation to skill in matters attached to cyberspace or a perceived gap between groups of members.

The current sub-theme revealed how senior officers perceive junior officers. In addition, narratives focusing on how technology is approached were highlighted in this sub-theme. In order to contribute to placing this sub-theme in context, Mannheim (1952) suggests that the aspect of "generation" relates to facets of identity, location, and age groups that are entrenched in a progression of a historical-social nature. Participant 3 declared that younger officers are more likely to use technology in the workplace. This participant's narrative also focused on the accessibility of awareness material such as bulletins, which would defy the need for quick and efficient ways to address cybersecurity education and enhance the construction of a digital culture in the organisation.

Moreover, Participant 3, for example, also highlighted the emphasis on the difference between generations and ranks:

> *"Yeah, you know, the measures that we have are traditional measures and not in line with technological advancements, and policies are outdated. When I worked in a different environment, that is when I first realised that an IT qualification is something serious. You know we had [these] young guys working there with this qualification and what I noticed was that we cannot cope with this current scope of digital awareness and cannot cope with these guys"* (Participant 3, senior military officer).

This sub-theme was important to understand how a digital culture has formed among members and the extent to which aspects relating to technology had already been integrated in the organisation. Furthermore, the aspect relating to awareness in this sub-theme is also relevant. Participants 1 and 7 indicated that they believed that the senior management in the organisation were not aware of cybersecurity threats that might be experienced and that all members should embrace cybersecurity awareness. However, given that the participants preferred to use their own personal devices, as noted in the previous sub-theme, *Personal devices are considered more efficient to store organisational information*, cyber awareness must be regarded as important. Senior management must therefore not be out of touch with cybersecurity threats.

The following narratives, obtained from Participants 1 and 7, focused on the role of seniority. What emerged was the difference in perceptions between younger officers and senior officers and their outlook on cyber, along with the use of technology. Moreover, the perceived gap might also imply that certain officers limit their interactions with cyber. It therefore appeared that this perception might be driving a wedge between those who are more familiar with cyber and technology and those who are not fully aware of the dangers associated with cyber and technology.

> *"There is a culture, but whether we follow the rules and guidelines is another story. Often commanders do not exercise or implement these guidelines and it*

> *should be from the bottom [up] so that NCOs are also aware of the dangers and threats”* (Participant 1, senior military officer).
>
> *“The top structure of the DoD are not aware of the dangers that the officers are experiencing. I believe that they are confused. But we are also not excused from this as our officers are also responsible for finding out about cyberattacks and security”* (Participant 7, senior military officer).

As derived from the comments by Participants 1 and 7, aspects relating to the implementation of awareness measures and the associated culture seem to present a challenge to senior management. These views were those of senior officers and the excerpts indicated a much deeper underlying issue that did not necessarily rest with the individual but with the broader organisation. In addition, the Defence Review (RSA, 2015a) reflects that cybersecurity is one of the main aspects of importance to the organisation, in which awareness creation is considered a priority. The interviewed members did not necessarily believe this to be a priority, as shown in the results related to best practices, presented in Sub-theme 2.2, which underlined the uncertainty of best practices in cybersecurity protocols. It should be highlighted that the values and the rationale of an organisation also determine how awareness and management practices concerning cybersecurity facilitate the construction of a mature digital culture among all members (Al-Izki & Weir, 2016; Barton et al., 2016). Moreover, the next excerpt also deals with the aspect of education and awareness, and how senior officers view junior members. Participant 8’s narrative placed this view in context with regard to education in particular:

> *“I think it all comes down to education, uhm. Let’s take the lower-ranking guys and they are on social media and skipping and all these things are* lekker[30]*, and they don’t always think twice before putting information online. Yeah, and I just think they need education”* (Participant 8, senior military officer).

The current sub-theme focused on the role of cyber and technology and how these factors appear to be capable of causing division between military members of different seniority in rank. It is apparent from Participant 8’s comment that lower-ranking military

[30] The word *lekker* refers to an act that is enjoyable or pleasant (*Collins Dictionary*, 2022).

members are not taking online security practices seriously. The next sub-theme focuses on the demand for faster and more efficient communication.

5.6.4 Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice

The last and final sub-theme in this section emphasises the increased need for information to reach recipients more quickly and more efficiently. Eight of the 10 military officers interviewed reported that there was greater emphasis on using social media platforms as an alternative to redundant channels of communication. The transmission of sensitive information on digital platforms may not necessarily be secure as malicious software may target both recipients and senders (Almara'beh et al., 2016). The DoD has issued a directive that highlights the transmission of organisational information that addresses the aspects of protection, controlled access, and assurance of protection (RSA, 2011a). One of the aspects that became apparent in this sub-theme was the tendency of military officers to use third-party applications such as WhatsApp or other forms of social communication platforms. What this means is that users sign up for and comply with regulated terms and conditions when using certain digital platforms; thus, when users share personal data, it enables algorithms to develop a digital footprint (Adjei, Adams et al., 2020; Adjei, Pearl et al., 2020). This digital footprint allows for traits and attributes to be linked to individual users, which ultimately creates an identity in information systems (Adjei, Adams et al., 2020; Adjei, Pearl et al., 2020). Nevertheless, social media platforms such as WhatsApp were identified by Participants 3 and 10 to be most efficient in terms of expediting communication. The excerpts of Participants 3 and 10 are presented as follows:

> *"... although WhatsApp is a quicker way to receive information, especially when I'm out of town and where I cannot send emails, I mean it's a quicker way to send and receive information. My issue is that it's not regulated or internalised. Remember when the cellphone came in, there was a policy on how to manage information on how to use it"* (Participant 3, senior military officer).

> *"Yes, there are people in units that use these software and applications, but they do so because it's a cheap and easy way of communication. My view on*

> *that is, and I say we having a meeting tomorrow, and they don't consider that sensitive or whatever, then it's okay, but if your borders have been breached and we are under attack, then information cannot take place over WhatsApp. So you cannot share sensitive information over social media like WhatsApp. Rather small things like to communicate a meeting or starting time of work the next day ..."* (Participant 10, senior military officer).

The aforementioned participants' narratives denote the practice of using social media as ways to bridge the gap between information and communication efficiency. These participants suggested that WhatsApp was more efficient than the official means of communication in the organisation. However, this type of communication comes at a cost as users' privacy and personal information may be at risk owing to the proposed updated WhatsApp policy (Jacobs, 2021a; 2021b). In expanding on this, the application of communication through WhatsApp as a platform can be seen in Participant 9's narrative:

> *"When I am looking for specific information, for instance, it has happened when you are drafting a letter within a short time space and that letter must go to somebody, but you [are] not sure where the signature block should be and how it should look like, and then you phone somebody in that environment and ask that person to take a photo of a letter and send it to me as an example"* (Participant 9, senior military officer).

The excerpt above represents the participant's view regarding the application of online behaviour when using WhatsApp as a means to communicate. From this perspective, it is clear that the participant viewed some of the administrative aspects as challenging and preferred a more efficient means to communicate, confirm procedure, and relay information. WhatsApp was noted as an effective way to communicate, although there are certain SANDF directives that prohibit WhatsApp as an official communication tool to pass on information.

5.7 Theme 4: The view on cyberthreats is constructed based on experiences in the physical domain

This theme focuses on the construction of threats based on prior experience of the physical domain. What this means is that users often migrate their personal experiences and adopt the same measures in a different space. For example, a user might have been a victim of cybercrime and afterwards applied a more stringent belief and behaviour system when using the Internet. Such an individual's information-sharing practices often also change after a loss, usually in the form of money. Users may thus see this space as potentially hazardous to their wellbeing (Moustafa et al., 2021).

Understanding challenges and having experienced cyberthreats are said to have an impact on how security behaviour is exercised (Moustafa et al., 2021). Perception is believed to be the main lens through which individuals evaluate their personal environment (Huang et al., 2010). Theme 4 drew on the participants' narratives to show how the experiences of members were able to influence cybersecurity practices, and included two sub-themes. The first of these sub-themes was *Information security as a practice*, which dealt with the issue of how security as a practice is constructed and applied through behaviour in an organisational and personal setting. The second sub-theme was *Perception as an important aspect to military members*. This sub-theme showed how military officers perceive the public and how the organisation and its members are in turn viewed by the public. The second sub-theme also highlighted the perceptions of members of their own organisation. The frequency with which the codes were repeated in the analysis procedure revealed that the code "access to information" appeared nine out of 10 times during the analysis of Sub-theme 4.1. The first sub-theme was thus regarded as significant. The second sub-theme revealed that nine of the 10 participants demonstrated a level of wariness concerning the way that members perceive one another.

5.7.1 Sub-theme 4.1: Information security as a practice

Information security in this section deals with the notion that resources and tools are used to secure the organisation's information. This sub-theme also related to the behaviour of the participants in the workplace and their approach to managing digital security. In this sub-theme, the excerpts of Participants 1, 6, and 10 are presented to indicate the lack of direction associated with the execution and application of cybersecurity guidelines. Moreover, this sub-theme contributes to the main theme, which emphasises that cyberthreats are constructed as they are based on experience. Secondly, the sub-theme reveals the participants' information on security awareness as a factor that contributes to the current demeanour of military members with regard to security behaviour. It is important to note that nine of the 10 senior military officers indicated that they practised information security through either being aware of cyberthreats or applying security guidelines through behaviour. The codes "information security", "DoD software", and "access to information" were grouped under this sub-theme. Participants 1, 6, and 10 argued that information security was of key importance when navigating cyberspace. The following three excerpts denote the security behaviour applied to both organisational and personal contexts:

> *"You know, from a personal point of view, the nature of my information might be very personal for me so, for me, uhm, I am aware of the dangers and consequences in going onto an open Wi-Fi network and, uhm, I tend to ignore the security risk to myself, but within the security domain I find myself [in], I tend to be cautious when around those networks with my work hardware"* (Participant 1, senior military officer).

> *"I would change my passwords once a month, but I would use the same one for all my accounts and devices. It's been like this for years because if you check my Facebook, WhatsApp, Twitter, or banking details ... are all the same. In my personal capacity, I am weak, hey, because most of my passwords are the same throughout the bank and social media. There are loads of sites so I prefer to have one password for all my things"* (Participant 6, senior military officer).

> *"Uhm, if you lock it in a safe, uhm, then it depends who has access to that safe, you see. I think that there needs to be a central point. It can either be locked in a unit level or counter-intelligence office or officer commanding or your staff head if it's in an admin or staff environment at your higher headquarters. But it should not be that everybody has got access to that mobile device or memory stick of some sort to store sensitive information. There should be one access point to that document and it should be locked in a safe, totally sealed in an envelope for safekeeping"* (Participant 10, senior military officer).

Participants 1, 6, and 10's narratives highlight that the way that information is treated is of key importance for security. Participant 1 emphasised that in his professional capacity he regarded information security as a practice more seriously than in his personal capacity. This could be the case as information security is an important factor in the organisation and would be regarded as a critical component in maintaining national security. Furthermore, Participant 6 mentioned that he used one specific password for all social media platforms, including banking platforms. Participant 6 also indicated that official passwords were only changed once a month, which is indicative of security awareness about potential threats. The challenge in a situation such as this would be when a user utilises the same password and safety protocols on all devices. In this context, if the organisation supplies members with devices and they are taken home, as noted in the sub-theme *Personal devices are considered more efficient to store organisational information*, then it might compromise the safety of the information on that device. Participant 10 believed that accessing information in the organisation could be done using a central location. Apart from accessing information at a central location, it is important to note that access to specific software might enable users to practise security in a digitised environment and also maintain security.

5.7.2 Sub-theme 4.2: Perception as an important aspect to military members

This sub-theme addresses the importance of perception. By showing the narratives of the participants through text, it is possible to indicate how this sub-theme connects to the overarching theme of this study, which sought to explore the perceptions of cybersecurity among South African military officers. Perception is an important precursor to predicting the potential response to issues, but might also be a reflection of the behaviour that is exhibited (Saban et al., 2021). Saban et al. (2021) note that as perceptions related to information security increase, awareness of and dedication to upholding security also increase. However, when challenges related to implementation are experienced, they may decrease awareness of and dedication to maintaining information security in an organisation. Moreover, the role of perceptions in organisations is important for understanding how employees are able to respond to change, roles, and shifting social identities (Saban et al., 2021). With cyber now also being considered a domain of warfare, which stretches across traditional domains such as air, land, sea, and space, the need for an altered approach to security in a digital space is equally important. Organisations that fail to adapt to change and introduce mechanisms to enhance their employees' flexibility towards change may find themselves under increasing pressure (Armenakis & Bedeian, 1999). It should be highlighted that seven of the 10 senior military officers interviewed regarded public perception of the organisation as important. Viewing the narratives of the members interviewed, it was possible to draw upon certain perceptions that might give an idea of how cyber is approached. Participants 5 and 9's narratives include arguments why public perceptions of the government are important:

> *"Currently, yeah, uhm, I don't think there is good control over it. I just think there are people posting on the DoD web and there's undisciplined comments being made and stuff. So, I think it can be a big threat in general and I do believe that most people are not very secure. We know about the dangers, but I don't think we are doing enough. I have the ability to access my phone and laptop with my thumb scanner, but now I am thinking I should have actually applied it and I haven't"* (Participant 5, senior military officer).

> *"Uhm, I don't think people are aware of what they should be doing and how they should treat information; for instance, the in thing as of late is, when you get a signal, you take a photo and send it to your colleague via WhatsApp, though WhatsApp is encrypted. But the thing is, once the information is out in the public domain, it's public knowledge and with the right software you are able to access that information. I often think that one should rather leave your cellphone at home or in your car so that you are not tempted. And I think that we are checking our messages and communicate with [one] [an]other through WhatsApp every single day"* (Participant 9, senior military officer).

Based on these two narratives, it was evident that Participants 5 and 9 thought that information-sharing practices were not sound. Furthermore, Participant 9 indicated that secure information-sharing practices were lacking and that sensitive information was shared on online social communication platforms such as WhatsApp. The other four senior military officers who suggested that perception was not important were of the general view that the SANDF should be an entity where the dissemination of potentially sensitive information to the public remains restricted. In addition, it emerged that information can be accessed through pictures that are taken to share critical signals through a third-party platform. This narrative is of key relevance to understand that information is accessible to the public and can potentially create a negative perception of the security mechanisms used by the organisation to communicate, and it should therefore be noted that it appears to be essential to secure sensitive information.

In addition, Participant 4 also made reference to information sent through social communication platforms such as WhatsApp not being confined to one specific location but rather directed to the organisation's data bank. Expanding on this notion, the next comment by Participant 4 was in line with the abovementioned opinions that emerged from the narratives. Participant 4 suggested the following:

> *"We share too many things in the organisation and a lot of information is founded on rumoured information, but usually where there's smoke, there's fire. So we disclose information more easily. A lot of military information is shared with civilians and the next moment this information is in the newspapers and blown out of context"* (Participant 4, senior military officer).

Participant 4 made reference to information-sharing practices and held the view that information was shared too easily and without the proper mechanisms in place to safeguard communication. The participant also alluded to the practice of sharing information with civilians. Some participants were also of the view that information could be shared online and with civilians as long as it did not pertain to sensitive operational activities.

Regarding perceptions, Participant 10 pointed out their importance in information sharing to members of the organisation:

> *"In actual fact, it should be a lifestyle. They should not only be informed; they should live it. For example, if I take a picture of one of my colleagues and put it on social media, what perception are you creating to the general public about the South African soldier? But, if I innocently put something online where we as soldiers are singing, then the perception will be on the outside, look at these soldiers; they are dancing and singing. Should they not be drilling, for example? So it creates a total[ly] different perception. We saw during the Armed Forces Day, where the sergeant major brought the guys to attention, and some of them were just standing around. That says to me there's no discipline, you see, and that's the perception that is created. People create their own perceptions on social media but also internationally, how other armed forces are viewing the South African soldier"* (Participant 10, senior military officer).

Participant 10 indicated that managing information should be a lifestyle and that it should be integrated throughout the organisation. Social media is perceived as a space in which individuals should navigate carefully, as Participant 10’s narrative shows. Furthermore, this participant referred to a video clip that captured the members of the military standing around instead of coming to attention when instructed to do so. This video clip was circulated on social media platforms after a certain Armed Forces Day event. The perception of the organisation on the outside was clearly equally important to the participant, as they suggested that civilians’ perception of the SANDF could be poor. Moreover, the international perception by foreigners of the organisation was also pointed out as a security risk as the circulated video apparently showed that there was very little discipline in the ranks. Linking the participant’s narrative to the possible construction of cyberthreats, it should be stated that perceptions could have an impact on the measures that could possibly be implemented in the organisation.

A challenging aspect that had been dealt with throughout the analysis of the sub-theme was the code “vigilance”, which featured prominently in the interview data. The participants acknowledged that perceptions regarding securing of information were seen as a challenge that needed to be revised. As recorded, if the overall perception is that there is a lack of seriousness about implementing cybersecurity measures and that cyber awareness training is necessary, the likelihood exists that the perceptions of information security would not be considered as important by some members of the organisation.

This sub-theme ultimately drew on a social process that had a “domino effect”. If there was a challenge with implementing awareness mechanisms among the top structure, then members lower down the ranks probably would not consider it as important. The disclosure of potentially sensitive information to the public and the lack of compliance with existing directives are thus symptoms of a larger organisational void in cultivating awareness and cannot be isolated to individual participants in the study.

5.8 Summary of findings

The primary aim of this chapter was to determine what influences perceptions of cybersecurity and how they influence the organisation relating to the sharing of information in a digital space and the level of awareness that constitutes best practice.

In relation to the third secondary research question, which focuses on cybersecurity awareness, the responses showed that not all military officers were in agreement about the idea that awareness was needed in the organisation. In addition, some of the dominant responses showed that senior officers located at the SANDC were aware of cyberthreats. Four main themes emerged from the analysis process:

5.8.1 Theme 1: Knowledge production and training focusing on cybersecurity awareness

Two sub-themes emerged from Theme 1, namely *Awareness and knowledge of cyberspace and its associated dangers* and *The establishment of cybersecurity awareness among military members*. Cybersecurity education for all members was also a code indicated in Sub-themes 1.1 and 1.2. These sub-themes focused on the construction of cybersecurity awareness among South African military members located at the SANDC. It was noted in the qualitative narratives that some members challenged the concept of creating awareness among all members in the organisation, although it was captured in Sub-theme 1.2 that the organisation should consider implementing and introducing cybersecurity awareness training for all members of the organisation, from the bottom up. This is of key importance for the attempt to produce knowledge of cybersecurity awareness in the organisation. These two sub-themes captured the views of military officers by identifying the gap in training in a technological age, where knowledge and awareness are essential for understanding the damage that could be inflicted through cyberspace.

5.8.2 Theme 2: Challenges of trust with technology and members

This theme focused on challenges related to trust in technology and members. Theme 2 had two sub-themes: *Vigilance among members of the organisation owing to differences in how cyberspace is approached* and *The uncertainty of cybersecurity best practices and protocols in the organisation*. The second theme addressed the unique challenges members face in the organisation, which can be linked to the construction of cybersecurity and the efforts to implement this. The codes “trust in one another” and “trust in technology” emerged from the analysis process and were formulated in a subsequent step as a sub-theme that formed part of Theme 2.

5.8.3 Theme 3: The construction of a digital culture among members

In this theme, the focus was on the individual in the armed forces and how they were able to integrate technology in their day-to-day organisational duties. Theme 3 had four sub-themes. The first sub-theme, *Culture of digital security among officers*, showed that the digital culture in the organisation needed to be developed. The creation of awareness initiatives is therefore seen as a challenge and that it would require additional effort to promote a space where technology is accepted and secured. Sub-theme 3.1 captured the essence of a digital culture among members and provided a glimpse into how senior members viewed this in relation to the organisation. The second sub-theme, *Personal devices are considered more efficient to store organisational information*, focused on the idea that personal devices are seen as more efficient to store organisational information. Sub-theme 3.2 indicated that members are more inclined to use their personal devices as a means to store information, but also that sharing the information is much faster as a result. The code "personal devices" became apparent several times in the analysis process and could consequently be linked with this specific sub-theme. The third sub-theme, *Cyber increases the skills gap between more senior and junior military officers*, focused on how cyberspace use advances the skills gap between senior and junior members. Sub-theme 3.3 essentially drew from the way that senior members perceive younger military members relating to their efforts to secure information in practice, as well as how comfortable younger members are with technology. Based on the findings and codes that emerged from the data derived from Sub-theme 3.3, it should be highlighted that a gap was identified between senior and junior members. The fourth sub-theme, *The demand for faster and more efficient communication is becoming normalised practice,* focused on the demand for faster and more efficient communication, which is becoming normalised practice. It emerged that there are no clear guidelines on the use of third-party open-source platforms such as WhatsApp. In addition, senior members also use social media platforms to convey sensitive information. This behaviour is therefore not limited to junior members.

5.8.4 Theme 4: The view on cyberthreats is constructed based on experiences in the physical domain

This theme connects with the second secondary research question of this study as it conveys the perception of cybersecurity. Two sub-themes emerged from this dominant theme. The first sub-theme focused on *information security as a practice*. This was followed by Sub-theme 4.2, which focused on *perception as an important aspect to military members*. There was a focus on perceptions and how practices could be linked to information security. The participants confirmed feeling that information practices in the organisation were a challenge, which was suggestive of the trend in other sub-themes presented in this chapter. There is also an element of consistency in what emerged from the narratives. Sub-theme 4.2 gauged perception as an important aspect to military members, which was regarded as valuable as it indicated systemic organisational challenges. The measures employed to highlight cybersecurity awareness were impacted by the perceptions of the respondents of technology and the construction of threats. Sub-theme 4.2 thus drew on elements that could help provide insight into the broader systemic issues relating to the construction of security and how these perceptions are impacted.

5.9 Conclusion

This chapter focused on presenting the findings of the qualitative interviews, which focused on senior military officers enrolled for a professional military course at the SANDC. The findings were presented in line with the study’s secondary research questions. One of the key findings that emerged from the qualitative narratives was that the participants considered training and education to be of key importance in creating cybersecurity awareness. It was also revealed in Theme 1 that in order to create awareness across the organisation, all South African military members require training in cybersecurity. What also emerged from the narratives was that some participants were vigilant about how other military members used cyberspace and applied their security behaviour. Theme 2 revealed that there were some participants who viewed the organisational guidelines on cybersecurity as not being clear. It was also evident from the narratives in Theme 3 that there was a demand for more efficient technological tools in the organisation. However, from the excerpts it was noted that the use of personal devices might place the organisation’s information at risk. Theme 4 revealed that cybersecurity behaviour was impacted by experience to threats and knowledge of the subject matter. In addition, the perceptions of participants regarding organisational practices related to securing and communicating information were presented. The ease of communicating organisational information on social media platforms was questioned by the participants.

This chapter presented the narratives of 10 participants located at the SANDC. The findings presented in this chapter allowed for the construction of scale items and dimensions of the COQ, which were important for Phase 2 of the study. The themes presented formed the foundation for the quantitative findings in Chapter 6 (see Appendix S). The codes extracted during CA was used to inform the scale items of the COQ in Phase 2. The codes used to inform the construction of items were presented in Chapter 4 (see Section 4.8.1.3). These codes, along with the themes presented in this chapter, formed the basis of the four dimensions and scale items for the questionnaire used in Phase 2 (see Section 4.8.3).

The chapter that follows presents the findings derived from the COQ, which focused on SAMA and the SANWC.

CHAPTER 6:
PHASE 2: DESCRIPTIVE AND THEMATIC ANALYSES

6.1 Introduction

This chapter contains a discussion of the perceptions and contextual realities, which were derived through the COQ, of South African military officers in the SANDF. The findings in this chapter moreover play an integral part in the triangulation process of the study, as referred to in Chapter 4. This chapter consolidates the findings determined by the dimensions of the COQ and the themes that emerged from the short narratives. This forms the basis of the triangulation, which combines both the quantitative and qualitative findings presented in Chapter 7. The information in this chapter achieves a consolidated view of the perceptions of cybersecurity among selected South African military officers. The COQ focused on gauging the SANWC and SAMA participants' awareness[31] of cybersecurity and not necessarily their level of knowledge of cybersecurity. Furthermore, the researcher thematically analysed the short questions in the COQ and separated the quantitative results of the COQ into two sections according to the relevant military organisation, namely SAMA and the SANWC. SPSS version 24 (IBM Corporation, 2016) was utilised for the quantitative analysis of the COQ. The qualitative results of the COQ, however, combined the results obtained from SAMA and the SANWC. The reason for this was to display the results of the two different data-collection sites clearly.

The objectives of the study, as previously presented, outlined three specific research questions that guided the quantitative and qualitative analysis of the COQ. This chapter seeks to answer the three secondary research questions by way of presenting the COQ scale items and short narrative responses. These three secondary research questions are as follows:

1) How do South African military officers conceptualise cybersecurity awareness?
2) How do South African military officers perceive cybersecurity threats within the SANDF?
3) What are the perceptions of cybersecurity awareness through the lens of the military officer?

[31] The researcher focuses on awareness as it pertains to participants' perceptions, views, and feelings towards events or objects. In the case of the COQ, dimensions were created to explore their awareness of cybersecurity and not their level of knowledge, which may refer to their exposure to education and facts on the subject matter.

6.2 Results derived from SAMA

6.2.1 Demographic information

This section presents the demographic information relating to the SAMA sample. The display and interpretation of the demographics are an integral part of the argument put forward in this study. The display of demographic information is important as it allows for a basic view of the characteristics of the SAMA sample. In addition, the demographic information assists with providing further information about the context of the selected sample population, in particular the younger generation.

Table 6.1: Ethnicity of selected military officers at SAMA

Ethnicity	Frequency	Percentage
African	94	83
Coloured	6	5
Indian	1	0.9
White	9	8
Other	2	2
Total	**113**	**100**

Table 6.1 indicates that the majority of the respondents who answered the questionnaire were African (83%), a very small percentage were Indian (0.9%), and only six individuals were coloured (5%). In addition, only nine (8%) white respondents completed the questionnaire. Two respondents preferred not to disclose any information concerning their ethnicity.

Table 6.2: Gender of selected military officers at SAMA

Gender	Frequency	Percentage
Female	38	34
Male	67	59
Missing value	8	7
Total	**113**	**100**

The data displayed in Table 6.2 indicate that the minority of the respondents were female (34%) and the higher percentage male (59%). It appeared from the results that eight respondents preferred not to disclose information related to their gender as the questionnaire did not explore respondents' views on gender. The researcher rounded these percentages off, and the relationship was a very broad representation of the distribution of male and female in the greater SANDF.

Table 6.3: Arms of service of military officers located at SAMA

Arms of service	Frequency	Percentage
SA Army	66	58
SAN	24	21
SAAF	15	13
SAMHS	4	4
Missing value	4	4
Total	**113**	**100**

Table 6.3 indicates that the majority (58%) of the participants were in the SA Army. Furthermore, the second highest number of participants (21%) were in the SAN. The third highest number (15%) were in the SAAF. Military officers from the SAMHS were the smallest group (4%) to complete the questionnaire. Moreover, four respondents did not disclose their arms of service. The low numbers might be an indication of the student intake for that specific cohort, in which a minimal number of students from the SAAF and SAMHS were enrolled. The researcher concluded that the SAMA sample's composition possibly reflected the general composition of the SANDF in that the SA Army is the largest component of the SANDF, followed by the SAAF, the SAN, and finally the SAMHS.

Table 6.4: Rank of military officers at SAMA

Rank	Frequency	Percentage
Lieutenant Colonel	1	1
Captain/Lieutenant (SAN)	4	4
Lieutenant/Sub-Lieutenant (SAN)	62	55
Second Lieutenant / Ensign	11	10
Midshipman / Candidate Officer	33	29
Missing value	2	1
Total	**113**	**100**

Table 6.4 shows that the majority (55%) of the participants held the rank of Lieutenant and Sub-Lieutenant. Midshipmen and Candidate Officers are equal in rank in the different arms of service; the ranks Midshipman and Candidate Officer were therefore combined. A total of 29% of the participants were Midshipmen / Candidate Officers. Only 10% of the participants identified themselves as holding the ranks Second Lieutenant and Ensign. These ranks were also combined owing to their equal status in their respective arms of service. The rank Captain or Navy Lieutenant comprised a minority of 4%. The rank Captain in the SA Army is equal to Lieutenant in the SAN. These two ranks were therefore also combined. Moreover, 5% of participants held the rank of Ensign. One Lieutenant Colonel participated in the study. The participant who

had the most senior rank was a Lieutenant Colonel. The next section deals comprehensively with the responses of military officers to the scale items listed in the COQ.

6.2.2 Quantitative results of the COQ: Descriptive analysis

6.2.2.1 Dimension 1: Information-sharing culture in the organisation

This dimension focused on the information-sharing culture among selected respondents at SAMA and is further elaborated on in the section that follows after Table 6.4. One hundred and thirteen respondents located at SAMA completed the questionnaire and, where applicable, the mismatch in the table can be ascribed to the non-response to questions. A percentage difference was therefore found between the items, owing to the aforementioned missing responses to items in the questionnaire.

Table 6.5: Information-sharing culture in SAMA

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
1	*I feel that it is safe to share information on social media.*	44%	35%	16%	3%	2%
2	*I feel that my personal information is important.*	4%	2%	23%	70%	1%
3	*I feel passwords are enough to protect my personal information stored on my work computer/laptop.*	24%	40%	25%	11%	0%
4	*I feel that using a storage device (USB) is the best way to store information.*	19%	44%	29%	7%	1%
5	*I change my passwords on my laptops, cellphone, and computer on a regular basis.*	10%	31%	39%	19%	1%
6	*I feel safe using free Wi-Fi from public places.*	29%	49%	19%	2%	1%
7	*I sometimes connect my cellphone or laptop to a public Wi-Fi connection.*	21%	20%	53%	4%	2%
8	*I feel comfortable posting about my personal life on social media.*	48%	39%	10%	2%	1%
9	*I feel comfortable posting information about my workplace activities on social media.*	66%	24%	4%	3%	3%
10	*I feel that my work should have more cybersecurity awareness campaigns.*	6%	5%	24%	62%	3%
11	*I have read about an information-sharing policy at my workplace.*	5%	18%	57%	17%	3%
12	*I feel that my workplace should implement an information-sharing policy.*	4%	4%	48%	41%	3%
13	*I am aware of guidelines at my workplace promoting cybersafety.*	4%	21%	54%	19%	2%

* Totals do not add up to 100% due to missing data.

It is important to note that the researcher presents the findings in a cluster format, which implies that Questions 1 to 9 represent how respondents considered information-sharing practices and the security behaviour attached to them. Question 1 of the COQ revealed that 79% of the respondents disagreed with sharing information online, whereas 44% of the 79% indicated that it was unsafe to share their personal information on social media, although 19% of the respondents felt it was safe to share their information on social media. With regard to Question 2, most (93%) of the respondents felt that their personal information was important. Question 2 also showed that 70% of the respondents felt very strongly that their personal information was important and that it should not be shared in an online space. As high a percentage as 64% of the respondents indicated in response to Question 3 that they felt their passwords were not enough to protect the personal information stored on their official computer/laptop, while 38% of the respondents were comfortable with their passwords protecting their personal information on their official computer/laptop. A high 63% of respondents indicated in response to Question 4 that using a storage device (USB) was unsafe for storing information, while 33% indicated they felt it was safe to store organisational information on a USB. Relating to Question 5, 58% of the respondents indicated that they changed their passwords on their laptops, cellphones, and computers on a regular basis, while 41% of individuals did not change their passwords on these devices regularly. Most (78%) of the respondents to Question 6 emphasised that they did not feel safe using free Wi-Fi in public places, with only 20% of the respondents felt safe doing so. Question 7 elicited that 57%, just over half of the respondents, occasionally connected their cellphones or laptops to a public Wi-Fi server, whereas 41% indicated that they did not. A high 87% of the respondents to Question 8 indicated that they felt uncomfortable posting about their personal life on social media, while 12% stated they were comfortable with submitting posts about their personal life on social media. The responses to Question 9 revealed that 91% of the respondents felt uncomfortable about posting information about their workplace activities on social media, with only 7% of the respondents admitting to feeling sufficiently comfortable to post about workplace activities on social media. The responses to Questions 10 to 13 show how the respondents reacted to items directed at the way that information-sharing practices is applied in the workplace and their responses to the impact of policies on this. A large majority (86%) of the respondents to Question 10 felt that their workplace should have more cybersecurity awareness campaigns, while 62% of them felt very strongly about having cybersecurity awareness campaigns in their workplace. Question 11 showed that 74% of the respondents indicated they had read about an information-sharing policy in their workplace, with only 23% of respondents disclosing that they had no knowledge of an information-sharing policy in their workplace. Question 12 showed that 89% of the respondents felt their workplace should implement an information-sharing policy, while 8% felt it was not necessary for their workplace to implement an information-sharing policy. Question 13 revealed that 73% of the respondents said they were aware of guidelines promoting cybersafety in their workplace, while only 25% of the respondents admitted to being unaware of such guidelines in their workplace.

6.2.2.2 Dimension 2: Security orientation among military officers

Dimension 2 focused on how military officers orientated themselves in cyberspace by specifically viewing how cybersecurity threats might manifest. Within this dimension, there were elements of missing data, which implied that some participants did not respond to all the items in the questionnaire.

Table 6.6: Security orientation among selected SAMA participants

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
18	*When I use the Internet, I am aware of the dangers of cyberthreats/attacks.*	4%	3%	50%	40%	3%
19	*I feel that information security is important in my workplace.*	1%	1%	37%	57%	4%
20	*When I feel unsafe using the Internet, I decide to log out.*	5%	8%	40%	42%	5%
21	*I sometimes save my personal information on my work laptop or computer.*	20%	33%	35%	8%	4%
22	*I am aware of technology that can be used to hack computers in my workplace.*	17%	26%	33%	20%	4%
23	*I update myself with cybersecurity issues.*	5%	30%	45%	15%	5%
24	*I sometimes try to include official cybersafety guidelines in my workplace.*	7%	34%	46%	8%	5%
25	*I know of colleagues who have had their personal or work laptops/computers hacked.*	8%	34%	37%	18%	3%

The first cluster in Dimension 2 focused on Questions 18 to 21, relating to the respondents' practical application of online security behaviour. The responses to Question 18 show that 90% of the respondents indicated that they were aware of the dangers of cyberthreats or attacks when using the Internet, while only 7% of the respondents said they were unaware of cyberthreats or attacks when using the Internet. Almost all (94%) the respondents to Question 19 indicated they felt that information security was important in their workplace. Question 20 showed that 82% of the respondents, with 42% feeling very strongly about this, indicated that when they felt unsafe using the Internet, they would log out. However, 13% of the respondents stated they would stay online despite feeling unsafe. Just under half (43%) of the respondents indicated that they would occasionally save their personal information on their work laptop/computer, whereas a little over half (53%) of the respondents noted that they would not save their personal information on their work laptop/computer.

The focus in the second cluster of Dimension 2 considered how respondents applied safety precautions by using guidelines. The responses to Question 22 showed that a slight majority (53%) of the respondents indicated that they were aware of technology that could be used to hack into computers in their workplace, while 43% of the respondents were not knowledgeable about technology that could be used to hack into the computers in their workplace. In answering Question 23, 60% of the respondents indicated that they kept themselves updated about cybersecurity matters, while 35% of the respondents indicated that they did not remain updated relating to cybersecurity matters. Over half (54%) of the respondents indicated in Question 24 that they occasionally included official cybersafety guidelines in their workplace, while 40% of respondents did not include cybersafety guidelines in their workplace. It emerged from Question 25 that 55% of the respondents were aware of colleagues who have had their personal or work laptops/computers hacked, while 42% did not know of colleagues who had experienced hacking of their colleagues' private or work laptops/computers.

6.2.2.3 Dimension 3: The officers' views of cybersecurity

This dimension focused on how military officers viewed cybersecurity. The questions primarily focused on the views of the military officer concerning cybersecurity in the workplace. In Dimension 3, the researcher did not have a group of cluster questions.

All items within this dimension focused on how the respondents considered the danger of cyberthreats in the workplace. In Dimension 3 it was evident that some respondents did not respond to all the items in the questionnaire. The missing values are reported as a percentage so that a total of 100% can be reached in each case item.

Table 6.7: SAMA officers' view of cybersecurity

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
29	*I feel that the Internet is safe to use.*	18%	38%	36%	4%	4%
30	*I am aware of the cyberthreats that are affecting the workplace.*	4%	21%	57%	13%	5%
31	*I am aware of cyberattacks that have happened at my workplace.*	10%	49%	34%	4%	3%
32	*I feel that all my work colleagues should learn the skills that can help them fight cyberthreats at work.*	0%	3%	41%	52%	4%
33	*I feel that the cybersecurity guidelines at my organisation will not limit the duties and tasks of military officers.*	2%	14%	51%	27%	6%
34	*I feel that there is a need for the military to control cyberspace.*	1%	6%	41%	47%	5%
35	*I feel that all Internet activity in my workplace should be monitored to prevent cyberthreats.*	3%	7%	41%	45%	4%
36	*I feel that monitoring the Internet at my work will change how people think about cybersecurity.*	4%	12%	43%	38%	3%
37	*I feel that all my colleagues are informed of cyberthreats or attacks at our workplace.*	16%	42%	30%	7%	5%
38	*I feel that the organisation pays attention to cyberthreats and attacks in the country.*	15%	30%	43%	7%	5%
39	*I feel that cyberspace is a new space to carry out warfare.*	2%	9%	39%	46%	4%
40	*I feel that my work colleagues are aware of the cybersecurity guidelines at our workplace.*	12%	38%	41%	4%	5%
41	*I am aware of my colleagues who are knowledgeable about cybersecurity*	5%	25%	52%	13%	5%
42	*I am aware of the consequences of cyberthreats for the organisation and the country.*	4%	13%	49%	28%	6%
43	*I feel that cyberthreats cannot harm the workplace.*	54%	30%	6%	4%	6%
44	*I feel that all officers in my workplace should be aware of the effects of cyberthreats.*	3%	3%	30%	60%	4%

The responses to Question 29 showed that 56% of the respondents felt the Internet was not safe to use, while 40% felt it was safe to do so. The majority (70%) of the respondents indicated in response to Question 30 that they were aware of the cyberthreats affecting their workplace, while 25% of the respondents were not aware of any cyberthreats. Most (59%) of the respondents noted in Question 31 that they were not aware of cyberattacks that had taken place in their workplace, with only 38% of respondents indicating that they knew of cyberattacks in their workplace. The responses to Question 32 showed that most (93%) of the respondents, with 52% of them feeling strongly in this regard, felt that all their colleagues at work should learn the skills that would help them fight cyberthreats in their environment. A small percentage (3%) of the respondents indicated that they did not feel that all their colleagues at work should learn the skills necessary for fighting cyberthreats at work.

The information supplied in respect of Question 33 showed that most (78%) of the respondents felt cybersecurity guidelines in their organisation would not limit the duties and tasks of the military officers, while 16% of the respondents felt that the cybersecurity guidelines would limit military officers' duties and tasks. The responses to Question 34 showed that 88% of the respondents felt that a need existed for the military to control cyberspace, while only 7% felt it was unnecessary for the military to control cyberspace. At the same time, 86% of the respondents to Question 35 felt that all Internet activity in their workplace should be monitored to prevent cyberthreats, while 10% of the respondents felt that it should not be monitored to prevent cyberthreats. The majority (81%) of the respondents to Question 36 indicated that they felt that monitoring the use of the Internet in their workplace would change what people thought of cybersecurity, while 16% felt that monitoring the Internet would not change what people thought of cybersecurity.

It was evident from the responses to Question 37 that 58% of the respondents felt that not all their colleagues were informed about cyberthreats or attacks in the organisation, while 37% felt that their colleagues were informed of cyberthreats or attacks in their workplace. Question 37 in this dimension might appear to overlap with Question 25 in Dimension 2. Question 37 focused on the views of the respondents and how others might perceive cybersecurity in the workplace, while Question 25 dealt with the respondents' awareness of whether their colleagues had been a victim of a cyberattack. This indicates that the responses to Questions 25 and 37 are connected as they highlight that limited cybersecurity awareness may be linked to security vulnerability in individuals' security behaviour.

The responses to Question 38 showed that only 50% of the respondents felt that their organisation paid attention to cyberthreats and attacks in South Africa, whereas 45% of the respondents felt that their organisation did not pay attention to cyberthreats and attacks in South Africa. Most (85%) of the respondents to Question 39 felt that cyberspace was a new space in which to carry out warfare, while 11% did not feel that cyberspace was a new space for conducting warfare. Question 40 showed that there were mixed views on cybersecurity guidelines in the workplace as 45% of the respondents felt that their colleagues were not aware of the cybersecurity guidelines in their workplace, while 50% of the respondents felt that their colleagues were aware of existing cybersecurity guidelines in the workplace.

The responses received to Question 41 revealed that 65% of the respondents were aware of colleagues who were knowledgeable about cybersecurity, while 30% of the respondents were not aware of colleagues who were knowledgeable about cybersecurity. Most (77%) of the respondents indicated being aware of the consequences of cyberthreats for their organisation and South Africa, while 17% of respondents indicated that they were not aware of the consequences of cyberthreats for their organisation and South Africa. Most (84%) of the respondents to Question 43 were of the view that cyberthreats might harm their workplace, with 54% of them stating they felt strongly that this might be the case. Question 44 indicated that most (90%) of the respondents, of whom 60% felt very strongly about it, felt that officers in their workplace should be aware of the effects of cyberthreats.

6.2.2.4 Dimension 4: Cybersecurity posture in the organisation

Dimension 4 focused on the cybersecurity posture of SAMA military officers in the workplace. The questions primarily focused on the practical activities of addressing cybersecurity behaviour in the workplace. In Dimension 4 it was evident that a minority of the respondents did not respond to all the items in the questionnaire.

Table 6.8: Cybersecurity posture of selected SAMA participants

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
45	*I feel that I behave the same on the Internet when I am at home or at work.*	15%	24%	45%	12%	4%
46	*I feel that knowing about cyberthreats may change how I communicate with others.*	3%	8%	52%	33%	4%
47	*I feel that using free software to fight cyberthreats and attacks in my workplace is unsafe.*	4%	17%	48%	26%	5%
48	*I feel that my workplace should develop its own software to fight cyberthreats and attacks.*	2%	4%	39%	51%	4%
49	*I feel that a cyber education programme for all members will increase cybersecurity in my workplace.*	2%	1%	36%	57%	4%
50	*I feel that education and training will help to change the security behaviour of members in my workplace.*	0%	2%	38%	55%	5%
51	*I feel that cyber-related education should be included in some of the work training programmes.*	0%	2%	40%	53%	5%

The findings derived from Question 45 showed that 57% of the respondents felt that their behaviour on the Internet was the same regardless of their context – work or home. However, 39% of the respondents indicated that they behaved differently on the Internet depending on whether they were at home or at work. Question 46 showed that 86% of the respondents indicated that if they had the knowledge, they would change how they communicated with others about cyberthreats. A minority of 11% of the respondents felt that they would not change how they communicated with others, regardless of whether they knew about cyberthreats or not. Seventy-four percent of the respondents to Question 47 indicated that it was unsafe to use free software to fight cyberthreats and attacks in their workplace, while 21% of the respondents felt safe using free software to fight cyberthreats and attacks in their workplace.

Most (90%) of the respondents to Question 48, of whom 51% felt very strongly in this respect, indicated feeling that their workplace should develop their own software to fight cyberthreats and attacks. Question 49 of the COQ showed that the majority (93%) of the respondents, with 57% of them feeling very strongly about this, felt that cyber-related education programmes for all members of the military would increase cybersecurity in their workplace. Furthermore, most (93%) of the respondents to

Question 50, with 55% of them feeling very strongly in this regard, indicated that they felt education and training would help to change the security behaviour of personnel in their workplace. The responses to Question 51 showed that most (93%) of the respondents felt strongly, with 60% indicating feeling very strongly, that cyber-related education should be included in some of their work training programmes.

6.3 Results derived from the SANWC

This section presents the findings on the SANWC respondents by first pointing out the demographic information of the sample. Thereafter, the next section presents the SANWC responses to the COQ dimensions, and then concludes with a synthesis of the SANWC results.

6.3.1 Demographic information

This section presents the demographic information relating to the SANWC sample. The display and interpretation of the demographics are an integral part of the argument put forward in the study. Table 6.9 provides information on the ethnicity of the SANWC sample. Displaying the demographic information is important as it allows for a basic view of the characteristics of the SANWC sample.

Table 6.9: Ethnicity of selected participants at the SANWC

Ethnicity of military officers	Frequency	Percentage
African	39	56
Coloured	9	13
Indian	2	3
White	19	27
Other	1	1
Total	**70**	**100**

The information supplied in Table 6.9 clearly evidences that the majority (56%) of the respondents were African. The second highest group comprised respondents who indicated that they were white (27%), with a smaller percentage (3%) being Indian, whereas coloured people represented only nine respondents (13%) who completed the questionnaire. One respondent did not indicate their race in the questionnaire.

Table 6.10: Gender of selected participants located at the SANWC

Gender of military officers	Frequency	Percentage
Female	23	33
Male	46	66
Missing value	1	1
Total	**70**	**100**

Table 6.10 indicates that the majority (66%) of the respondents were males, whereas a smaller percentage (33%) were females. It appeared from the results that all the respondents disclosed information related to their gender. However, it is worth noting that the questionnaire did not explore the view of respondents on gender. The researcher rounded up these percentages and the relationship is thus a very broad representation of the male and female distribution in the greater SANDF. In addition, there was one participant who did not want to disclose the gender in the SANWC sample population group.

Table 6.11: Arms of service of selected participants in the SANWC

Military division	Frequency	Percentage
SA Army	41	59
SAN	7	10
SAAF	12	17
SAMHS	7	10
Missing value	3	4
Total	**70**	**100**

Table 6.11 indicates that the majority (59%) of the respondents were in the SA Army. The second highest percentage (17%) of respondents indicated being in the SAAF. Military officers from the SAMHS and the SAN represented very few respondents to the questionnaire, with 10% each, and three respondents did not disclose their arms of service. It should be stated that foreign senior military officers were excluded from the findings relating to the SANWC as this study only focused on the views of South African military officers.

Table 6.12: Rank of selected military officers at the SANWC

Rank of military officers	Frequency	Percentage
Commander	7	10
Lieutenant Colonel	63	90
Total	**70**	**100**

Table 6.12 indicates that the majority (81%) of the participants held the rank of Lieutenant Colonel, while seven (10%) participants held the rank of Commander. The ranks Commander and Lieutenant Colonel are the same. However, the terminology that the arms of service use differ, with Commander being the operative term in the SAN and Lieutenant Colonel in the SA Army. It is worth indicating that the ranks of Commander and Lieutenant Colonel are both senior in the two arms of service. These respondents were part of the middle management cohort who were part of the Joint Senior Command and Staff Programme.

6.3.2 Quantitative results of the COQ: Descriptive analysis

A total of 70 respondents completed the questionnaire, and it should be noted that the mismatch in the tables can be ascribed to some respondents failing to answer certain question items in the COQ. A percentage difference is therefore found in the items due to missing responses in the questionnaire.

6.3.2.1 Dimension 1: Information-sharing culture in the organisation

This dimension focused on the information-sharing culture among the respondents at the SANWC.

Table 6.13: Information-sharing culture in the SANWC

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
1	*I feel that it is safe to share information on social media.*	34%	26%	7%	1%	32%
2	*I feel that my personal information is important.*	2%	2%	8%	54%	34%
3	*I feel passwords are enough to protect my personal information stored on my work computer/laptop.*	19%	24%	18%	7%	32%
4	*I feel that using a storage device (USB) is the best way to store information.*	10%	27%	26%	4%	33%
5	*I change my passwords on my laptops, cellphone, and computer on a regular basis.*	4%	16%	31%	16%	33%
6	*I feel safe using free Wi-Fi in public places.*	28%	28%	11%	1%	32%
7	*I sometimes connect my cellphone or laptop to a public Wi-Fi connection.*	21%	13%	30%	4%	32%
8	*I feel comfortable posting about my personal life on social media.*	40%	22%	6%	0%	32%
9	*I feel comfortable posting information about my workplace activities on social media.*	48%	16%	3%	0%	33%

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
10	*I feel that my work should have more cybersecurity awareness campaigns.*	2%	2%	17%	46%	33%
11	*I have read about an information-sharing policy at my workplace.*	7%	8%	33%	19%	33%
12	*I feel that my workplace should implement an information-sharing policy.*	2%	0%	29%	37%	32%
13	*I am aware of guidelines at my workplace promoting cybersafety.*	5%	15%	36%	12%	32%

Table 6.13 indicates that 60% of the respondents, in their responses to Question 1, indicated that it was unsafe to share their information on social media, with 34% feeling very strongly that it was unsafe to do so. In contrast, 8% felt it was safe to share their information on social media. Most (62%) of the respondents to Question 2 indicated that their personal information was important, and 54% felt very strongly about this. Almost half (43%) of the respondents to Question 3 said they felt that their passwords were insufficient to protect their personal information stored on their work computer/laptop, while 24% of these respondents were comfortable that their passwords protected their personal information on their computer/laptop. Moreover, it was shown through the responses to Question 4 that 37% of the respondents felt using a storage device (USB) was not the best way to store information, while 30% did not disagree with storing information on a storage device.

Furthermore, the responses to Question 5 indicated that 47% the respondents changed their passwords on their laptops, cellphones, and computers on a regular basis, while 20% did not change their passwords regularly. In addition, the majority (56%) of the respondents to Question 6 indicated that they did not feel safe using free Wi-Fi in public places, with only 12% of them indicating that they felt safe doing so. Less than half (34%) of the respondents to Question 7 indicated that they occasionally connected their cellphones or laptops to public Wi-Fi connections, while 33% indicated that they did not connect their phones or laptops to public Wi-Fi. The majority (62%) of the respondents to Question 8 pointed out that they did not feel comfortable posting about their personal life on social media, while 6% testified to being sufficiently comfortable doing so.

The responses to Question 9 showed that most (64%) of the participants felt uncomfortable with posting information about their workplace activities on social media, with only 3% of respondents feeling comfortable doing so. A high percentage of 63% of the respondents indicated in response to Question 10 that their workplace should have more cybersecurity awareness campaigns. In contrast, only 4% of the respondents felt very strongly about not having increased cybersecurity awareness campaigns in their workplace. Furthermore, 52% of the respondents to Question 11 indicated that they had read about an information-sharing policy in their workplace, with only 15% of respondents indicating that they had not read about such a policy. Question 12 showed that 66% of the respondents felt their workplace should implement an information-sharing policy, while 2% did not feel it was necessary for their workplace to implement such a policy. To Question 13, 48% of the respondents indicated that they were aware of guidelines that promote cybersafety in their workplace, while only 20% of the respondents indicated they were largely unaware of such guidelines in their workplace.

6.3.2.2 Dimension 2: Security orientation among military officers

Dimension 2 focuses on how military officers orientated themselves in cyberspace by specifically viewing how cybersecurity threats might manifest. Within this dimension, there were elements of missing data, which implied that a large portion of the SANWC participants did not respond to all the items in the questionnaire.

Table 6.14: Security orientation among selected SANWC participants

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
18	*When I use the Internet, I am aware of the dangers of cyberthreats/attacks.*	1%	4%	30%	30%	35%
19	*I feel that information security is important in my workplace.*	1%	3%	17%	45%	34%
20	*When I feel unsafe using the Internet, I decide to log out.*	3%	3%	25%	34%	35%
21	*I sometimes save my personal information on my work laptop or computer.*	16%	14%	30%	7%	33%
22	*I am aware of technology that can be used to hack devices in my workplace.*	10%	25%	20%	12%	33%
23	*I update myself with cybersecurity issues.*	6%	28%	25%	7%	34%
24	*I sometimes try to include cybersafety guidelines in my workplace.*	7%	22%	29%	9%	33%
25	*I know of colleagues who have had their personal or work laptops/computers hacked.*	11%	27%	20%	10%	32%

The findings derived from the responses to this section of the COQ showed that 60% of the respondents to Question 18 indicated they were aware of the dangers of cyberthreats/attacks when using the Internet, whereas only 5% of the individuals responded that they were unaware of cyberthreats or attacks when using the Internet. In addition, the responses to Question 19 showed that 62% of the respondents felt that information security was important in their workplace. Moreover, 59% of the respondents to Question 20 reported that when they felt unsafe using the Internet, with 34% of them feeling very strongly about this, they would log out. However, 6% of the respondents, as indicated in Question 21, declared that they would stay online even when feeling unsafe. Less than half (37%) of the respondents indicated that they would occasionally save their personal information on their work laptop/computer, while an almost equal portion (30%) of the respondents said they would not save their personal information on their work laptop/computer.

The responses to Question 22 showed that 32% of the respondents were aware of technology that could be used to hack into computers at their workplace, while 35% of the respondents indicated that they were not knowledgeable about technology that could be used to hack into computers at their workplace. Furthermore, the responses to Question 23 showed that 32% of the respondents kept themselves updated regarding cybersecurity issues, while 34% of them indicated they did not do so. The responses to Question 24 showed that less than half (38%) of the respondents indicated that they occasionally adhered to cybersafety guidelines in their workplace, while 29% of respondents indicated that they did not follow these procedures. In addition, 30% of the respondents indicated in Question 25 that they were aware of colleagues whose personal or work laptops/computers had been hacked, while 38% said they were unaware of colleagues who had experienced hacking of their work laptops/computers.

6.3.2.3 Dimension 3: The officers’ view of cybersecurity

This dimension focused on how military officers view cybersecurity. The questions primarily focused on SANWC military officers’ views concerning cybersecurity in the workplace.

Table 6.15: SANWC officers' view of cybersecurity

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing value
29	*I feel that the Internet is safe to use.*	12%	12%	28%	5%	43%
30	*I am aware of the cyberthreats that are affecting the workplace.*	5%	20%	37%	7%	31%
31	*I am aware of cyberattacks that have happened in my workplace.*	9%	33%	20%	6%	32%
32	*I feel that all my work colleagues should learn the skills that can help them fight cyberthreats at work.*	1%	1%	23%	45%	30%
33	*I feel that the cybersecurity guidelines in my organisation will not limit the duties and tasks of military officers.*	3%	7%	29%	29%	32%
34	*I feel that there is a need for the military to control cyberspace.*	1%	4%	25%	35%	35%
35	*I feel that all Internet activity in my workplace should be monitored to prevent cyberthreats.*	2%	2%	27%	37%	32%
36	*I feel that monitoring the Internet at my work will change how people think of cybersecurity.*	2%	5%	28%	32%	33%
37	*I feel that all my colleagues are informed of cyberthreats or attacks in our workplace.*	15%	32%	14%	7%	32%
38	*I feel that the organisation pays attention to cyberthreats and attacks in the country.*	10%	30%	21%	7%	32%
39	*I feel that cyberspace is a new space to carry out warfare.*	3%	1%	28%	36%	32%
40	*I feel that my work colleagues are aware of the cybersecurity guidelines in our workplace.*	11%	30%	21%	6%	32%
41	*I am aware of my colleagues who are knowledgeable about cybersecurity.*	4%	15%	36%	11%	34%
42	*I am aware of the consequences of cyberthreats for the organisation and the country.*	4%	7%	42%	14%	33%
43	*I feel that cyberthreats cannot harm the workplace.*	42%	20%	3%	1%	34%
44	*I feel that all officers in my workplace should be aware of the effects of cyberthreats.*	0%	0%	19%	47%	34%

The responses to Question 29 revealed that 33% of the respondents felt that the Internet was not safe to use, while 24% felt it was safe to use. In Question 30, 44% of the respondents reported being aware of cyberthreats affecting their workplace, while 25% of the respondents were not aware of any cyberthreats. In addition, most (42%) of the respondents in Question 31 were not aware of cyberattacks that had occurred in the workplace, whereas 26% of the respondents were aware of cyberattacks having taken place in the organisation. Furthermore, most (68%) of the respondents in Question 32, with 45% feeling strongly about this, felt that all their work colleagues should learn the skills that would help them to fight cyberthreats at work. Only two (3%) respondents to Question 32 felt that it was not necessary for all their work colleagues to learn the skills required for fighting cyberthreats at work.

The responses to Question 33, as shown in Table 6.12, indicated that most (58%) of the respondents felt that cybersecurity guidelines in their organisation would not limit the duties and tasks of the military officers, while 10% of the respondents felt that the cybersecurity guidelines would have a limiting effect on the military officers' duties and tasks. The responses to Question 34 showed that 60% of the respondents felt there was a need for the military to control cyberspace, while only 5% of the respondents felt that there was no need for the military to do so. It was clear from the outcome to Question 35 that 64% of the respondents felt that all Internet activity in their workplace should be monitored to prevent cyberthreats, while 4% of the respondents indicated that the Internet should not be monitored for this reason. The majority (60%) of the respondents indicated in Question 36 that monitoring the Internet in the workplace would change the way people think of cybersecurity, while 7% felt that monitoring the Internet would not change the way that people regarded cybersecurity.

The responses to Question 37 indicated that 47% felt that not all their colleagues were informed of cyberthreats or attacks in their workplace, whereas 21% felt that their colleagues were informed of these threats. The responses to Question 38 signified that 28% of the respondents felt that their organisation paid attention to cyberthreats and attacks in South Africa, but at the same time 40% of the respondents felt that their organisation did not pay attention to cyberthreats and attacks in South Africa. Most (64%) of the respondents to Question 39 felt that cyberspace was a new space in which warfare could take place, while 4% felt that cyberspace was not a new space for warfare. Question 40 showed that there were differences in views on cybersecurity guidelines in the workplace as 41% of the respondents felt that their work colleagues were not aware of cybersecurity guidelines in their workplace, while 27% of the respondents felt that their work colleagues were well aware of cybersecurity guidelines.

Furthermore, 47% of the respondents indicated in Question 41 that they were aware of colleagues who were knowledgeable about cybersecurity, while 19% of the respondents were not aware of colleagues who had knowledge of cybersecurity. Most (56%) of the participants to Question 42 pointed out that they were aware of the consequences of cyberthreats in their organisation and in South Africa, but 11% of the participants indicated that they were not aware of any such consequences. Moreover, most (62%) of the respondents to Question 43 revealed that cyberthreats were able to harm the organisation, while 4% of respondents indicated they did not believe that cyberthreats could harm the organisation. Most (66%) of the respondents in Question 44, with 47% feeling very strongly about it, felt that all officers in their workplace should be aware of the effects of cyberthreats. In the same question, 100% of the SANWC respondents were of the opinion that they should not be aware of the effects of cyberthreats.

6.3.2.4 Dimension 4: Cybersecurity posture in the organisation

This dimension focused on SANWC military officers' behaviour in ensuring cybersecurity in the organisation. The questions primarily focused on the practical activities in addressing cybersecurity behaviour in the workplace.

Table 6.16: Cybersecurity posture among selected SANWC officers

No.	Statements	Strongly disagree	Disagree	Agree	Strongly agree	Missing values
45	*I feel that I behave the same on the Internet when I am at home or at work.*	6%	14%	32%	15%	33%
46	*I feel that knowing about cyberthreats may change how I communicate with others.*	1%	2%	32%	32%	33%
47	*I feel that using free software to fight cyberthreats and attacks at my workplace is unsafe.*	2%	9%	38%	18%	33%
48	*I feel that my workplace should develop their own software to fight cyberthreats and attacks.*	1%	5%	28%	32%	34%
49	*I feel that a cyber education programme for all members will increase cybersecurity in my workplace.*	0%	0%	22%	44%	34%
50	*I feel that education and training will help to change the security behaviour of members in my workplace.*	0%	0%	26%	40%	34%
51	*I feel that cyber-related education should be included in some of the work training programmes.*	0%	0%	21%	45%	34%

The responses to Question 45 indicated that 47% of the respondents felt that their behaviour on the Internet was the same regardless of their context, whether at work or at home. However, 20% of the respondents indicated they behaved differently on the Internet depending on whether they were at home or at work. Question 46 revealed that 64% of the respondents felt they would change how they communicated with others if they knew about cyberthreats. However, very few (3%) of the respondents felt that they would change how they communicated with others if they knew about cyberthreats. The majority (56%) of the respondents to Question 47 agreed that it was unsafe to use free software to fight cyberthreats and attacks in their workplace, while 2% strongly disagreed with this and 9% disagreed that it was unsafe to use free software for fighting cyberthreats. Most (60%) of the respondents to Question 48, with 32% feeling very strongly about this, felt that their workplace should develop its own software to fight cyberthreats and attacks. The responses to Question 49 of the COQ showed that most (66%) of the respondents, with 44% of them feeling very strongly in this regard, felt that cyber education programmes for all members of the military would increase cybersecurity in their workplace. As indicated by the responses to Question 50, most (66%) of the respondents reported that education and training would help to change the security behaviour of colleagues at their place of work. Of these, a high percentage (40%) indicated feeling very strongly about education and training. Most (66%) of the respondents to Question 51, with 45% of them feeling very strongly about this, felt that cyber-related education should be included in some of their work training programmes.

6.4 Short question results of the COQ: Thematic analysis

The short questions in the COQ were analysed as one unit, and the data gathered from SAMA and the SANWC were combined. With the short question responses combined for SAMA and the SANWC, the researcher was able to provide codes that form part of the thematic analysis process (see Section 4.8.2.2). The short question codes were quantified and thematically grouped (see Appendix N). The themes derived from the data therefore represent both SAMA and the SANWC as they were relevant to both organisations, with the most significant difference being that the views expressed were from a junior and a senior group of SANDF officers. It is worth noting that not all respondents shared their views on the short questions; however, it is important to note that the respondents were not compelled to answer these questions.

6.4.1 Theme 1: Information sharing on best practices requires implementation

The theme *Information sharing on best practices requires implementation* centred on the notion that (1) existing security measures are not applied in the organisational context, and (2) that there was a need for the organisation to create a culture that focuses on securing information in a digital space, which is often described as relaxed.

6.4.1.1 Sub-theme 1.1: Information security requires devotion

This theme focused on the information-sharing practices and measures that were often not implemented in the organisation. This theme and the findings presented for Dimension 1 were concurrent. Overall, the majority (38%) of the participants from SAMA and the SANWC indicated that best practices related to cybersecurity were often not implemented owing to the low priority it received. The participants viewed this as an important aspect relating to creating awareness in the organisation and cultivating a culture that was in line with cybersecurity trends. The information supplied in the analysis process and coding development necessitated highlighting that the participants viewed progression in the application of cybersecurity measures as limited (14%). The execution of policies appeared to be one of the major factors that emerged from the data, which could be linked to the main theme. The majority (19%) of the participants viewed the implementation of policy related to cybersecurity as limited. Developing and sustaining an information security culture in an organisation requires altered mindsets, perceptions, and behavioural change to implement and comply with policies and processes (Ahmad & Huvila, 2019). The implementation of policies does not rest on the premise that members should adopt principles and processes alone. It is worth noting that implementing a cybersecurity policy that deals with the urgent issues relating to digital security in organisations should be done by means of a more holistic approach that considers both the social and technical aspects (Dong et al., 2021; Van’t Wout, 2019; Jansen van Vuuren et al., 2013). The argument can also be made that introducing a cybersecurity policy that focuses on information security can be approached differently due to variations in the security needs of personnel, the level of awareness among personnel, and the organisational climate, which might affect implementation (Dong et al., 2021; Mashiane et al., 2019; Van’t Wout, 2019; Jansen van Vuuren et al., 2013). The following excerpts indicate how the participants felt about the implementation of policies that were directed at creating information security awareness and providing a context in which implementation is reviewed:

> *"Not being implemented accordingly. Still needs a concrete structure of support"* (Participant 23, Lieutenant – SAMA).
>
> *"There is awareness and ISS presentations or courses presented to military officers. Military officers are aware of cybersecurity and follow the rules"* (Participant 84, Lieutenant – SAMA).
>
> *"Cybersecurity is like any other form of security. You can never have enough of it, and no matter how perfect your system and SOPs [standard operating procedures] are, you will get robbed/hacked/phished someday"* (Participant 3, Lieutenant – SAMA).
>
> *"It's relatively new and not well implemented"* (Participant 27, Candidate Officer – SAMA).
>
> *"Yes, the organisation is executing policies, but is approaching cyber from a very basic nature. Policies are also not really focused on cyber"* (Participant 5, Lieutenant Colonel – SANWC).
>
> *"It is of great importance for both the safety of the organisation and protection of my information, yet it is still under-emphasised to ensure cybersecurity"* (Participant 34, Lieutenant – SAMA).
>
> *"It has not been fully implemented, especially among the young generation that share about each and everything on the net"* (Participant 3, Lieutenant Colonel – SANWC).
>
> *"Implement policies that will serve as a guideline in terms of who is allowed to share what kind of information on the Internet. Which computers are being used with [the] Internet? Who is allowed to connect the workplace computers with the outside net?"* (Participant 20, Ensign / Candidate Officer – SAMA).
>
> *"Get involved and ... execution of policies"* (Participant 20, Lieutenant Colonel – SANWC).

> *“Training and implementation of well-drafted policies and with monitoring of activities on well-protected computers and smartphones”* (Participant 28, Lieutenant Colonel – SANWC).
>
> *“By putting policies in place and educating people about cybersecurity or perhaps implementing courses”* (Participant 37, Candidate Officer – SAMA).

The aforementioned excerpts clearly indicate the differing views of the participants regarding the implementation of cybersecurity policies and how awareness is created in the organisation. These views were presented in the narratives of Participants 5, 34, and 84. However, there was a balanced view among the participants from SAMA and the SANWC regarding the lack of cybersecurity policy implementation in the organisation. The data derived from the responses and the participants’ narratives enabled the researcher to confirm that there was indeed a majority view (14%) that the application of cybersecurity was considered to be limited and needs attention to enable the construction of a digital culture. However, 16% of the participants felt that cybersecurity awareness existed in the organisation, but that it was not fully implemented (see SANWC Participants 5 and 84). These responses represent the stronger indicator and the narratives are expected to support the stronger indicator. These narratives were consequently not lone-standing indicators. It should therefore be emphasised that one of the main aspects of creating an information-related security culture that focuses on cultivating awareness among members of the organisation is clear communication among all levels of the organisation with regard to the way that best practices are enforced throughout. Furthermore, there was an expectation that all members must understand the basic premise of what it means to be secure and how an organisation that intends to secure data that could be of key importance to administrative and operational activities might achieve this goal. This section is concluded by emphasising the following three important aspects:

1) The findings of the scale items for the SAMA and SANWC participants showed that a culture of information sharing prevailed in the organisation. However, the short questions pointed to the notion that there were often challenges with the implementation of security guidelines and policies.

2) The thematic finding related to information security also suggested that most participants located at SAMA and the SANWC were cautious when sharing information with colleagues, which implied a trust issue.
3) Awareness creation of and training in cybersecurity were pertinent in the organisation.

6.4.2 Theme 2: Cautionary behaviour is linked to the navigation of cyberspace

In order to create an environment in which members of the military are aware of the cyber-related dangers that might compromise their information, and also they themselves, the existing precondition demands that knowledge regarding this space must be present. Generally, most military officers located at SAMA and the SANWC highlighted that they navigated the Internet with caution. This implied that there was cybersecurity awareness among members. The participants in each of these sample groups recorded that a measure of vigilance prevailed when they navigated the Internet and completed tasks. However, a small percentage of participants in both sample groups did not portray this sense of vigilance and thus represented risk and vulnerability in maintaining cybersecurity. This main theme has one sub-theme, which focused on cautiousness when navigating the Internet.

6.4.2.1 Sub-theme 2.1: Cautiousness when navigating the Internet

The codes that emerged from the data indicated that navigating cyberspace (Internet) was considered to be a space where most participants exhibited vigilance, discipline, and care. The excerpts below indicate that members were generally aware of the dangers posed by the Internet and actively prevented failure in security by adjusting their behaviour appropriately.

Moreover, these extracts presented below highlight how awareness in cybersecurity was applied in a digital space:

> *"[I] don't have access to Internet at our workplace, but if I do have access I will ensure that my personal information is not displayed at all time[s] when I log in"* (Participant 2, Colonel – SANWC).
>
> *"Monitor what I send on the Internet"* (Participant 57, Lieutenant – SAMA).

> *"If I see that something is suspicious, I log out immediately"* (Participant 96, Lieutenant – SAMA).
>
> *"I am aware of sites that could have a potential risk involved. Don't actually take risks"* (Participant 10, Lieutenant – SAMA).
>
> *"I am very sceptical of what websites I visit and I need every detail of what I surf on the Internet"* (Participant 10, Lieutenant – SAMA).
>
> *"I'm dead, I do not participate much; for YouTube I only watch videos and do not subscribe"* (Participant 43, Lieutenant – SAMA).
>
> *"These days I'm becoming more cautious when I am on the Internet. The behaviour has changed since I joined SANDF"* (Participant 31, Lieutenant – SAMA).
>
> *"Carefree and exploratory"* (Participant 28, Candidate Officer – SAMA).

The abovementioned extracts emphasise that there was a mixed response from the participants in both sample population groups. The majority (45%) of the participants at SAMA and the SANWC were very cautious when navigating cyberspace and sharing information. Participants (12%) from both sample groups refrained from placing personal information online or logged out immediately if there were signs of suspicious activity on a specific website. On the other hand, some of the participants (13%) at SAMA indicated that their level of caution towards the Internet could not be rated high, but rather that they considered their security behaviour online as relaxed and carefree. To the contrary, almost all the participants at the SANWC were generally more cautious and considered cybersecurity as very important. It is important to note that this theme presented some key aspects:

1) The cybersecurity behaviour among the participants was generally linked to cautiousness when navigating the Internet, although some participants in the SAMA population group indicated that they were not very aware when browsing or sharing information online or characterised their behaviour as carefree (see SAMA Participant 28).
2) Participants located at the SANWC generally considered the Internet as a space where one should always be alert and aware of the threats. This section

of short questions was directed at obtaining deeper contextual meaning of what had been selected in the scale items of the COQ.

The next theme addresses the element of training and education as a possible way to increase security measures when engaging in cybersecurity.

6.4.3 Theme 3: Cybersecurity training and education as a way to enhance security measures

Cybersecurity awareness is constructed on the basis that information is readily available on the topic of interest to the individual and that there is space for learning to take place (Alharbi & Tassaddiq, 2021; Van't Wout, 2019; Zwilling et al., 2020). The crux of this theme was that cybersecurity education was required in the organisation and that information about important aspects relating to threats should be made available to members of the organisation. Moreover, it can be confirmed that there was uniformity in the data about the availability of cybersecurity information-related training and education. This main theme had one sub-theme, which focused on awareness training for all members.

6.4.3.1 Sub-theme 3.1: Cybersecurity awareness training for the entire organisation

This sub-theme addresses the management component of the main theme by highlighting that the majority (54%) of the respondents were of the view that education should be provided to members through regular training sessions that focus on guidelines on how to manage technology and be secure in the workplace. The theme also connected with the scale items presented in Dimension 3 (Questions 29 to 44). This connection rested on the premise of cybersecurity awareness and training. The questions relating to Dimension 3 primarily focused on "knowledge", "training", and "awareness". In the analysis of this theme, emphasis was also placed on the implementation of cybersecurity guidelines. A minority (5%) of the respondents from SAMA and the SANWC indicated that the organisation needed to implement cybersecurity policies and guidelines. It was revealed through the analysis of the short questions that 26% of the respondents felt that stricter measures needed to be employed when addressing cybersecurity in the workplace. This response can be viewed as an alternative for providing cybersecurity awareness training for military members. On the negative side, the findings derived from the SAMA and SANWC participants indicated that the respondents felt that some of their colleagues might not be aware of cybersecurity guidelines (see Question 40 in Appendix E). The limited access to guidelines, a factor that emerged from the responses, also indicated that there was a need for educational material to be available at all times. This view was corroborated by Participant 37, who suggested that continuous exposure to cybersecurity education and awareness programmes was important. This view can be substantiated by the responses to Question 44. The SAMA and SANWC respondents were in agreement that cybersecurity awareness training was important for the organisation. However, a minority (2%) of the respondents from SAMA indicated in Question 50 that they disagreed with cybersecurity training offered to military members and that it would have a positive impact on their behaviour. All respondents were in agreement in Questions 50 and 51 that cybersecurity awareness training would have a positive impact on their colleagues' security behaviour. In addition, the respondents from both sample population groups indicated that the organisation should do more in its pursuit to create cybersecurity awareness (Question 38). Moreover, the respondents felt that more cybersecurity policies needed to be implemented in the organisation, which links Question 38 with Question 39, which highlights the seriousness attached to cyberspace as an emerging warfare domain. The following excerpts argue that awareness training in cybersecurity should be made available to all military members in the organisation:

> *"People should be given awareness training and the training should be practical for individual[s] to experience the danger. For now it still sound[s] like a dream and it happens to others, and our workplace is protected, and [the] organisation is taking care of cybersecurity management"* (Participant 57, Lieutenant Colonel – SANWC).

> *"The best way is to provide training to all employees of the organisation in order to manage and control the security of the organisational information"* (Participant 20, Lieutenant – SAMA).

> *"Training member[s] continuously on the subject, continuous monitoring. Constant awareness programmes"* (Participant 37, Lieutenant Colonel – SANWC).

> *"Ensure an understanding/orientation of cybersecurity for members who are in the organisation, with focus [on] members using the work computer networks. Develop a cyber unit to secure all organisational communication of info"* (Participant 102, Midshipman, SAMA).
>
> *"Secured and monitored lines. But access must be granted for us to do business"* (Participant 65, Lieutenant Colonel – SANWC).
>
> *"It is to educate and instil methods in the work programme"* (Participant 47, Lieutenant – SAMA).
>
> *"Do not bring foreign gadget[s] to the defence force systems. Don't connect your phone to the system. Internet should be used independently. Documents should not be mailed as [Gmail] and [WhatsApp]"* (Participants 63, Commander – SANWC).
>
> *"Password[s] should be created for all members to monitor the flow of information. Certain information should be given to people with top secret security classification to ensure it's managed and kept safe"* (Participant 21, Lieutenant – SAMA).
>
> *"To have training and programmes that make members aware of cybersecurity awareness"* (Participant 49, Lieutenant Colonel – SANWC).

Developing and maintaining cybersecurity skills is an important component of cultivating a culture of security. It is important to note that the majority of the respondents, in the short questions, were in favour of cybersecurity training being offered in the organisation and the implementation of stricter security measures through monitoring of devices. The majority of the respondents indicated in Dimension 3 that there was a need to develop and train members to be aware of cyberthreats in the organisation. However, a combined minority (5%) of the respondents located at SAMA and the SANWC indicated that there was no need to create awareness and offer cybersecurity training to military members. This theme originated from the short questions, which focused on the view of security and the posture to this emerging topic in the SANDF. The participants' extracts highlighted this theme and suggested that the best way to manage cybersecurity was to create opportunities for learning and training. This sub-theme affirmed the responses to the COQ scale items as the findings from both the SANWC and SAMA participants showed that training was needed for all military members. In order for threats to be more identifiable in the SANDF (Questions 37 and 44), Participants 37, 47, and 49 made reference to the need for additional training on cybersecurity in the SANDF. Furthermore, the responses in Dimension 3, which focused on knowledge and awareness of cybersecurity, also corroborated the views of, for example, Participants 20, 37, 47, 49, 57, and 102, as indicated in the excerpts presented above. However, some respondents considered the use of stricter security measures as an alternative measure to address the skills gap in cybersecurity. Participants 21, 63, and 65 were in favour of monitoring devices in the workplace and employing stricter security measures relating to accessing information. The stricter response to monitoring Internet activity in the workplace aligned with the responses to Question 35 as the majority of the respondents from SAMA (86%) and the SANWC (64%) were in favour of this practice. There was also a combined minority (14%) of respondents from both sample groups who were not in agreement with monitoring of the Internet in the workplace. This sub-theme focused on cybersecurity awareness training for military members. The presentation of responses to the short questions showed that there was indeed agreement among SAMA and SANWC members regarding the need for cybersecurity awareness training.

6.5 Summary of findings: Descriptive and thematic analyses

This section consolidates the findings of the SAMA and SANWC participants. Inherently, the comparison between SAMA and the SANWC involves a junior-senior ranks outlook on the dimensions.

6.5.1 Dimension 1: Information-sharing culture in the organisation

This dimension is grounded in the theme *Information sharing on best practices requires implementation*. The information supplied in this section highlighted that an information-sharing culture existed in SAMA’s and the SANWC’s selected sample population groups. Tables 6.9 and 6.10 revealed that it was generally regarded as unsafe to share information online. With regard to Question 2, the responses of both sample population groups concurred as most military officers indicated that their personal information was important. Officers located at SAMA responded more strongly to Question 3 than the respondents at the SANWC. The focus in Question 3 was on the use of passwords in securing ICT devices such as laptops. The responses to Question 4 were, however, mixed as the SANWC recorded a poor response to whether the use of a USB storage device was sufficient for securing information. The SAMA respondents' responses to Question 4 showed that more than half of the respondents agreed that using a USB device was not the best way to secure data.

With regard to Question 5, both the SAMA and SANWC respondents indicated that they regularly changed the passwords on their devices. Question 6 showed that the majority of the respondents at SAMA and the SANWC felt unsafe when using public Wi-Fi. The SANWC respondents presented a mixed reaction about connecting their devices to public Wi-Fi, whereas the SAMA respondents signified a strong response that indicated disagreement as they felt safe connecting their devices to a public Wi-Fi service.

Furthermore, Question 8 revealed that most participants at SAMA and the SANWC were not comfortable with posting about their personal life on social media. Question 9 in the COQ also showed that participants from SAMA and the SANWC were not comfortable with sharing information about their organisation on the Internet. In addition, the participants from SAMA and the SANWC all indicated in response to Question 10 that they were in agreement that cybersecurity awareness campaigns should be promoted more in their organisation. The responses to Question 11 indicated that the participants from both SAMA and the SANWC were aware of information-sharing policies in the organisation. Building on this, Question 12 revealed that most participants at SAMA and the SANWC were aware of e-safety guidelines and practices that were promoted in the organisation. It is worth noting that Questions 11 and 13 were mutually supportive as both refer to knowledge of best practices and guidelines. This mutuality strengthened the argument that awareness of cybersecurity existed. However, in the SANWC group, many respondents, who were senior officers, indicated that they were largely unaware of cybersecurity guidelines in the organisation.

With the aforementioned responses in mind, it could be highlighted that three key aspects can be taken from Dimension 1 among the SAMA and SANWC sample population groups. These three aspects are: (1) there were good indicators of an existing information-sharing culture in SAMA and the SANWC, (2) most respondents were applying security measures in a personal and organisational capacity, and

(3) the respondents from SAMA and the SANWC both indicated that the organisation could do more in terms of promoting cybersecurity awareness. On the negative side, some SAMA respondents felt that it was completely safe to share information online. This was in agreement with the short narratives provided by the SAMA sample group, which identified potential vulnerability and risk. The next section, located within Dimension 2, focused on Theme 2 (*Cautionary behaviour is linked to the navigation of cyberspace*), which can be connected to the responses received in this dimension (information-sharing culture) of the COQ.

6.5.2 Dimension 2: Security orientation among military officers

The responses to Question 18 denoted consistency as the participants from both SAMA and the SANWC indicated that they were aware of the dangers attached to cyberthreats/attacks when using the Internet. The responses to Question 19 also showed that information security was considered important by the SAMA and SANWC participants. In support of this argument, the responses to Question 20 suggested that the majority of the respondents from SAMA and the SANWC logged out of applications when they felt unsafe. Question 21 reported a mixed reaction as some participants from SAMA and the SANWC indicated that they would not store personal information on their organisational devices, while a number of respondents from SAMA (36%) and the SANWC (30%) indicated that they would store some personal information on organisational devices.

Question 22 suggested that there was a slight majority in both the SAMA and SANWC participants, whose responses indicated that they were aware of technology that could be used to hack into devices in their organisation. In addition, data derived from Question 23 showed that SANWC military officers varied in their responses as a slight majority did not update themselves about security challenges that could occur. To the contrary, the majority of SAMA participants confirmed that they kept themselves updated about security issues.

Question 24's responses reflected that both the SAMA and SANWC respondents tried to include cybersecurity measures in their day-to-day activities, which implied that a certain level of e-safety was employed. Moreover, SAMA and SANWC respondents indicated that they were aware of people whose computer devices had been hacked. The researcher argues that this awareness of cybersecurity incidents occurring in the organisation might be an element that could give respondents a heightened sense of security. In summary, this section showed several key points:

1) Most participants from both sample groups showed that they were aware of cybersecurity threats when browsing the Internet. This implied that there was a foundation of cybersecurity awareness when navigating cyberspace and when confronted with possible threats.
2) There were also indicators of some emphasis on security measures being used when confronted with a possible cyberthreat as both sample groups showed a strong drive to adopt security behaviour if they felt unsafe when in cyberspace. In addition, this dimension was located in Theme 2: *Cautionary behaviour is linked to the navigation of cyberspace*.
3) The narratives presented also make reference to cautiousness when navigating cyberspace and the adoption of security behaviour when confronted with more information about potential risks. However, there were narratives that indicated that a slight minority of the respondents considered their cybersecurity behaviour as relaxed and carefree (see Respondent 43, Theme 2).

6.5.3 Dimension 3: The officers' view of cybersecurity

Tables 6.13 and 6.14 indicated that it should be emphasised that the SANWC and SAMA respondents were aware of the existing cyberthreats that could compromise security. The responses to Question 29 indicated that there were mixed views about whether the Internet was a secure domain or not. While half of the junior officer respondents at SAMA suggested that cyberspace was not a secure domain, 40% were of the view that it was a secure space. The findings derived from the SANWC disclosed that the senior officers responded similarly. The responses to Question 30 showed that there was a strong sense of agreement between SANWC and SAMA respondents about whether cyberthreats could have an impact on the organisation. The responses to Question 31 indicated that most of the respondents from SAMA and the SANWC were not aware of any cyberattacks that had occurred in the organisation. Furthermore, the responses to Question 32 revealed that most respondents at SAMA and the SANWC indicated that their colleagues would benefit from acquiring skills to counteract potential cyberthreats in the workplace. The responses to Question 33 showed that most SAMA and SANWC officers admitted to being of the opinion that cyber guidelines would not limit their interactions in the workplace. A strong positive response to Question 34 indicated that the respondents from SAMA and the SANWC were of the opinion that cyberspace needed to be controlled by the military. In addition, the responses to Question 35 focused attention on monitoring Internet activity in the workplace and supported the positive responses to Question 34.

The responses to Question 36 showed a strong preference for the idea that monitoring the Internet in the workplace would contribute to an alternative way of thinking about cybersecurity. The responses to Question 37 showed agreement between the responses by the SANWC and SAMA respondents, namely that not all members of the organisation were aware of cyberthreats or attacks in the workplace. The responses to Question 38 highlighted that a discrepancy existed between the SAMA and SANWC participants' responses. The majority (50%) of the SAMA respondents indicated that the organisation did pay attention to cyberthreats. However, 45% responded that the organisation did very little to advance cybersecurity. The majority (40%) of the SANWC respondents believed that the organisation did very little concerning cyberthreats. The responses to the short questions (see Theme 3) pointed out that cybersecurity awareness was necessary in the organisation to educate its members about cyberthreats. A connection therefore exists between the COQ scale item responses and the short question responses. Most respondents to Question 39 indicated that cyberspace was a new domain in which warfare might be carried out. In response to Question 40, 50% of the respondents from SAMA and 40% from the SANWC indicated that their colleagues were unaware of cybersecurity guidelines in the organisation. The short narrative responses from the SAMA and SANWC respondents also confirmed this as 5% of the codes that appear in the thematic analysis showed that cybersecurity policy implementation was a challenge (see Appendix N). The SAMA respondents (45%) and the SANWC respondents (27%) indicated to a greater and lesser degree that their colleagues were aware of cybersecurity guidelines.

The responses to Question 41 indicated that the majority of the respondents from both SAMA and the SANWC confirmed having colleagues who were knowledgeable about cybersecurity. This supports the responses to Question 42, as the respondents from SAMA and the SANWC showed a strong indication that they were aware of the consequences relating to cyberthreats. The majority of the responses to Question 43 divulged that the respondents from both SAMA and the SANWC were cognisant of the idea that cyberthreats could inflict harm on the organisation. Questions 41, 42, and 43 built upon each other and this security aspect was reinforced by Question 44. There was consensus among the SAMA and SANWC respondents about Question 44, as they indicated that all officers in the workplace should be made aware of cyberthreats that exist in that space. In taking a summative view of the findings in Dimension 3 (Officers' views of cybersecurity), it became clear that (1) most respondents at SAMA and the SANWC were aware of the implications of cyberthreats, (2) the respondents maintained that training for all members related to cybersecurity was important, (3) the positive response towards monitoring of the Internet to protect the organisation and the country was highly rated for both the SAMA and SANWC respondents, and (4) responses to questions geared towards training and education (Questions 32, 33, 37, 38, 41, and 44) also received a highly positive response from both SAMA and SANWC respondents. The next section, located within Dimension 4, focuses on Theme 3: *Cybersecurity training and education as a way to enhance security measures*, which connected to the responses received in this dimension of the COQ.

6.5.4 Dimension 4: Cybersecurity posture in the organisation

In Dimension 4, it became evident that, among the respondents from both the SANWC and SAMA, online behaviour relating to cyberspace was replicated in their personal and professional capacity, as can be observed in the responses to Questions 45 and 46. A very small portion of the respondents, in both the SAMA and SANWC sample population groups, indicated that they practised online behaviour relating to cyberspace and networks differently depending on whether they were acting in their professional or personal capacity. In addition, the majority of the respondents in both sample population groups indicated that they would communicate more cautiously in cyberspace if they were more knowledgeable about and aware of cybersecurity threats. The majority of the respondents from both sample population groups indicated in response to Question 47 that they were aware of the dangers associated with the use of free online software in their professional environment. In addition, a small percentage of the participants indicated in Question 48 that free software could be used to counter cybersecurity threats and attacks in the workplace. In contrast, most of the respondents from SAMA and the SANWC thought that the SANDF should develop security-enhancing software that belonged to the SANDF to address cybersecurity threats.

The respondents from SAMA and the SANWC generally indicated that cybersecurity awareness education would improve overall digital security in the organisation. In addition, the respondents highlighted that training and education in cybersecurity awareness would assist with improving the broader security behaviour of members of the military, as emerged from the responses to Question 49. In Questions 50 and 51, it is important to note that the respondents from the SANWC responded negatively to the creation of a cybersecurity education programme for all military personnel by indicating they did not believe this would advance digital security in the organisation. To the contrary, the respondents from SAMA highlighted that training for all military personnel would be beneficial. The majority of the respondents from both SAMA and the SANWC indicated in response to Question 52 that cybersecurity education training should be introduced in official training.

In summary, the replication of security behaviour among both sample groups appeared to be consistent. This implies that some cybersecurity measures had been put in place in the respondents' personal and professional capacity. However, practising security behaviour was done differently depending on the respondents' personal and professional context. This raises concerns as it highlights that security was not practised consistently, even though security practices were replicated in the personal or professional space. The respondents indicated that they were generally cautious when navigating cyberspace, but would be more aware of how they communicated with others, depending on the nature of the threat observed.

With regard to the use of freely available open-source software in cyberspace, the respondents indicated that they believed this could potentially be dangerous and expose the organisation to harm. Yet, a very small percentage of respondents from both sample groups indicated that open-source software could also potentially be beneficial. In terms of cybersecurity training, both sample groups agreed that the organisation could benefit from providing more education on cybersecurity in the organisation. However, the SANWC respondents indicated that training and education in cybersecurity should not be provided to all members of the organisation.

Reservations regarding cybersecurity training could be due to the voluntary and involuntary security threats coming from the human element. The researcher considers the finding related to training for all members and the respondents' reservation about "all" perplexing. The reasoning behind this reservation about training all members was not explored further. The key points in this section were (1) that cybersecurity training and education were essential for the organisation and (2) that the risks associated with navigating cyberspace could be better understood if threat information and guidelines were more readily available.

6.6 Conclusion

One of the main findings that emerged from the COQ was that education and training were considered an imperative component in creating cybersecurity awareness in the organisation, although it was also noted by a small percentage of the respondents at the SANWC that this may not necessarily be reserved for everyone. What also emerged was consistency between junior and senior branches of military training in how the Internet was approached in the organisation and how information sharing was regarded. A great need, as the respondents indicated, exists for cybersecurity guidelines to be implemented and enforced by the organisation. This showed the necessity for greater involvement on the part of the organisation with regard to cybersecurity measures. The sharing of information and the policies that direct them were identified by the respondents from both the SANWC and SAMA as being present in their respective units or workplaces, as indicated in Dimension 1. Furthermore, it became apparent that there was not much difference between the views of the respondents located at SAMA and those at the SANWC relating to cybersecurity awareness training for military members. The findings of the qualitative short questions that were included in the COQ revealed a small measure of disjointedness between the responses to the scale items and what was reported in the short questions. This could be ascribed to survey fatigue or that the meaning of the questions was not adequately apparent to the diverse range of respondents.

The chapter that follows discusses the interview themes and findings of the COQ.

CHAPTER 7: DISCUSSION OF INTERVIEW THEMES AND CYBERSECURITY ORIENTATION QUESTIONNAIRE (COQ) FINDINGS

7.1 Introduction

This study aimed to explore the perceptions of cybersecurity among South African military officers. This chapter's key contributions rest on the inclusion of data derived from the COQ (Likert scale items and short questions) to supplement the findings derived from the semi-structured interviews. This chapter offers a discussion of the main findings of the study by focusing first on establishing the context of the findings presented in Chapters 5 and 6. An overview of the research questions in relation to the themes and COQ scale items is also presented. This is done to show how the findings were triangulated and how they confirm the themes that emerged in Phase 1. A discussion of the research questions in relation to the triangulated findings follows. The chapter's conclusion includes an overarching summary of the exploration of cybersecurity among South African military officers.

7.2 Summary and discussion of the CA findings

This section provides a summary and the context of the findings that emerged from the interview and the questionnaire. The purpose of this section is to present the findings of both the interview and the COQ dimensions. The presentation of the findings also adds weight to the argument in the rationale of the study, namely that questionnaires alone are not sufficient to provide a lens on cybersecurity behaviour but do well in capturing specific aspects of cybersecurity awareness. Consequently, this section will firstly focus on the interview themes and then turn to the discussion of the four dimensions of the COQ, in which the responses to the scale items are discussed. A summarised approach to the discussion and presentation of the findings, followed by a brief discussion in context, provide a practical means of showing triangulation. For the sake of clarity, the themes and sub-themes of Phase 1 are presented in Table 7.1.

Table 7.1: Distribution of themes in Phase 1

Interview main themes	Interview sub-themes
Theme 1: Knowledge production and training focusing on cybersecurity awareness	Sub-theme 1.1: Awareness and knowledge of cyberspace and its associated dangers
	Sub-theme 1.2: The establishment of cybersecurity awareness among military members
Theme 2: Challenges of trust with technology and members	Sub-theme 2.1: Vigilance among members of the organisation owing to differences in how cyberspace is approached
	Sub-theme 2.2: The uncertainty of cybersecurity best practices and protocols in the organisation
Theme 3: The construction of a digital culture among members	Sub-theme 3.1: Culture of digital security among officers
	Sub-theme 3.2: Personal devices are considered more efficient to store organisational information
	Sub-theme 3.3: Cyber increases the skills gap between more senior and junior military officers
	Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice
Theme 4: The view on cyberthreats is constructed based on experiences in the physical domain	Sub-theme 4.1: Information security as a practice
	Sub-theme 4.2: Perception as an important aspect to military members

It was necessary to contextualise this study’s findings as this section aims to present the findings in context, which were based on the CA of the SANDC interviews.

Phase 1’s findings indicated that there were many facets to cybersecurity perceptions. It was therefore important to highlight that cybersecurity still appears to be an emerging concept, which could be shown in how the participants reacted to the question about how the organisation approached cyber (see Sub-theme 1.1: *Awareness and knowledge of cyberspace and its associated dangers*). Furthermore, Sub-theme 1.2 focused on *the establishment of cybersecurity awareness among military members* and the findings showed that training in cybersecurity was required at the entry level.

Viewing the themes in context, cybersecurity training and providing education in novice Internet security skills currently did not appear to be of significant concern owing to the lack of attention it received from the SANDF. In the context of Sub-themes 1.1

and 1.2, the argument can be made that the SANDF could equip its members to be proficient in cybersecurity skills by using specialist knowledge that draws on experience of the industry[32]. This should go beyond merely questioning cybersecurity awareness in the SANDF context to interrogating the priority given to cybersecurity awareness training in the broader context of South Africa.

Theme 2, *Challenges of trust with technology and members*, produced two sub-themes, namely *Vigilance among members of the organisation owing to differences in how cyberspace is approached* and *The uncertainty of cybersecurity best practices and protocols in the organisation*. Sub-theme 2.1 indicated the vigilance associated with practising cybersecurity in the organisation. This sub-theme furthermore identified a challenge as some participants felt they could not trust their colleagues because of the way they used the Internet and how they practised cybersecurity. Most participants also felt that the organisation was not enforcing the existing cybersecurity policies, which could be why the prevailing perception was that the safety of personal and organisational information might be compromised. Considering Sub-theme 2.1 in context, it is relevant to note that the uncontrolled use of social media could be a threat to the SANDF, especially since most participants indicated they had adopted a digital way of living, characterised by a blended dynamic, where occupational and personal activities easily interlink. This reaffirms the stance that the military officer is not isolated from society.

In the defence environment, trust is regarded as invaluable as the success of operations relies completely on accurate and reliable information, which can only be the case where trust prevails. In an organisational context such as the SANDF, social exchanges between the various levels of functioning, for example the tactical, operational, and strategic, play an important role in the interchange of information and, more importantly, the relationship among members of the military who have positions at each of those three levels. It is therefore considered imperative for trust to be developed as information is filtered down the ranks. Establishing trustworthy relationships as a basis of forming healthy relationships is of cardinal importance for mission success. Consequently, employee organisational trust can be considered an

[32] See Duvenage (2019) on strategies to increase cybersecurity awareness in Chapter 2.

essential forecaster of organisational trust. Based on the findings, it is argued that cybersecurity behaviour is not all that secure and that the element of trust is broken.

Sub-theme 2.2 focused on the uncertainty of cybersecurity best practices and protocols in the organisation. Most participants felt unsure about the cybersecurity practices in the SANDF. Sub-theme 2.2 also drew attention to knowledge and understanding of best practices and guidelines. It can therefore be argued that the challenge with achieving information security in organisations might be due to the lack of enforcement of polices that focus on cybersecurity. Furthermore, the element of compliance with policies might also be considered a key factor in how personnel approached security[33]. As noted earlier, the argument was made that the challenge to achieve information security in organisations is the lack of enforcement of policies that deal directly with cybersecurity and inconsistent approaches to the use of devices.

The third theme focused on the construction of a digital culture among members. This theme produced four sub-themes: 3.1: *Culture of digital security among military officers*, 3.2: *Personal devices are considered more efficient to store organisational information*, 3.3: *Cyber increases the skills gap between more senior and junior military officers*, and 3.4: *The demand for faster and more efficient communication is becoming normalised practice*. When viewing the findings of Sub-theme 3.1, the majority opinion among the participants was that the culture associated with digital security was limited as six of the 10 senior military officers interviewed indicated that the existing culture that embraced technology was limited. It can be said that organisational security culture might be influenced by the overall morale of personnel and the need to adhere to proposed guidelines in organisations. In addition, the findings derived from this sub-theme suggested that the interviewed SANDC participants were aware of the limited digital culture in the organisation, which aligns with the notion that the challenge in shaping organisational culture includes the establishment of a cybersecurity culture. The researcher argues that an additional factor that influences human behaviour is the possible inclusion of technology, which is used interchangeably between occupational settings and personal life. The possibility that a digital security culture would be fully embraced is also presented as a challenge as the South African Minister of Defence indicated in the Defence and Military Veterans Department Budget Vote 2021/22 that

[33] See Alotaibi et al. (2017) on the aspect of compliance with policies in an organisation and how this may impact organisational security culture.

the cybersecurity tools used in the SANDF were dated and required attention (RSA, 2021).

In addition to the discussion on Sub-theme 3.1, the focus of this study was on the military officer; hence the continuous reference to the human element. The context of the findings was directed at the notion that information security management, which forms part of cybersecurity, largely depends on the human factor. While the resource allocation for new technology and cybersecurity was not clearly stated in the DoD's annual report of 2020/2021 (RSA, 2020b), it is of key importance to note that the military officers interviewed had made some effort to embrace using technological devices in their personal lives and consciously or unconsciously apply this in their professional work environment. It is worth noting that the SANDC participants were of the view that embracing technology and fusing it with the notion of security can be considered a challenge. Moreover, based on the views of the participants interviewed at the SANDC, it emerged that there is hesitancy to embrace technology in the organisation. What should be acknowledged in respect of this theme is that the respondents displayed flexibility and the desire to integrate technology into their everyday functioning in the organisation. Where an organisation has values that accept change and is willing to be flexible in its values, it is likely that digital transformation can occur.

Linking Sub-theme 3.1 to RQ1 enabled the researcher to highlight that the passive creation of a digital culture might not promote knowledge construction nor direct employees' efforts and attention to adopting cybersecurity behaviour[34]. The researcher argues that the limited production of cybersecurity awareness and the lack of enforcement of security policies might not advance the notion of forming a digital security culture. In addition, most participants indicated that there was a limited digital security culture in the organisation. Very few participants in Sub-theme 3.1 indicated that a digital security culture existed. The researcher argues that limited knowledge production of cybersecurity awareness in the organisation might place the organisation in an even more vulnerable security position. The construction of cyberthreats among the participants could be described as cautious owing to their identified hesitation to

[34] See discussion by Fichman et al. (2014) in Chapter 2 on the role of innovation and digital transformation in organisations.

integrate new technology and their description of an organisational culture that does not embrace a digital environment comfortably.

Sub-theme 3.2 suggested that the participants who were interviewed felt more comfortable and safer using their personal devices such as laptops, storage devices, and cellphones than using the devices allocated for use by the organisation. This concern with safety was raised when the participants indicated that organisational devices were often infected with viruses. The participants indicated that they needed to be more cautious when transferring information from an organisational computer or device to their own personal storage device or computer. In addition, the use of personal devices among the interviewed participants suggested an element of work-related demands and security concerns. Moreover, the use of personal devices in the organisation might be linked to concerns about privacy. Personnel thus tended to feel that using their own devices would limit privacy concerns as they were able to scrutinise which applications were safe to use and how cybersecurity was maintained.

Sub-theme 3.2 also drew on information derived from the interviews that storage and computer devices were used to navigate day-to-day activities in the organisation. One of the main codes that emerged from the data analysis was the usage of personal devices. It should be mentioned that the relevant argument in Sub-theme 3.2 was that the participants would rather use their own devices to store and peruse the organisation’s information. Some participants testified to being unable to trust the DoD’s computers, which had been provided to them, because they were at greater risk of viruses, as noted in the excerpts from the SANDC interview transcriptions. Some participants also revealed that they had very little faith in the DoD’s systems, although the emphasis they placed on the internal networks had been recorded as somewhat reliable for storing information. The overall perspective was that there was also a level of convenience associated with using a personal storage device. Tasks associated with professional duties could be carried out or continued in the setting of the participants’ personal capacity or “after hours”, as noted in the qualitative excerpts.

Most participants indicated that when they felt unsafe on the Internet, they immediately logged off, especially when they were on a particular website or computer device. The participants indicated being aware of security issues and that they could take the necessary precautions when they used their own devices. Moreover, DoD Instruction DODI/CMI/00008/2001 (RSA, 2011a) suggests that members are advised against privately storing information that is linked to the organisation and that private computers used for DoD reasons will be subjected to audit. The risks associated with cyberthreats are heightened when personal devices are constantly used for uploading information from DoD networks and computers[35]. Malicious software on DoD computers and the aspect of convenience were pointed out by most of the participants as being the main reasons for giving preference to their personal devices.

Sub-theme 3.3 focused on how cyber increases the skills gap between more senior and junior military officers. When linking the role of top management to the increasing gap between military officers, the organisational culture factor should also be included. The findings suggested that most participants were aware of cyberthreats, although the findings in Sub-theme 3.3 referred to the notion that cybersecurity might be relatively new, which might provide some basis for the lack of attention received from senior management[36].

The findings also referred to the notion that some participants considered junior members to have had greater exposure to new technological interfaces, which allowed them to adjust more easily to embedding tools in their work-related activities, as well as their personal lives. Finally, financial and cultural factors might play a role, which could have an impact on perceptions and attitudes of members of the military about the role of work in the organisation. It is worth noting that the researcher did not control for financial and cultural factors in the study.

When linking Sub-theme 3.3 to cybersecurity awareness, the argument could be made that if the subject was not considered a priority, then this element of concern would undoubtedly have had an impact on how some participants perceived cybersecurity in the workplace. Nonetheless, the second aspect of this sub-theme addressed the factor of seniority and hierarchy in cybersecurity practices. Sub-theme 3.3 identified that the participants (senior military officers) who were interviewed suggested that junior officers were not acting cautiously in cyberspace. The researcher therefore argues that issues pertaining to cybersecurity practices have less to do with the element of hierarchy and rank, and more with the aspects of training and generational differences – in addition to how security behaviour is practised

[35] Khan et al. (2020) argue that most individuals lack basic knowledge of information security, which increases their risk of falling victim to cyberthreats.

[36] See arguments by North and Fiske (2012) and Fatokun et.al. (2019) in Chapter 2 about the role of age in organisational settings and its impact on cybersecurity.

online. By linking this to Sub-theme 3.3, the researcher notes that the interview extracts referred to the notion that younger military members were perhaps more likely to engage in riskier online security behaviour when using social media platforms and technology. The participants indicated that younger members were more likely to share information online without considering the consequences of security. In expanding this discussion, Sub-theme 3.4 focused on faster and more efficient means of communication. In Sub-theme 3.4, most participants showed that social media platforms such as WhatsApp were more efficient ways of communicating tasks and important information[37].

The discussion relating to the summary and contextualisation of themes continued in Theme 4, *Cyberthreats are constructed based on experiences in the physical domain*, which had two sub-themes: 4.1: *Information security as a practice* and 4.2: *Perception is an important aspect for military members*. Sub-theme 4.1 entailed how the participants made sense of information security by applying their perceived awareness of threats and best security practices when using the Internet in the workplace. In Sub-theme 4.1, the participants referred to how information security was practised differently depending on personal or professional context. The crux of the main theme remained that threat perception was constructed according to previous experience. Most participants indicated that they were aware of the dangers in cyberspace. However, the participants were also aware of their own vulnerabilities in relation to cybersecurity and organisational information. Sub-theme 4.2 showed that the participants' perceptions were an important factor that referred to how military officers regard themselves according to the perception of others. It appeared that one of the reasons that the participants felt they needed to be cautious in cyberspace or to be careful about monitoring their own behaviour was their concern for the organisation's reputation.

7.3 Discussion of COQ scale items for the SAMA and SANWC respondents

The COQ entailed four dimensions, namely (1) information-sharing culture, (2) security orientation, (3) views of cybersecurity, and (4) cybersecurity posture in the organisation. This section of the discussion focuses on the findings obtained from

[37] See discussion by Murire et al. (2021) in Chapter 2 regarding the use of personal devices and information security awareness among personnel and information security awareness.

these four dimensions as applicable to the SAMA and SANWC sample populations. The findings related to the four dimensions clearly indicated that there was an identifiable pattern across the two sample population groups. Furthermore, the percentages presented in the tables that follow were extracted from the original COQ dimensions for SAMA and the SANWC. These percentages display the responses of "strongly disagree" and "disagree" as combined. The same modus operandi was followed in the context of "strongly agree" and "agree". The discussion of the COQ dimensions in the section that follows refers only to the highest percentage for each sample population group. This section is therefore not a reiteration of the content presented in Chapter 6, but rather a discussion of scale items in relation to the context and the findings reported in the literature. Presenting the two sample groups in separate tables according to the dimensions allows for the triangulation of the findings as the discussion entails viewing them in context. The following sections provide a summary of the dimensions and discuss the context of the responses.

7.3.1 Dimension 1: Information-sharing culture in the organisation (SAMA and SANWC)

This section addresses the combined findings of the SAMA and SANWC participants related to the information-sharing culture in the organisation. A description of the combined findings is provided in Table 7.2.

Table 7.2: Information-sharing culture among SAMA and SANWC population groups

Statements	Disagree/ strongly disagree (SAMA)	Disagree/ strongly disagree (SANWC)	Agree/ strongly agree (SAMA)	Agree/ strongly agree (SANWC)
Q1: I feel that it is safe to share information on social media.	79%	60%	19%	8%
Q2: I feel that my personal information is important.	6%	4%	93%	62%
Q3: I feel passwords are enough to protect my personal information stored on my work computer/ laptop.	64%	43%	36%	25%
Q4: I feel that using a storage device (USB) is the best way to store information.	63%	37%	36%	30%

Statements	Disagree/ strongly disagree (SAMA)	Disagree/ strongly disagree (SANWC)	Agree/ strongly agree (SAMA)	Agree/ strongly agree (SANWC)
Q5: I change my passwords on my laptops, cellphone, and computer on a regular basis.	41%	20%	58%	47%
Q6: I feel safe using free Wi-Fi at public places.	78%	56%	21%	12%
Q7: I sometimes connect my cellphone or laptop to a public Wi-Fi connection.	41%	34%	57%	34%
Q8: I feel comfortable posting about my personal life on social media.	87%	62%	12%	6%
Q9: I feel comfortable posting information about my workplace activities on social media.	90%	64%	7%	3%
Q10: I feel that my work should have more cybersecurity awareness campaigns.	11%	4%	86%	63%
Q11: I have read about an information-sharing policy in my workplace.	23%	15%	74%	52%
Q12: I feel that my workplace should implement an information-sharing policy.	8%	2%	89%	66%
Q13: I am aware of guidelines at my workplace promoting cybersafety.	25%	20%	73%	48%

The scale items in the COQ for the SAMA and SANWC sample population groups indicate unambiguously that a clear pattern emerged in Dimension 1, which focused on the information-sharing culture in the organisation. For the most part, the respondents from SAMA and the SANWC gave consistent responses. The respondents were of the view that it was not safe to share information on social media sites, which indicated that a level of security awareness prevailed among the respondents. Users' perceptions of sharing information in cyberspace could be linked to factors such as awareness and knowledge. The researcher argues that the presence of these factors might facilitate Internet users to be more aware of the space they are navigating, which means they might be able to anticipate cyberthreats. In addition, the respondents also felt that their personal information was important, which might imply that the ill-considered exchange of personal data in cyberspace might leave users vulnerable to being exploited.

Questions 3 to 7 focused on practising information security in the organisation by specifically considering the user's behaviour. The responses from each of the sample population groups clearly showed that users felt their passwords were insufficient to secure their information. This emphasises the limitations of security as users were aware of their own security-related vulnerability against the background of cybersecurity. The aforementioned outcome also allowed the military officer to become aware of possible security measures that could be used to mitigate potential risk. The respondents in both sample groups furthermore agreed that they changed their passwords regularly, which might also point to self-responsibilisation[38]. Questions 6 and 7 suggested that the SAMA respondents were aware of the potential threats attached to connecting to an unsecured wireless network. To the contrary, the SANWC respondents presented mixed views, which possibly indicated questionable security practices.

In addition, the participants indicated that the organisation needed to do more concerning cybersecurity awareness, as pointed out in Question 10. It is thus argued that the organisation should emphasise enhancing the security awareness of personnel by evaluating security behaviours and information security practices and using this approach as a platform to improve current systems. The findings in this regard pointed out that both sample populations acknowledged the existence of vulnerabilities in their information security practices, such as the storage of data and password management.

The last three questions in the first dimension referred to the respondents' knowledge regarding information-sharing policies in the organisation. The overall responses from these three questions (Questions 10 to 13) suggested that most respondents were aware of the existence of such policies in the organisation. However, some responses showed mixed views regarding the awareness of such policies. When broadening this view to include the armed forces context, then operational activities in the mission area and day-to-day functioning of members also require information to reach the desired cybersecurity objectives.

[38] Self-responsibilisation refers to the dynamic where users become aware of their own security flaws and possibly change their attitude to mitigate unintentional security risks (Pollini et al., 2021).

Questions 10 to 13 showed that there was overall awareness relating to information security and the sharing of data in a personal and professional capacity. The policy and formal procedural questions in Dimension 1 indicated that the respondents were largely aware of policies being circulated in the organisation. The section that follows, including Table 7.3, deals with Dimension 2, which focused on the security orientation of the respondents located at SAMA and the SANWC.

7.3.2 Dimension 2: Security orientation among military officers (SAMA and SANWC)

This section addresses the combined findings of the SAMA and SANWC respondents related to security orientation. The description of the combined findings is provided in Table 7.3.

Table 7.3: Security orientation among the SAMA and SANWC population groups

Statements	Disagree/ strongly disagree (SAMA)	Disagree/ strongly disagree (SANWC)	Agree/ strongly agree (SAMA)	Agree/ strongly agree (SANWC)
Q18: When I use the Internet, I am aware of the dangers of cyberthreats/ attacks.	7%	5%	90%	60%
Q19: I feel that information security is important in my workplace.	2%	4%	94%	62%
Q20: When I feel unsafe using the Internet, I decide to log out.	13%	6%	82%	59%
Q21: I sometimes save my personal information on my work laptop or computer.	53%	30%	43%	37%
Q22: I am aware of technology that can be used to hack devices in my workplace.	43%	35%	53%	32%
Q23: I update myself with cybersecurity issues.	35%	34%	60%	32%
Q24: I sometimes try to include cybersafety guidelines in my workplace.	41%	29%	54%	38%
Q25: I know of colleagues who have had their personal or work laptops/computers hacked.	42%	38%	55%	30%

This section highlights the pattern observed in the data across the SAMA and SANWC sample population groups. The focus of Dimension 2 was on how well the respondents orientated themselves to practices concerning adherence to cybersafety guidelines, as well as to what degree they were aware of cybersafety issues. Based on the pattern that emerged from Dimension 2, it was evident that the respondents were aware of cybersecurity threats and that information security was important to them. Viewing this finding in context, the responses showed that the respondents embraced responsibility as active agents in the cybersecurity process. The argument can be made that those respondents who indicated that they were aware of cybersecurity threats might have a strong sense of security behaviour in cyberspace. It is worth noting that the findings presented for Questions 21 and 22 revealed that the respondents made reference to devices that could be used to hack into computers or perform data breaches in the organisation, which clearly indicated a distinct dissonance between the responses of the SANWC and SAMA sample population groups.

There was a level of awareness in both sample population groups, yet the practice relating to how information security was performed and how users orientated themselves with the practice differed in the SANWC population sample. It emerged that, based on the responses to Question 23, the respondents from the SANWC were less likely to update themselves on cybersecurity issues than those at SAMA. Based on the responses to Dimension 2, the junior SAMA population group probably possessed more cybersecurity awareness and, with regard to certain aspects, might have orientated themselves better in cyberspace and with practices relating to cybersecurity. Yet, the responses to Questions 23, 24, and 25 made it apparent that attempts to obtain knowledge on issues on cybersecurity were not performed regularly, which might pose security-related challenges to the organisation and to them as individuals. It also became clear that the SANWC respondents were less aware of security incidents that had occurred in the case of their colleagues[39]. This could be an indication that the exposure to cyber and to information relating to cybersecurity might be limited[40]. It is therefore of key importance for personnel to remain up to date with relevant security risks and possible threats that members of the military might encounter in a professional or personal context.

[39] See Alotaibi et al. (2017) in Chapter 2 on the increased vulnerability linked to cybersecurity awareness and the possible increase in human error.

[40] See Daengsi et al. (2021) on how training and prior exposure to cyber may facilitate awareness.

Alternatively, the researcher also formed the view that the sample population groups might have interpreted the risk factor differently. When perusing the responses where disagreements between the SANWC and SAMA sample groups were recorded, it was relevant to note that if users were to share information more frequently, based on the idea that they felt comfortable using the Internet, then the argument derived from the responses in this dimension could possibly focus on personality and sense of risk.

7.3.3 *Dimension 3: The officers' view of cybersecurity for SAMA and SANWC respondents*

This section addresses the combined findings related to the SAMA and SANWC respondents' views on cybersecurity. A description of the combined findings is provided in Table 7.4.

Table 7.4: SAMA and SANWC military officers' view of cybersecurity

Statements	Disagree/ strongly disagree (SAMA)	Disagree/ strongly disagree (SANWC)	Agree/ strongly agree (SAMA)	Agree/ strongly agree (SANWC)
Q29: I feel that the Internet is safe to use.	56%	24%	40%	33%
Q30: I am aware of the cyberthreats that are affecting the workplace.	25%	25%	70%	44%
Q31: I am aware of cyberattacks that have happened in my workplace.	59%	42%	38%	26%
Q32: I feel that all my work colleagues should learn the skills that can help them fight cyberthreats at work.	3%	2%	93%	68%
Q33: I feel that the cybersecurity guidelines in my organisation will not limit the duties and tasks of military officers.	16%	10%	78%	58%
Q34: I feel that there is a need for the military to control cyberspace.	7%	5%	88%	60%
Q35: I feel that all Internet activity in my workplace should be monitored to prevent cyberthreats.	10%	4%	86%	64%
Q36: I feel that monitoring the Internet at my work will	16%	7%	81%	60%

Statements	Disagree/ strongly disagree (SAMA)	Disagree/ strongly disagree (SANWC)	Agree/ strongly agree (SAMA)	Agree/ strongly agree (SANWC)
change how people think of cybersecurity.				
Q37 I feel that all my colleagues are informed of cyberthreats or attacks in our workplace.	58%	47%	37%	21%
Q38: I feel that the organisation pays attention to cyberthreats and attacks in the country.	45%	40%	50%	28%
Q39: I feel that cyberspace is a new space to carry out warfare.	11%	4%	85%	64%
Q40: I feel that my work colleagues are aware of the cybersecurity guidelines in our workplace.	50%	41%	45%	27%
Q41: I am aware of my colleagues who are knowledgeable about cybersecurity.	30%	19%	65%	47%
Q42: I am aware of the consequences of cyberthreats for the organisation and the country.	17%	11%	77%	56%
Q43: I feel that cyberthreats cannot harm the workplace.	84%	62%	10%	4%
Q44: I feel that all officers in my workplace should be aware of the effects of cyberthreats.	6%	0%	90%	66%

Dimension 3 focused on the respondents' view of cybersecurity and the general feeling towards how the organisation approached cybersecurity. The findings in this dimension revealed that, generally, the participants were aware of cyberthreats in the organisation. Most respondents indicated that they were not aware of cyberattacks that have occurred in their organisation. The researcher considers this as a point of importance as the respondents showed their ability to differentiate between threats in the organisation and previous attacks that had taken place. The responses also showed that there was a need for cybersecurity training and education in the workplace[41].

[41] See Fatokun et al. (2019) in Chapter 2 on the education of online users concerning cyberthreats.

Most respondents highlighted that cybersecurity policies and guidelines would not deter them from performing their duties. It is argued that, in context, policy is an important guiding factor in the way that personnel can engage with their organisational duties. The onus is therefore on military members to display the element of understanding these policies and regulations. Furthermore, the perception of how colleagues complied with policies was a further point that emerged as one that requires attention. In reference to Questions 40 to 42, for example, it was evident that most respondents viewed some of their colleagues as not complying with organisational cybersecurity polices and guidelines. The link between awareness of online threats and awareness of policy was clear in the responses to Question 42, which suggested that most respondents from SAMA (77%) and the SANWC (56%) were aware of the consequences associated with a lack of compliance with cybersecurity guidelines in the organisation.

Furthermore, there was a difference between how the SAMA and SANWC respondents viewed organisational priority to cyberattacks and threats that may occur in South Africa (see Question 38)[42]. The DoD’s annual report for 2020/2021 (RSA, 2020b) highlights the development of cyber capacity throughout the organisation. However, with regard to the importance that has been attached to the concept of a cybersecurity agenda being promoted throughout the organisation, it fell well below the main agenda items, which were to increase capacity and enhance facilitating infrastructure to combat the country’s digital space (RSA, 2015a). When viewing the DoD’s annual report for 2020/2021 (RSA, 2020b), it became evident that the COVID-19 pandemic had received priority. Cybersecurity as an emerging threat had thus temporarily made way for a more existential security issue that threatened health security as an important domain of human security.

In focusing attention on the COQ, most respondents from both SAMA and the SANWC felt that the SANDF should be the dominant actor in cyberspace. This was presented in Questions 34 and 35. Whereas Question 34 dealt with the armed forces’ monitoring of cyberspace, Question 35 focused on the role of monitoring of devices in the workplace to act as a mitigating factor in the way that users navigate cyberspace. In Question 35, there was agreement by both sample populations that Internet activity

[42] See discussion by Nævestad et al. (2018) in Chapter 2 on the role of support by management and the element of awareness.

should be monitored. This could also be linked to Sub-theme 3.2, which centred on how military officers considered the use of their personal devices to engage in communication and for reasons of information storage and day-to-day work activities.

The factors proposed by Alotaibi et al. (2017), as presented in Chapter 2, were consistent with the findings derived from Sub-theme 3.2, which showed that the respondents were sometimes required to communicate by means other than the official and prescribed format. It was therefore found necessary for military officers to be more flexible about the technological devices they use and the way traditional conceptualisation of military communication has thus far been conducted.

The researcher argues that one of the reasons for the use of personal devices could be ascribed to the risk of the organisation actively monitoring network activity[43]. The responses to Question 35 and the concomitant qualitative theme presented a contradiction and therefore needed additional exploration. Moreover, it was noted in the responses that monitoring of the Internet in the workplace should be carried out by the organisation. At the same time, most respondents indicated that the monitoring of the Internet might alter their online behaviour. This would leave the organisation in a precarious position. In terms of policy linked to DoD Instruction DODI/CMI/00008/2001 (RSA, 2011a), all military personnel who access devices and DoD networks will be monitored, which is to ensure that there is a clear audit trail of all Internet activity. Furthermore, it is evident that respondents from the SANWC felt that the organisation performed well in prioritising cybersecurity, whereas those from SAMA felt that the organisation did very little to deal with cybersecurity, which linked up with the next dimension, namely the respondents' behaviour in cyberspace.

7.3.4 Dimension 4: Cybersecurity posture in the organisation of SAMA and SANWC military officers

This section addresses the combined findings of the SAMA and the SANWC participants related to the cybersecurity posture of SAMA and SANWC military officers. The description of the combined findings is provided in table 7.5.

[43] It can be argued that the monitoring of employee Internet use may be problematic in many respects; the first issue being that the organisation might encroach on privacy. Internet use by personnel might be a mitigating act to ensure that personnel are protected against possible vulnerabilities or threats (Moussa, 2015).

Table 7.5: The cybersecurity posture of military personnel at SAMA and the SANWC

Statements	Strongly disagree/disagree (SAMA)	Strongly disagree/disagree (SANWC)	Strongly agree/agree (SAMA)	Strongly agree/agree (SANWC)
Q45: I feel that I behave the same on the Internet when I am at home or at work.	39%	20%	7%	47%
Q46: I feel that knowing about cyberthreats may change how I communicate with others.	11%	3%	85%	64%
Q47: I feel that using free software to fight cyberthreats and attacks in my workplace is unsafe.	21%	11%	74%	56%
Q48: I feel that my workplace should develop their own software to fight cyberthreats and attacks.	6%	6%	90%	60%
Q49: I feel that a cyber education programme for all members will increase cybersecurity in my workplace.	3%	0%	93%	66%
Q50: I feel that education and training will help to change the security behaviour of members in my workplace.	2%	0%	93%	66%
Q51: I feel that cyber-related education should be included in some of the work training programmes.	2%	0%	93%	66%

Dimension 4 displayed agreement on how the participants replicated their personal online security behaviour in their professional context. The findings of Dimension 4 strongly showed that obtaining knowledge of and training in cybersecurity threats would influence how the participants interpreted and adjusted their online security behaviour. Most respondents from SAMA and the SANWC indicated in Question 45 that their online security behaviour could be applied to both their personal and professional or working context[44].

The findings also showed that there was a need to develop software and tools for the SANDF to combat cybersecurity threats (see Questions 47 and 48). Linking the scale items attached to the aforementioned interview theme, it was suggested that respondents might consider utilising their own software on personal devices in

[44] See argument by Ertan et al. (2018) in Chapter 2 on habitual behaviour and its impact on security culture.

organisational settings to protect them and their information against malicious software. Providing efficient platforms might inspire users to have greater confidence in the organisation's ability to address cybersecurity threats[45].

In addition, the aforementioned alluded to the notion that the participants functioned in a blended digital lifestyle that incorporated both their professional context and personal lives. The overall response to the questions related to education and training in cybersecurity (Questions 46, 49, 50, and 51) was that a dire need existed for programmes to target the online security behaviours of personnel in the organisation. The researcher is of the view that incentives might also assist with how users respond to cybersecurity threats. The overall findings in this dimension showed that the respondents had indicated the need for cybersecurity training. Training, once completed, might have an impact on the way officers engage in communications with others, and might also contribute to assisting other colleagues in the SANDF to enhance their cybersecurity skills set. The respondents recognised behavioural change after training as a consequence of receiving education and training. The next section focuses on the themes extracted from the short narratives attached to the COQ.

7.4 Discussion of themes extracted from the short narratives of SAMA and SANWC military officers

This section presents a discussion of the themes extracted from the short question responses of the COQ. These short question responses were a combination of the SAMA and SANWC sample population group.

7.4.1 Theme 1: Information sharing on best practices requires implementation

The findings attached to this theme showed that the SAMA and SANWC respondents were of the view that cybersecurity was relatively new to the organisation and required some adaptation on the part of the organisation. This theme also identified that information-sharing practices and measures were often not implemented in the organisation. This might consequently have an impact on how military officers in the

[45] See the discussion in Chapter 2 by Patil and Joshi (2014) on the use of antivirus software and the role of the user in maintaining online cybersecurity.

armed forces perceive sharing of official information on digital platforms. When referring to the findings and placing them in context, it is worth noting that the information-sharing practices could also be linked to organisational culture[46].

7.4.2 *Theme 2: Cautionary behaviour is linked to the navigation of cyberspace*

This theme centred on the SANWC and SAMA participants describing their online security behaviour as cautious. The findings related to Theme 2 showed that most of the respondents were very vigilant when navigating cyberspace. However, there were some military officers who considered their behaviour as relaxed. The majority of the respondents indicated that being aware of threats in cyberspace allowed for adequate preventative measures to be employed. The findings therefore implied that most participants were aware of cyberthreats, which could explain why the participants were vigilant in cyberspace and how they practised online security behaviour. It could also be argued that the participants had had some level of exposure to cybersecurity information but not necessarily training. Furthermore, to elevate the level of risk awareness of employees who already have a basis of knowledge on cybersecurity, the management of the organisation should consider using simulation and case studies, as well as regular feedback sessions, about potential threats.

7.4.3 *Theme 3: Cybersecurity training and education as a way to enhance security measures*

This section focuses on the need for the organisation to provide training and education in cybersecurity for all members in the organisation, irrespective of rank. The argument can be made that cybersecurity awareness training is an essential part of understanding how personnel perceive risk in organisations[47]. The researcher argues that a delay in training and a lack of clarity might moreover result in management not considering the acquisition of security management tools and technology. The identification of cybersecurity awareness training by the respondents also concerned the involvement of senior management in the organisation. The researcher argues that if there was a lack of training in and awareness of cybersecurity, it might take some

[46] See Al-Dawod and Stefanska's (2021) discussion in Chapter 2 regarding organisational culture and its impact on perceptions and how this impacts information sharing and prior exposure to cybersecurity training.

[47] See Al-Dawod and Stefanska's (2021) discussion in Chapter 2 on the role of the human factor.

time to understand and obtain clarity regarding a cybersecurity-related incident[48]. This argument could be extended by suggesting that a delay in training and a lack of clarity on cybersecurity might prolong the acquisition of security management tools and new technology in the organisation.

7.4.4 Summary of section

This section provides a summary and contextualisation of the research findings by highlighting several key points. The data presented in this section showed that information often overlapped, which confirmed certain aspects of the focus in this section, including a discussion of the findings in relation to the research questions. Four key points emerged from this process, which can be expressed in a summary that incorporates the short question responses and responses from the scale items:

1) The SANWC respondents appeared to present more problematic behaviour as some of the members did not practise cybersecurity awareness. The SAMA respondents, on the other hand, indicated having cybersecurity awareness and they practised online security behaviour. However, there were some SAMA respondents who considered their online security behaviour to be carefree. Furthermore, both the SAMA and SANWC respondents indicated that they were aware of cyberthreats and their implications. However, there was a balanced view in responses from the SANWC respondents concerning the practice of security when attempting to connect their devices to open-source connections (Wi-Fi). The responses to the COQ short questions also showed a variety of views relating to online cybersecurity practice.
2) The conceptualisation of cybersecurity awareness among the SANWC and SAMA respondents appeared to be that the Internet should be navigated with caution, which included the associated security behaviour. Most respondents viewed the Internet as a space that should be navigated with caution. However, at the same time, both the SANWC and SAMA respondents acknowledged that they had colleagues who were not aware of a cybersecurity policy in the workplace. The findings of the COQ also showed

[48] See Prevezianou's (2021) discussion in Chapter 2 on the role of awareness regarding the understanding of a threat.

that the interpretation of risk differed among the respondents from SAMA and the SANWC. This might point to a larger organisational issue, namely identifying the perception that cybersecurity was not a priority. It can therefore be said that if the organisational culture surrounding cybersecurity is not highlighted by senior management, it might not be considered important by the rest of the personnel.

3) In terms of security behaviour, the SAMA and SANWC respondents were of the view that cybersecurity threats could pose security challenges for the organisation. The combined responses of the two sample groups indicated that stricter security measures needed to be implemented in the organisation. Overall responses related to the SANWC indicated that the majority of the respondents did not update themselves about cybersecurity tools that could be used to cause data breaches or commit other forms of hacking. Most respondents from the SANWC were also distrusting of others when sharing information in cyberspace and considered the space to be dangerous. Furthermore, a minority of the SAMA respondents used social media platforms to update themselves with information. A similar response was found in the SANWC respondents' answers to the short questions, where a few respondents indicated that they only used the Internet when absolutely necessary. However, the general response among the respondents was that cyberspace required security behaviour that was characterised by being cautious. This might also point to the frame of reference of the topic and the amount of exposure to issues pertaining to cybersecurity in the workplace.

4) The majority of the respondents in the SAMA and SANWC sample population groups were of the opinion that cybersecurity training and education were limited and had been identified as a gap in the training needs of military members. The responses to the short questions indicated that most respondents considered the priority accorded to cybersecurity in the organisation as very low. Additional responses to the short questions, where most respondents indicated that limited information security awareness existed in the organisation, supported this finding. However, some respondents acknowledged that there was a culture of information security. Through the lens of the military officer, it is important to indicate that the SANWC and SAMA respondents agreed that all military officers should be

> made aware of cybersecurity threats. This might be an indication that if adequate threat information was not received in a professional context, the participants would seek and obtain security elsewhere, in their personal capacity. Such a situation might also be an indication that clarity was required regarding organisational policies relating to information security and information sharing, as well as cybersecurity. In addition, the indication of a training and education deficit means that a lack in this regard should be resolved (see Question 38). Furthermore, the short questions of the COQ showed that there was not only a need to introduce cybersecurity education to the entire organisation, but also to educate personnel about the policies and directives in use. This would help to eliminate the root of the existing uncertainty.

The section that follows engages in a discussion on answering the research questions in relation to the findings presented in the sections presented above.

7.5 Discussion of the research questions

The previous section presented the summary and contextualisation of the findings across Phases 1 and 2. This section discusses the study’s three secondary research questions, following the sequence of these research questions presented in Chapter 1, and relates them back to the introduction to this chapter. RQ1 focused on how South African military officers conceptualised cybersecurity awareness and also centred on the aim of the study, namely exploring the perceptions of cybersecurity among military officers in the SANDF. RQ2 focused on how South African military officers perceived cybersecurity threats by specifically pointing to aspects relating to how they perceived threats and the implications of this in context. RQ3 focused on the elements attached to the military officers’ views of cybersecurity awareness in the organisation to determine how the military positioned itself within the broader issue of awareness creation in the organisation. The researcher consolidated the findings of the SANDC, SAMA, and SANWC respondents and created indicators to answer the three secondary research questions. The indicators in the model that was created linked with the main research question, accompanied by the three secondary research questions, as a guide to answering the main research question. The indicators used in this discussion are as follows: (1) information-sharing practices in the organisation,

(2) awareness of best practices and policy directives in the organisation, (3) awareness of online threats and perceived awareness of self in cyberspace, (4) cybersecurity training and skills development, and (5) trust in organisational processes and efficiency in technology use.

7.5.1 How do South African military officers conceptualise cybersecurity awareness?

This discussion of RQ1 is based on four indicators, which were extracted from the overall findings obtained in Phases 1 and 2 of the study, and which had been consolidated.

Indicators 1 and 2 in the findings of the study indicate that SANDC participants perceived cybersecurity initiatives in the organisation as requiring to be dealt with urgently, which could also be equated with cognisance that the technology should adapt to and keep abreast of the current times. The SANDC participants nonetheless acknowledged a measure of progress with establishing a digital culture in the organisation. However, they were dissatisfied with how members handled securitising information on digital platforms. Furthermore, these participants also considered browsing the Internet as a risk as it is a dangerous environment that requires a sense of caution and vigilance. In addition, the SANDC participants showed that cautiousness prevailed in dealing with new technology in the workplace and how colleagues approached cyberspace. The researcher noted that the participants at the SANDC were very suspicious of how other military personnel operated in cyberspace. This behaviour was characterised as failing to show an interest in the applicable policies and best practices in the organisation. Moreover, the participants in the SANDC sample also considered cybersecurity awareness training as important in the organisation. Adding to this, the COQ scale item findings showed that the SANWC and SAMA respondents also considered it necessary for military members in the organisation to receive cybersecurity awareness training and forming a hierarchy of support.

Addressing Indicator 3, it emerged from the findings that the SANDC participants and the SANWC and SAMA respondents replicated security behaviour in their personal and professional contexts. These SANDC participants and SAMA SANWC respondents mostly complied with vigilance-related features when navigating cyberspace. This revealed a foundation of existing security knowledge in all three sample population groups, as displayed through the cautiousness attached to information sharing on the Internet. The notion of caution was also present in the SANDC findings. The responses to the COQ's short questions and respective scale items also revealed that most SAMA and SANWC respondents were cautious when using the Internet and engaging in information-sharing practices. In addition, it is argued that there is a link between how cybersecurity was practised among respondents from the three sample population groups and the knowledge that had been acquired about cyberthreats and precautionary methods. However, it was worth noting that a minority of SAMA respondents considered their security behaviour as relaxed. Where cybersecurity training had been indicated by the three sample populations as limited in the organisation, it might be possible that previous security training had been acquired in a personal setting or aspects of information security had been included in a previous military training course.

This view also supplemented how the respondents (SANDC and SANWC senior military officers) perceived the junior members of the military in the organisation, namely as relaxed regarding security behaviour. The researcher submits that, based on the four indicators used to answer RQ1, the respondents perceived the overall cybersecurity awareness initiatives as limited and felt that the organisation should be more active in implementing awareness programmes. This showed that the respondents were cognisant of their training needs and the magnitude of the threats that are quickly multiplying in the country. The SANDC participants and SAMA and SANWC respondents also provided insight into the repercussions of cyberthreats and attacks. Although most respondents who had completed the COQ reported that they were aware of threats, some SAMA and SANWC respondents were not aware of attacks that had previously occurred.

Linking the findings to Indicator 3, RQ1 centred on the role of cybersecurity awareness through the lens of the South African military officer. The themes that emerged from Phases 1 and 2 suggested that cybersecurity awareness was considered a challenge in the organisation as some members were unable to access the available training. Theme 1, *Knowledge production and training focusing on cybersecurity awareness*, generally indicated cybersecurity awareness among the participants, which included cyberthreats, yet the organisation appeared to be doing very little to increase opportunities for the educational advancement of the participants. Sub-theme 1.1, *Information security requires devotion*, located in the thematic component of the COQ (short questions), highlighted a perceived lack of commitment by the organisation concerning cybersecurity. The sub-theme under discussion made specific reference to the cultivation of a cybersecurity culture among respondents. By linking the main theme, as it emerged from the CA, with the aforementioned sub-theme derived from the COQ, it was clear that the respondents considered the drive required for creating cybersecurity awareness as stalled.

7.5.2 How do South African military officers perceive cybersecurity threats within the SANDF?

This discussion of RQ2 is based on one indicator, which was extracted from the overall findings obtained from Phases 1 and 2 of the study and thereafter consolidated. Indicator 3 was considered in answering RQ2.

RQ2 focused on the participants' and respondents' perception of cybersecurity threats. Indicator 3 for online security behaviour showed that respondents from the SANWC and SAMA both indicated the inclination to take security precautions when they encountered a threat or online situation that made them feel vulnerable. Furthermore, it was suggested, based on the risk information that the participants and respondents previously obtained through available policies or directives, that this could have assisted these military officers to make an assessment of security flaws, which might in turn have had an impact on the online security behaviour they had expressed. The perception of risk was therefore crucial for identifying threats and to determine when online platforms presented a risk. Moreover, senior military officers at the SANDC linked physical security to digital security (see Theme 4 in Section 7.2). This theme also emphasised how SANDC participants navigated the physical domain by not connecting their devices to public Wi-Fi networks. The construction of threats among SANDC participants was linked to the physical domain, which indicated that they were synchronising online security behaviour with their physical environment. In addition, this could be corroborated by the behaviour of the SANDC participants (senior military personnel), which was characterised by vigilance in respect of technology and their colleagues. The SANDC-derived themes, when tested, also suggested that a skills gap existed between junior and senior officers. This appeared to be owing to the difference in how technology and the Internet were used in the workplace but also how senior officers perceived junior officers. This difference in perception further challenged the notion of how best practices might be interpreted and executed, as well as how the official means of communication were complied with. However, the general indication of the responses from the three sample groups was that the participants and respondents were overly cautious when sharing and communicating information online. However, there were some respondents in the SAMA group who characterised their security behaviour as relaxed. Similarly, there were also some respondents from the SANWC who indicated that they connected their personal devices to open public Wi-Fi connections. Advancing knowledge of cybersecurity issues might allow for better threat perception and self-assessment of the potential vulnerabilities relating to the human element.

The findings showed that the SAMA and SANWC respondents were aware of the threats to the organisation. In addition, the SANWC and SAMA respondents were also aware of their own security behaviours. This section relating to RQ2 thus concluded that military officers at SAMA and SANWC were aware of cyberthreats and might have the necessary knowledge to form adequate deductions regarding possible threats. The findings derived from the SANDC participants, however, were characterised by additional caution. The findings also showed that participants from the SANDC perceived junior military members as not using cyberspace effectively. This might also be linked with vigilance and trust relating to colleagues and security practices.

Viewing the findings in the context of RQ2, the researcher argues that when participants are suspicious of one another and the guidelines that safeguard members of the military, it might also have an impact on the cybersecurity culture, which might in turn influence how they perceive threats. On the other hand, the respondents from SAMA and the SANWC viewed the practice of cybersecurity as one that required vigilance. In addition, a clear misconception emerged regarding how senior participants viewed junior military members’ way of practising cybersecurity. This might have an influence on threat construction, and the way that a cohesive culture is framed around the sharing of information and how cybersecurity is practised. Moreover, it could be argued that while the senior participants’ perception was framed around junior participants’ careless way of sharing information and interacting with outsiders, the perspective of junior SAMA respondents showed a different view. The SAMA participants considered their behaviour relating to information sharing and technological use as safe. However, the SANDC participants' narratives indicated that their online security behaviour was generally less safe than that of the junior SAMA respondents. The researcher therefore argues that junior-ranking respondents from SAMA were more comfortable with using technology and the Internet. The researcher submits that senior participants located at the SANDC and senior respondents at the SANWC displayed an entrenched sense of cautiousness, which could be ascribed to apprehension about using new technology in the workplace and the scope of exposure to cyberspace. Furthermore, while the SANWC respondents acknowledged some perception of cybersecurity threats in the workplace, they were unable to indicate any devices that could be used for hacking into computers in the organisation. This finding could indicate a security risk and a void in cybersecurity knowledge at the senior management level.

7.5.3 What are the perceptions of cybersecurity awareness through the lens of the military officer?

This discussion of RQ3 is based on two indicators, which were extracted from the overall findings obtained in Phases 1 and 2 of the study and thereafter consolidated. Indicators 2 and 3 were considered in answering RQ3.

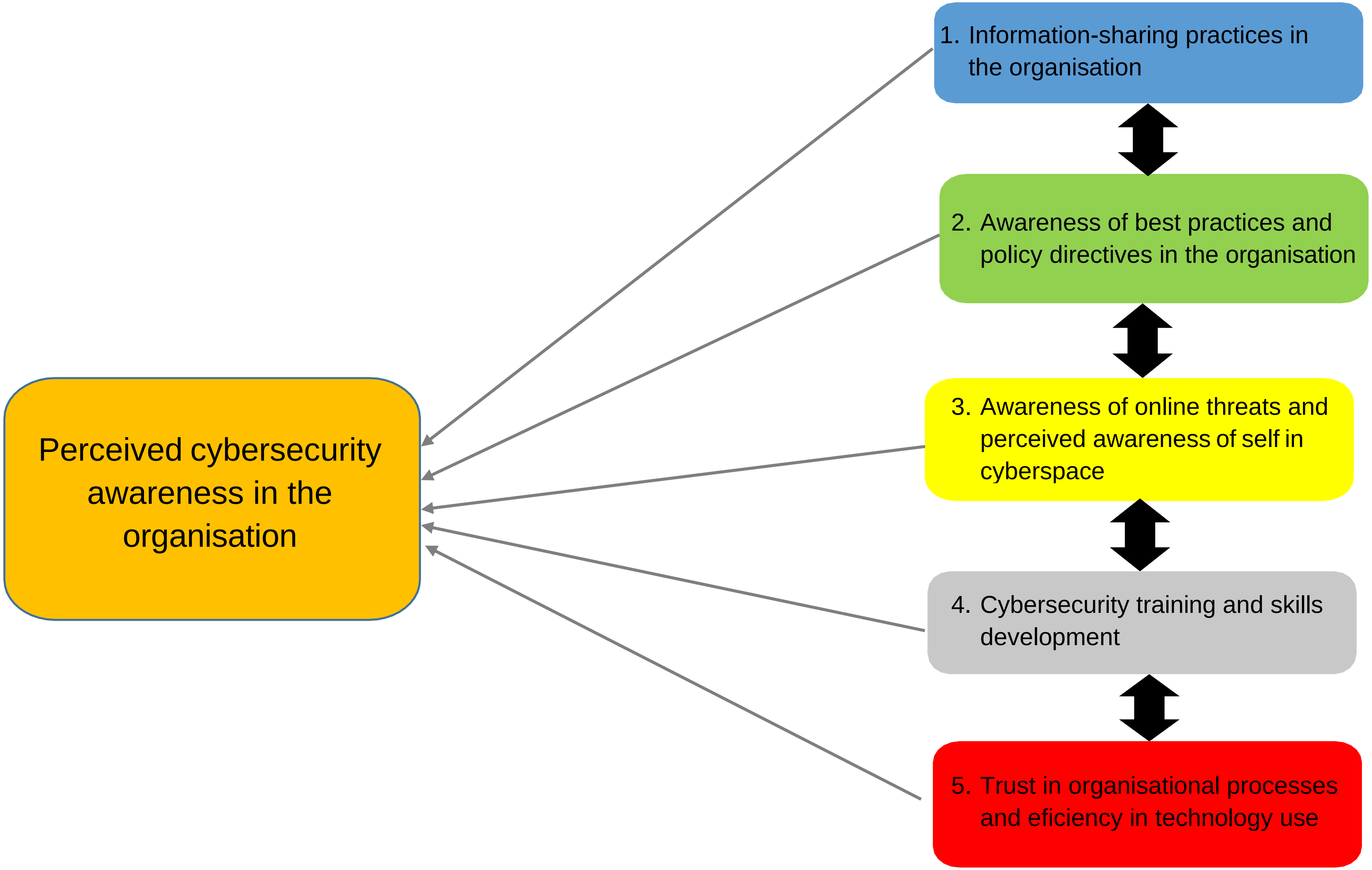
The findings of the COQ scale items for the SANWC and SAMA respondents indicated that there was a level of cybersecurity awareness among military officers, although the implementation of awareness guidelines and official best practices was less encouraging. Moreover, based on the indicated levels of awareness of cybersecurity, the SAMA and SANWC respondents indicated that they applied this awareness in their information-sharing practices and their security behaviour. Linking these findings relating to RQ3, the SAMA and SANWC respondents were found to be generally aware of the guidelines concerning cybersecurity awareness. A connection could be made between knowledge of guidelines and security behaviour online. This connection was based on the aforementioned findings derived from the dimensions of the COQ. Furthermore, when investigating the themes of the COQ, it became clear that a sense of caution prevailed among these respondents when they used the Internet.

Relating the COQ short question findings to the implementation of information-sharing policies and best practices, most of the respondents from the SANWC and SAMA indicated believing that there was an apparent lack of policy implementation relating to information security practices. This statement could be corroborated by the SANDC participants, as the thematic aspects pointed out uncertainty of best practices and protocols. Whereas the SANDC participants emphasised uncertainty in the application of guidelines and practices in this theme, it nevertheless contextually emphasised an overall lack of policy application, which questioned the implementation factor in organisational governance. When guidelines are not clear, the concomitant void may have an impact on the understanding and knowledge of the technological devices personnel might utilise in the organisation. Moreover, the findings showed that the aforementioned might also influence the measure of clarity about using personal devices to communicate organisational information. Considering an information-sharing culture and the practices associated with it, the SANDF participants displayed general mistrust relating to their colleagues' use of technology (Internet use and security behaviour). The existence of a limited digital culture was confirmed in the responses to the COQ's short questions. In addition, concerning culture, while it was indicated that this matter received limited attention in the organisation, it nevertheless offers a platform where a cybersecurity culture can be enhanced through communication between upper management and lower-ranking members of the military. The level of importance attached to the promotion of guidelines and best practices in an organisation might also have an impact on the construction of security and the level of skills imparted to employees. In this vein, the overall findings related to best practices in the organisation suggest that the participants and respondents were aware of policies and guidelines. However, the short questions affirmed a lack of implementation of cybersecurity best practices and that challenges with cultivating a cybersecurity culture were perceived.

7.5.4 Summary of research questions

The discussion of RQ1 focused on how South African military officers conceptualised cybersecurity awareness. Figure 7.1 points out how the findings derived from the SANDC, SAMA, and SANWC sample groups were linked to the secondary research question on how cybersecurity awareness was conceptualised by way of the various indicators that were also derived from the data. The researcher found five overlapping indicators pointing to the main research question, which was to determine the cybersecurity perceptions of South African military officers. The model presented in Figure 7.1 illustrates how the findings produced by the SANDC, SAMA, and SANWC respondents can be linked to RQ1, RQ2, and RQ3. It is important to note that the researcher constructed this model to capture how cybersecurity awareness can be viewed from the findings based on the five overlapping indicators.

Figure 7.1: Model of cybersecurity awareness among South African military officers


Perceived cybersecurity awareness in the organisation
1. Information-sharing practices in the organisation
2. Awareness of best practices and policy directives in the organisation
3. Awareness of online threats and perceived awareness of self in cyberspace
4. Cybersecurity training and skills development
5. Trust in organisational processes and eficiency in technology use

7.6 Indicators of cybersecurity awareness among South African military officers

The model of cybersecurity awareness among South African military officers is essentially a summary of the findings in a logical, condensed format, to enable the link between themes and scale items to be understood easily. Five identified indicators facilitated the exploration of military officers' perceptions of cybersecurity: (1) information-sharing practices in the organisation, (2) awareness of best practices and policy directives in the organisation, (3) awareness of online threats and perceived awareness of self in cyberspace, (4) cybersecurity training and skills development, and (5) trust in organisational processes and efficiency in technology use. Each of these indicators can be linked to the themes/sub-themes in Phase 1 and derived from the scale items and themes from the short questions in Phase 2. The model presented in Figure 7.1 thus connects the five indicators that inform the way that South African military officers perceive cybersecurity in the organisation.

7.6.1 Indicator 1: Information-sharing practices in the organisation

Two aspects in the model deal with an information-sharing culture and the overall conceptualisation of cybersecurity in the organisation. The researcher linked information sharing with aspects of organisational trust relating to cybersecurity, technological usage, efficiency in communication, and online behaviour. Information sharing in the context of the armed forces pertains to key strategic information that plays a role in successful military operational activities[49].

When turning the argument to culture in the organisation, the researcher maintains that the information-sharing culture was influenced by issues relating to how military officers in the organisation chose to adopt social media as their means of communication. This aspect is further influenced by the understanding and perceived view that personal devices were more efficient to use than the official means of communication. Moreover, junior respondents from SAMA were more inclined to use technology in the workplace. However, this use of technology also seemed to tie with the short question responses that highlighted a carefree and relaxed approach to

[49] See Marouf (2016) and Ertan et al. (2018) in Chapter 2 on the role of information sharing in organisations, as well as the role of senior management in this regard.

cybersecurity. Alongside this use of technology, stimulating unofficial forms of communication seemed to foster a better understanding of threats and the possible implications of sharing information online. In addition, the scale item findings derived from the COQ indicated that most respondents (SAMA and SANWC) were aware of cybersecurity guidelines in the workplace. This was supplemented by the responses to the short questions (COQ), where some respondents indicated that there was information security in the organisation. The SANDC participants' excerpts in Sub-theme 1.1, *Information security as a practice*, alluded to the general notion that cyberthreats could be harmful to the organisation. However, digital security management and how security was maintained appeared to be difficult.

In grappling with RQ1, the focus should be on those responses in the COQ dimensions that referred to how the participants perceived the cybersecurity behaviour of others in the workplace, and the perceived exposure others might have had to cybersecurity awareness. If an information-sharing culture defined by a lack of clear guidelines is present, this might distort the view of trust among personnel or trust in management. Sub-theme 4.1, *Vigilance among members of the organisation owing to differences in how cyberspace is approached*, drew directly on the level of trust among members of the organisation, but also provided a basis for the argument that trust was a factor in information sharing in the organisation.

The participants from the SANDC felt that a diminished sense of trust existed in the organisation, specifically of one another. It is important to note that SANDC participants, in their current ranking system, held senior positions as either wing managers or officers commanding in their respective units. The SANWC and SAMA respondents might not necessarily have been in a position of authority, with the required decision-making power to promote security agendas in the organisation. However, the respondents from the SANDC had the authority to promote information and agendas in their respective units as they were in a position of leadership, being officers commanding[50]. Vigilance is considered a topic that is viewed from a negative stance owing to the connotations of being alert from the individual perspective. Based on the psychology of being vigilant, it was surmised that a level of learning had taken

[50] See Siart et al. (2016) in Chapter 2 on the role of social status in hierarchical environments.

place, assuming that some trial-and-error events may have occurred prior to gaining experience. This is not in itself a negative but rather a positive view.

In addition, the majority of the participants noted that members of the military had a tendency to not share information with one another owing to their experience, which revealed that they had developed a certain level of vigilance. This highlighted the concept of trust in the organisation. The extract relating to this was included in Chapter 5 (which dealt with data analysis), which showed that there was some awareness that information had been posted on open-source applications such as WhatsApp. The extract pointed out that information might be used as leverage against personnel in the defence environment to exploit someone to gain sensitive information about ongoing operations in the organisation.

7.6.2 Indicator 2: Awareness of best practices and policy directives in the organisation

This indicator in the model was highlighted owing to the findings that pointed to the role of best practices and guidelines in the organisation. In addition, the indicator was an important factor in answering the research questions of the study as it framed the perception of cybersecurity awareness through the lens of South African military officers. The researcher argues that there is a link between awareness of cybersecurity threats and awareness of policy and guidelines regarding cybersecurity in the organisation. Knowledge and understanding associated with consequences emerged as a strong facet that influenced compliance with security guidelines among users.

The findings obtained from the COQ showed that the SANDC participants and SAMA and SANWC respondents were aware of cybersecurity guidelines and policies in the workplace (see Questions 11, 12, 13, 24, 40, and 42). In addition, awareness of directives and compliance with policy in the SANDF alluded to organisational governance possibly having an impact on the execution of best practices.

This indicator is important as the respondents indicated that policy and best practices were not clear in the organisation (see interview extract for Sub-theme 2.2: *The uncertainty of cybersecurity best practices and protocols in the organisation*). The respondents from the SANWC and SAMA sample groups highlighted that they had heard of a cybersecurity policy in the organisation, although a contradiction in the short questions emerged as the respondents reported the absence of such a policy.

This could therefore indicate a larger organisational issue and not necessarily how the individuals conceptualised cybersecurity in the organisation. The role of policy compliance in the SANDF can be linked to cybersecurity awareness training and it is therefore essential that the SANDF should enhance the training and awareness of its members in order to mitigate risks of human error.

The SANDC participants indicated uncertainty regarding best practices and guidelines, which tied in with the SAMA and SANWC respondents believing that their colleagues might not be aware of policies in the organisation. Both groups highlighted a challenge with the distribution of rules and regulations concerning cyber awareness. In addition, some SAMA and SANWC respondents noted that they were largely unaware of certain regulatory frameworks that might assist them in navigating cyberspace, whereas more senior military officers advanced that the policies and directives on cybersecurity were not clear[51]. When emphasising the link between policies and practising cybersecurity behaviour, the general impression gleaned from the data was that the SAMA and SANWC respondents indicated that the policies existed. Owing to the size of the SANDF, the argument could be made that not all directives or policies were shared in the same way. Filtering information across the organisation might therefore be a contextual challenge. In addition, where clear guidelines are lacking, it can influence how users interpret the approach to cyber as an emerging threat because of the impression that the organisation was not doing much about this. This impression could have been created by the unequal spread of information throughout the organisation, which might explain the differences in perception regarding policies and best practices. Moreover, the indicator relating to risk perception and online behaviour might also be linked to this factor on policies in that the unclear or unequal distribution of information might cause a change in attitude and perception about the matter.

7.6.3 Indicator 3: Awareness of online threats and perceived awareness of self in cyberspace

The findings showed that the respondents were aware of threats that originated in cyberspace. This is evident in the responses to the COQ dimensions.

[51] See Sub-theme 2.2, *The uncertainty of cybersecurity best practices and protocols in the organisation*, in Chapter 6.

Furthermore, the SAMA and SANWC participants were aware of security threats by practising behaviour that made them feel safe and maintained their perceived cybersecurity. The scale items (Questions 3 to 8) showed that the selected military officers were aware of the threats by displaying precautionary behaviour when they encountered a possible threat[52].

The researcher suggests that secure online platforms should serve as a basis for military officers to interact and share information with one another. Furthermore, it emerged from the SANDC findings that the organisation had not yet introduced new software to meet the need for efficient communication. This need was also expressed by a minority in the SAMA sample population group (see Appendix N). The findings of the COQ showed that some respondents were in favour of the SANDF advancing its own capabilities, instead of relying on software that was not owned by the SANDF itself[53].

The findings derived from the SANDC sample indicated that senior officers were critical of the behaviour of junior officers in terms of practising cybersecurity awareness through security behaviour. The data derived from the junior respondents from SAMA did not highlight this difference, nor did they indicate that senior members were less accepting of their online security behaviour. However, an element consistent across the three sample populations was that cybersecurity awareness should be developed and that management should make dealing with this growing concern a priority.

7.6.4 Indicator 4: Cybersecurity training and skills development

The findings indicated the necessity to develop the capacity of the SANDF concerning cybersecurity awareness. In addition, cybersecurity training and education programmes might be applicable to all members of the SANDF as navigating the Internet has become part of the organisation’s daily functioning. The SANDC findings related to Sub-theme 1.1 suggested a satisfactory level of cybersecurity awareness among the respondents as reference had been made to policies and how the SANDF should control this ephemeral space. The participants from the SANDC and respondents from the SANWC identified cyberspace as both potentially advantageous

[52] See Bulgurcu et al. (2010) in Chapter 2 on how security awareness is a potential indicator of security behaviour.

[53] Bălău and Utz (2017) highlight that organisations invest in this strategic activity to improve operational activities (see Chapter 2).

and as posing a risk. Sub-theme 1.2 highlighted that cybersecurity education training was required, with emphasis on accessibility by all. The majority of the participants in all three sample population groups indicated that there was a need to provide cybersecurity awareness training for military members.

In reference to Sub-theme 3.1, *Cybersecurity awareness training for the entire organisation*, it was clear that the management of the organisation should take note of the personnel's training needs, to advance their skills and knowledge of cybersecurity and orientation of the domain itself (see responses to Question 44 in Table 7.4 and to Question 49 in Table 7.5). While the findings did not indicate the lack of adjustment to new technology, they did, however, highlight the aspect of increased awareness of the matter.

Training and education programmes were highlighted in the interviews and emerged from COQ findings across all three South African military education, training, and development institutions as being limited. While the study did not probe these nuances among the three sample population groups, it nevertheless emerged that the culture regarding cybersecurity was challenged by broader contextual issues, namely a lack of resources and a deficit in funding[54]. This could therefore be a challenge for the SANDF as training and awareness programmes were generally viewed among the participants, as well as in the literature, as necessary although participants from all three institutions indicated a lack of urgency about the training of members. Theme 3 (short narratives of the COQ), for example, strongly indicated training and programmes in cybersecurity as a requirement for all members of the organisation. This view was also strongly shared by the participants from the SANDC, who expressed this need in Sub-theme 1.2: *The establishment of cybersecurity awareness among military members*[55].

7.6.5 Indicator 5: Trust in organisational processes and efficiency in technology use

Indicator 5, as derived from the findings, pointed out that a sense of awareness of the approach to cyberspace prevailed, and more specifically the online security behaviour

[54] See Janse van Rensburg (2019) in Chapter 2 regarding the aspect of training in the DoD and how training is affected by the available resource allocation.

[55] See Ntsaluba (2017) on formalised training on cybersecurity and Mkhonza and Letsoalo (2017) on organisational challenges related to the employment of interventions in large organisations.

of others. The findings indicated the trust factor, which was identified by the participants from the SANDC, who admitted to having very little faith in the security of the SANDF's computers and other members of the organisation. Furthermore, the SANDC-derived findings also emphasised that technology is possibly linked to the establishment of a digital culture, as illustrated in Theme 3: *The construction of a digital culture among members*. Moreover, Sub-theme 3.2 showed that participants accepted that doing their organisational tasks on their own technological devices was considered more efficient than on those of the SANDF.

In addition, this indicator was a double-edged sword as the use of more efficient communication concerned using personal devices, which might simultaneously be considered as a security risk, especially if the security behaviour of the respondents and measures that ensure their compliance with regulations were not in place. Sub-theme 2.1, *Vigilance among members of the organisation owing to differences in how cyberspace is approached*, drew directly on the level of trust among military members of the organisation, but also provided a basis for the argument that trust was a factor in how security behaviour was approached. Despite the limited trust in technology and in colleagues, there were some respondents from SAMA and the SANWC who called for stricter security measures through monitoring. In addition, some SAMA and SANWC respondents indicated that there was a security culture in the organisation.

7.7 Integration of the findings with ST

The previous section offered a discussion of the research questions. This section extends the discussion of this chapter by contextually applying the findings to ST. This section follows the main points of the theory and discusses them in relation to the findings derived from Phases 1 and 2. The researcher made the argument in Chapter 3 that securitisation might occur over a long period of time and might or might not complete this process in some contexts, as noted and explained in research by Van Ooijen (2020). The researcher notes that historically institutionalised security actors such as political institutions and military establishments may have more claim to ST than new actors entering the securitisation space. However, newer actors may also challenge the established conceptualisations of security.

The traditional view is that the military is used to protect the interest of the state and the state may often resort to the military as an intervention to the threat. This study included the newer conceptualisation of ST, which argues that newer actors may challenge existing ideas regarding security. It is worth noting that not all facets of ST might be applicable to, nor forced into, the interpretation of the findings. This is because the researcher explored cybersecurity at the individual level and not only at a macro level where one is able to view the security response mechanisms of the state. Subsequently, this section first considers the role of (1) the securitising actor and its place in the context of this study's findings, (2) the speech act and its implementation, and (3) the perceived role of ST in the South African military context.

7.7.1 The securitising actor and its contextual relevance for the findings

It is argued that the findings of this study contribute to explaining how cybersecurity threats were perceived among three military sample populations. Cybersecurity is a national threat that is underpinned by national legislation and the military (SANDF) is the primary agency with the responsibility for national cybersecurity. In this regard, the SANDF and militaries (South Africa and internationally) are also vulnerable. Due to this vulnerability, it becomes essential to focus on the South African military officer cohort regarding their cybersecurity behaviour. The researcher argues that the older thought on ST did not consider new and emerging threats such as cybersecurity or piracy in the maritime domain. New conceptual thought on the use of ST therefore includes these to open up new discussions on security. The role of the actors in ST also shifted as new "players" enter the fold and may even engage in the securitisation process. This softens the traditional view that only the state and its political actors may engage in securitisation speech acts where threats are vocalised. The findings showed that military officers speak and do security and are active agents in establishing new ways to address cyberthreats, whether it be in their personal or professional capacity.

The later conceptualisation of ST allows for new and less powerful actors to redefine security, as well as its meaning. This extension of meaning can be viewed in Sub-theme 3.3, where it was shown that the construction of a digital culture may increase the skills gap, which may be attributed to a difference among senior and junior officers. The extension of the conceptualisation of security and its meaning attributed by its actors can be seen in Indicator 2, which emphasised the aspect of awareness of best practices. The researcher argues that security actors (military officers) are allowed to have a variety of approaches to address security threats. Indicator 1 showed that there is a foundation in how threat information is shared but also understood. This forms part of the view that with new conceptualisations come new meaning. The interview findings suggested that the military officers considered cybersecurity threats as a challenge to the organisation and they thus adopted very cautious online security behaviour. However, there were exceptions concerning security behaviour. A closer look at the findings allowed for some understanding of how the participants viewed cyberspace and cybersecurity. The researcher also notes that while the current mechanisms to address security threats may not be perfect, they do fit within the micro-level view that actors may employ new logics of security to inform the speech act.

The traditional view of ST was to emphasise security matters that were framed around the state and the military. At the same time, the researcher positioned his argument on the idea that the military was an important factor in the security cluster and also an essential tool in national security (RSA, 2015a). In following this line of logic, the researcher indicated in Chapters 2 and 3 that he considered the individual (the military officer) as a key human factor in the securitisation process. An important distinction should be made. While the participants were not in positions of decision-making influence or possessed power at state level, they were also for the most part not practising as “functional securitising actors” in the securitisation process. The researcher posits that SANDF military officers take on an active audience member role within the ST process in the South African context. The South African military officer is not a passive receiver of speech acts, as can be observed in the findings; instead, they are active audience members who may function as potential securitising actors themselves through speech acts and behaviour. This view is in line with the later thought on ST, where the framework is considered dynamic, flexible, and intersubjective.

In addition, the researcher also argues that cybersecurity as a threat had not yet been fully securitised, nor had the securitising actor positioned it as existential in a convincing way. Moreover, the presence of a threat or crisis does not mean that it will receive a response. However, the general perception of the threat, which is essential for obtaining the necessary support for measures that deal with drafting policies and the mobilisation of resources to resolve the existential threat, can be traced.

The securitisation of cybersecurity in part extends the narrow view of what constitutes an existential threat to a referent object. Moreover, some findings of this study showed that situating national cybersecurity responsibility in the SANDF points to achieving securitisation (Bourbeau, 2015). This confirms that ST as a process takes time to actualise over an extended period. The researcher followed this argument in stating that the first tick box of securitisation has been marked by the South African Minister of Defence. This minister has proclaimed publicly that cybersecurity threats have the potential to be a threat to the nation state's national security and the users who navigate cyberspace. Regarding the apparent lack of understanding of this proclamation made by the securitising actor, the researcher argues that this might be a snapshot of a broader contextual issue that includes different actions, sequential decisions, and regulatory measures on cybersecurity threats.

The study's findings suggested that cybersecurity has not yet been fully securitised as the researcher, based on the findings and the key factors relevant to RQ1, submits that it was evident that the officers did not regard the military as taking the lead in prioritising cybersecurity. If cybersecurity was moved into the realm of political debate, the next step would be to obtain consensus that it poses an existential threat to the survival of the SANDF and thus the state itself. The recent Budget Speech Vote (2021/2022) indicated that the priority accorded to cyber became compromised to cope with the COVID-19 pandemic (RSA, 2021). However, the Minister of Defence had engaged in a securitising act, which was to announce the threat. Furthermore, the securitisation process had only commenced with the proclamation of the threat, and very little attention had been paid to obtaining clarity about the referent object and the introduction of emergency measures to address the state and securing its sovereignty; the organisation that upholds national security; and, lastly, the individual responsible for acting on security measures in order to maintain cybersecurity.

7.7.2 The speech act and its implementation in relation to the findings

As pointed out in Chapter 3 (see Section 3.5), not all threats require emergency intervention; the threat and the response to the threat therefore do not necessarily have to be at the apex of national security and the use of force. From the findings it appears that the SANDF does not address cybersecurity well enough for it to be taken seriously. However, in terms of viewing this specific finding from the ST framework, the researcher notes that threats are sometimes dealt with below the level of exceptionality, which highlights the point made at the onset of this section. Indicators 1, 2, and 3 point towards the conceptualisation of security and suggest that awareness is necessary to construct the importance placed on threats. One may thus assert that security is what the actors make it out to be. RQ1 focused on the conceptualisation of cybersecurity awareness, which centred on indicators linked to information sharing, training and education, and the awareness of best practices and policy.

Here the South African military officers offered new conceptualisations of how to engage with cybersecurity threats in the SANDF context. These conceptualisations of security may also carry some political weight as the role of the military officer is to inform decision making and guide operational activities. Their frame of understanding may therefore assist in how directives approach cybersecurity and how awareness of the topic is presented and hopefully increased. While the military practitioner is not in a position of political power, he or she may still inform certain decisions made by senior management in the organisation and thus having an influence on the language of security used and the manner in which threats are vocalised to political appointees. The literature showed, as captured in Chapter 3, that the speech act centres on the security utterance made by the securitising actor, which in turn leads to actions on proposed security measures.

Buzan et al. (1998) suggest that three conditions are attached to the speech act, which can be linked to the context of this study. Firstly, the speech act requires the utterance of a threat that should be characterised as existential and that emergency measures are to follow. The findings made it evident that the SANDC, SAMA, and SANWC participants indicated not only a lack of training and awareness of cybersecurity, but apparently also a limited amount of attention on cybersecurity threats. For example, the Minister of Defence has reported that cybersecurity threats could have a significant impact on national security. However, at the same time, very little was said about the existential nature of the threat and why it was deemed to be a danger to the various domains that comprise national security. The researcher argues that the findings derived from RQ1 and RQ2 showed that, with regard to the existing perceptions, cybersecurity was not framed as an existential threat. The participants did, however, indicate that they believed the armed forces should control cyberspace, which aligns with the idea that the SANDF is the apex entity to manage cyberattacks in the country. This indicates that although the speech act regarding the perceived danger of cyberthreats has not been proclaimed in its entirety, the participants were aware of the potential risk this presented to the organisation and its employees' personal information.

The second facilitating condition focused on the positions of the securitising actor, that of authority, and of the audience (Buzan et al., 1998). Here subjectivity relating to threats and the interpretation of security entered the field. Essentially, this facilitating condition dealt with the relationship between the securitising actor and the audience. It should be noted that the military officer was considered the referent object. While ST deals with higher-order threats such as migration, political challenges to territory, and issues of sovereignty, this study focused on the individual level in the military, and specifically on issues of individual cybersecurity. The argument was made that the human factor was often the point of entry for cyberattacks and threats. In addition, human error also entered the discussion as the factor could be associated with online security behaviour and the voluntary and involuntary errors people make when engaging with cybersecurity. The researcher argues that the securitising actor would be the South African Minister of Defence, who has already proclaimed cybersecurity as a threat to national security. The audience in this case was the South African military officer located at the SANDC, SAMA, and SANWC.

Based on the discussion of the findings relating to RQ2, it was apparent that the participants were aware of cybersecurity threats and took the necessary security precautions when they felt unsafe or uncomfortable. How information is received plays a role in how the participants practised cybersecurity behaviour. The researcher concurred with this statement and linked it to the role of the audience by pointing out that the participating military officers considered cyberspace a threat and that, in linking this to the discussion of RQ2, it was clear that the participants had adopted their security behaviour.

The participants also clearly felt that, as derived from the findings of RQ1, the organisation should do more regarding cybersecurity awareness campaigns. In addition, the participants were also aware of the threats that might be relevant to the organisation. The findings could inspire the assumption that the military officers were generally aware of threats and security behaviour. Therefore, while there was no explicit focus on the immediate emergency measures, as indicated in the first indicator, there was a consistency between the security utterance of cyber being a threat and how military personnel practised security behaviour. One may argue that while the audience is not always informed of the threat, the discourse of actors that have political power is an important and even critical factor in the perception of cybersecurity issues as threats to national security.

The third condition highlighted is where the securitising actor expresses the unique features of the threat to the audience (Buzan et al., 1998). Based on available contextual information, the Minister of Defence described cybersecurity more than once as posing a threat to national security (RSA, 2022). This is relevant to where the cyberthreats were elevated from normal level 1 and 2 issues, which deal with defacement and data breaches (see Section 2.10), to higher levels. With regard to national security, it should be highlighted that the minister has attempted to elevate the cyberthreat issue to more serious attacks such as organised crime and hacktivists (see Section 2.10). To the contrary, the military officers in this study did not have the higher-order power to proclaim cybersecurity as an existential theat. Although senior SANDC military officers were in positions of leadership in their respective units, it is important to emphasise that they did not have full authority to enforce political decisions. The broader contextual aspects of the speech act did receive attention when the South African Minister of Defence indicated in the Budget Vote Speech 2021/2022 (RSA, 2021) that cybersecurity threats poses a significant threat to the organisation. This again brings the role of other actors below the political level into play as actors, who engage with speech acts and as an audience to articulate cybersecurity as a dangerous threat to national security.

Linking the overall findings addressed here to ST, some observations are offered. Cybersecurity has not yet explicitly been declared an existential threat to the survival of the object of reference. The researcher furthermore submits that the declaration of cybersecurity as an existential threat has not yet taken place in the context of South Africa, although some elements of the process are visible at the national level. This view could be supplemented by taking cognisance of the limited resources for and financial allocation to cybersecurity as a threat to the SANDF, which in essence is the bastion of cybersecurity for South Africa. It was noted in the Budget Speech Vote 2021/2022 (RSA, 2021) that the current tools of the SANDF were regarded as outdated. Moreover, the quality of the speech act, based on media reports and DoD’s annual reports (RSA, 2021; 2018), suggests that for cyber to be fully elevated to being an apex national security issue requires investment in spite of it recently having to concede a priority position to contain the COVID-19 pandemic.

On a more optimistic note, the Budget Vote Speech for 2021/2022 (RSA, 2021) showed that there is a trend to elevate cyber as a threat to national security. Although the findings related to Indicators 1 to 5 express a perception that cybersecurity has not yet been elevated as posing an existential threat, the contextual developments of cybersecurity in the SANDF show some movement to address cyber as a security threat (RSA, 2022; 2021). Lastly, securitising actors may provide projected timelines of the threat by highlighting the security measures necessary for responding to a threat. In part, a temporal line is echoed in the legislative measures and the annual objectives of the SANDF where cyberthreats continue to be raised as a serious, and even a national, security concern.

7.7.3 The perceived role of ST in the South African military context

When linking the ST process to the findings, the interview themes and COQ short narrative themes are indicative of how the participants perceived cyberspace, as characterised by cautiousness and vigilance. One of the key aspects in ST is to understand what was said and performed in the past. In this vein, securitisation may take the form of discourse and identity as the characteristics of a threat are humanised or normalised. To a large extent, the findings at the SANDC showed that military officers acknowledged that cyberthreats are a security challenge in the organisation. However, at the same time, the findings also alluded to the idea that their organisation is not taking cybersecurity seriously. Herein rests the duality of the argument: on the one hand, the participants from the SANDC, SAMA, and SANWC indicated that there was a feeling that cybersecurity is a threat and poses a significant security risk for the organisation, while, on the other hand, the idea that training and education are not a point of focus may link with the notion that at senior levels the threat may not be seen to pose an immediate danger.

The interview findings also showed that the participants noted their personal feelings regarding cyberspace as a domain that is a dangerous space. The findings revealed that the participants (see Themes 2 and 4) considered their information security and their online safety as important and considered cyberattacks and threats as dangerous. The online security behaviour that was a consequence of these indicated feelings regarding cybersecurity might be useful in seeking a response from the audience if being shared with a designated audience. Indicators 2 and 3 showed that while not all military officers are in a position to enforce cybersecurity policies, they do have the ability to inform decisions and the creation of directives that are issued in the organisation. It appears that the participants were not entirely influenced by the political language of the Minister of Defence regarding the threat. However, formal documentation in their professional environment or personal environment contributed to their conceptualisation of cybersecurity as a threat. This section is concluded by emphasising the perceived success of ST in the context of the findings derived from the SANDF.

7.8 Conclusion

This chapter discussed the findings of Phases 1 and 2. The first section of the chapter provided an in-depth summary of the findings and discussed these in relation to context. Thereafter, the chapter focused on discussing the findings associated with the COQ scale items for the SAMA and SANWC sample population groups. A summary of the findings from both phases was provided, and several key points were presented. This chapter included a discussion of the research questions by elaborating on each of them while keeping the findings in mind. The research questions contributed to the overall aim of this study, which was to explore the perceptions of cybersecurity in the SANDF. The findings related to RQ1 revealed that the conceptualisation of cybersecurity awareness depended on three indicators, namely information-sharing culture, cybersecurity training and skills development, and awareness of policies. Moreover, the findings related to RQ2 showed that threat perception and online security behaviour captured how the participants perceived cybersecurity threats, while the findings related to RQ3 focused on the context of issues relating to organisational trust and how this linked to cybersecurity awareness. A summary of the findings included presenting a graphical model that illustrated how the various indicators assisted with exploring the perceptions of cybersecurity, as well as five awareness indicators as an overall outcome.

The chapter that follows provides the researcher’s concluding remarks about the study.

CHAPTER 8:
CONCLUSION

8.1 Introduction

This study explored the perceptions of cybersecurity among South African military officers by focusing on their conceptualisation of awareness and view of cyberthreats. The primary aim of this research was to explore what governed the perceptions of cybersecurity among military officers. The second aim of the study focused on what impact these perceptions of cyber could have on users when sharing information in a digital space. Three secondary research questions informed the exploration of the study:

1) How do South African military officers conceptualise cybersecurity awareness?
2) How do South African military officers perceive cybersecurity threats within the SANDF?
3) What are the perceptions of cybersecurity awareness through the lens of the military officer?

This chapter provides a brief overview of the previous chapters. Thereafter, the focus shifts to the limitations and contributions of ST in this study. The research questions of this study are also stated with reference to how the findings may answer the questions posed. Thereafter, the chapter offers a brief section on the limitations of the study. The contribution that this study makes is also presented in this chapter. Furthermore, this chapter also offers a discussion of the recommendations for future research. A reflection regarding the researcher’s personal experience of this doctoral study is also presented in this chapter. Lastly, final conclusions are offered by the researcher.

8.2 Overview of chapters

8.2.1 Chapter 1: Introduction

This chapter presented an overview of literature that focused on the development of cyberspace and the impact this domain has on the SANDF. The overview of the literature also referred to the aspect of information sharing as an element of cybersecurity. Focus was also placed on the South African military officer as a key element in the development of cybersecurity capacity. The chapter presented a brief introduction of ST and noted how the human element may feature in the process of securitisation. The chapter then briefly introduced the problem statement of the study. Thereafter, the chapter discussed the rationale, research, and research questions of the study. This chapter formed the foundation of the three research questions of this study.

8.2.2 Chapter 2: Review of literature on cybersecurity as an emerging threat

This chapter revealed that most of the existing literature focuses on governance and technical elements of cybersecurity. The chapter acknowledged that there is a void in the literature concerning the role of perceptions regarding cybersecurity awareness among South African military officers. The chapter offered a contribution to the literature by creating an operational definition of cybersecurity that encapsulates the human element as the centre. This built onto a discussion of the complex nature of cyberthreats. This chapter offered an extensive discussion of the cybersecurity legislative efforts made by the South African government. The chapter offered a brief discussion regarding elements of risk perception and how risk information is perceived in organisations. Additionally, a brief discussion of information-sharing behaviour and cybersecurity awareness creation concluded the chapter. This chapter contributed to the overall understanding of cybersecurity by discussing existing literature to gain an understanding of the emerging domain under exploration. The literature presented also assisted in the identification of knowledge gaps and an overall understanding of viewing the findings in context.

8.2.3 Chapter 3: Securitisation as a theoretical framework

Chapter 3 offered a discussion of the rise of new security threats in the 21st century and indicated that cyberspace is a threat that has emerged as a new security challenge for nation states and institutions. The chapter addressed the new conceptualisations of security threats by presenting various interdisciplinary views of security. This chapter discussed the rise and use of ST in contexts. The chapter also offered a critical review of ST by pointing out the pitfalls and potential aspects that might hinder development and thus its applicability and utility in newer contexts. The chapter identified the SANDF as a custodian of cybersecurity in the South African context, where the organisation has the responsibility to coordinate security efforts to address threats originating from the cyber domain. The chapter positioned itself within the focus of security studies and located cybersecurity threats along newer thinking on securitisation within the ST framework.

8.2.4 Chapter 4: Research methodology

Chapter 4 provided a discussion of the research design, which emphasised the sequential approach of Phases 1 and 2 of the study. This chapter also captured the reason why a mixed-methods approach was deemed suitable for the research questions and objectives of the study. The SANDC, SANWC, and SAMA sample population groups were also briefly discussed in this chapter, with emphasis on the element of junior and senior officers. The chapter further presented CA as an analysis technique for Phase 1 and pointed out how the codes and themes informed Phase 2 of the study, which focused on the construction of the COQ dimensions. The element of triangulation was briefly discussed as this is central to the use of the sequential design. Furthermore, the chapter discussed aspects related to validity and reliability. The study limitations were also addressed in this chapter.

8.2.5 Chapter 5: Phase 1: CA

Chapter 5 presented the qualitative findings of Phase 1 of the study and used CA to analyse and code the interview transcripts. The themes were presented in this chapter, and four main themes emerged. The key findings that emerged from the chapter were as follows:

1) Training and education are key in creating cybersecurity awareness.
2) The participants were vigilant about how other military members used cyberspace and applied their security behaviour.
3) There is a lack of clarity regarding the use of cybersecurity guidelines in the organisation.
4) More efficient technological tools are required, with an emphasis on personal device use.
5) Previous exposure to cybersecurity may assist in security behaviour and understanding the subject matter.

6) More accessible means of communication are required to convey information other than social applications.

The findings of Phase 1 assisted in the construction of COQ items and dimensions. The chapter also contributed to the understanding of cybersecurity awareness among a senior military sample group, namely the SANDC.

8.2.6 Chapter 6: Phase 2: Descriptive and thematic analyses

Chapter 6 presented the responses to the scale items in the COQ. The chapter presented the findings related to the SAMA and SANWC sample population groups. Education and training were highlighted as elements in the creation of cybersecurity awareness in the SANDF context. Information sharing on directives was noted as a developmental issue, where the respondents indicated that greater involvement was needed. Chapter 6 also yielded three themes from the short narrative questions. Theme 1 revealed that *information sharing on best practices requires implementation*; Theme 2 showed that *cautionary behaviour is linked to the navigation of cyberspace*; and Theme 3 focused on *cybersecurity training and education as a way to enhance security measures*. The chapter contributed to the importance of Phase 2 by supplementing the findings presented in Phase 1. The chapter also provided a snapshot of how the SAMA and SANWC respondents perceived cybersecurity through exploring the four dimensions of the COQ.

8.2.7 Chapter 7: Discussion of interview themes and COQ findings

Chapter 7 discussed the findings of the CA and COQ. The chapter offered a brief summary and discussion of the CA findings. Thereafter, a discussion of the various COQ dimensions was presented in line with the SAMA and SANWC sample population groups. A discussion of the themes extracted from the short narratives of the SAMA and SANWC sample population groups was presented, with emphasis on three themes. The chapter also critically engaged with the research questions by discussing them with reference to the CA and COQ findings. The CA and COQ findings were combined to provide an overall picture of cybersecurity awareness among SANDF military officers. This was performed by presenting five indicators. The CA and COQ findings were also discussed critically in relation to the relevant facets of ST, such as the securitising actor, speech act, and the perceived role of the military in the South African context. The discussion of the findings in this chapter contributed to viewing the various facets of cybersecurity awareness in the South African context, as well as from an ST perspective.

8.3 Contribution of ST to the study

This study recognised the role of ST and expanded the exploration of this theory by indicating how ST and cybersecurity as a fast-growing threat to national security interact. Although the existential threat argument might be perceived as a central limitation, the military connection to extraordinary responses ties into how weak cybersecurity awareness and behaviour inhibit military organisations such as the SANDF in playing their role. Examining the perception of cybersecurity among South African military officers in the context of ST contributes to the cybersecurity debate in South Africa and the SANDF. The theoretical contribution of this study also explored ST in a non-Western context and noted cybersecurity as an emerging threat domain in the South African context. In this manner, the research contributes to the exploration of cybersecurity among an armed forces population.

ST has undergone several developments in the past decade; this study thus adds to the growing debate surrounding the securitisation of cyberspace and the military by viewing the individual as central to the security debate. This development made ST more relevant to the study as it considered alternative contexts – those falling outside the Western trend – to explain how threats are communicated. It was important to put on record that no longer might only the authoritative actors engage exclusively in the speech act and call for emergency measures. The authority and power have broadened to include entities outside of the state to employ the speech act. The focus migrated from those traditionally in power to include other, non-political entities, where these entities continue to apply pressure instead of power. This study fitted into this nexus of pressure from these entities, away from the traditional Western concepts of who has the power to engage in the securitisation process.

Furthermore, it also allowed for a more grounded approach to viewing how cyberthreats have become a danger to society. Using ST in this study assisted with understanding the meaning attributed to threats and security and how responses unfold. The contextual perceptions of participants in the armed forces might therefore allow for greater insight into the challenges experienced in this domain, as well as to increase the level of understanding of cybersecurity as a facet of the referent object. The study cultivated greater understanding of the conceptualisation of cybersecurity and of how cyberthreats are perceived among military officers. The findings of this study revealed that cybersecurity behaviour and conceptualisation might be experienced differently. This difference in perspective was in line with the view that the audience does not necessarily have to accept the conventional security framing of a threat in order for the speech act to be a success. Cybersecurity awareness in the SANDF might therefore be able to contribute to understanding threats and thus enable cultivation of new attitudes and behaviour towards cyberspace and its potential threats.

The existential and extraordinary measures were two elements of ST that were not satisfied. The other elements in the securitisation process could be observed, but future progress would reside in bringing newer thought into the ST process to account for a number of shifts: who can securitise (other than political actors); what threats beyond armed attacks are potentially existential; and convincing audiences by way of non-political actors to respond comprehensively to previously neglected threat sectors, of which cybersecurity is one.

8.3.1 Limitations of the use of ST in this study

The use of ST as a framework could be criticised as this theory is still undergoing development, especially in its application to various contexts outside the Western setting (Kapur & Mabon, 2018). The focus of this study was to view the key points in ST and doing so in the context of the findings. Moreover, the philosophical level of the theory focused on the higher-order actors and processes with an existential narrative, and not specifically on individual and institutional elements. This study, however, dealt with the human factor and selectively used elements of the theory to explain the greater ST process and how this might occur in the South African context. The challenge of applying ST in the South African context is that the securitisation process of cybersecurity is non-linear. Although later reviews of the theory did make allowances for non-Western contexts, they might not necessarily have considered all the contextual challenges in which a security issue might occur. However, ST currently does make allowance for the notion that it may take some time for threats to be elevated to a point where they are considered existential. Since the element of time is not indicated in the ST process, the argument can be made that the non-linear process evidenced by cybersecurity in the South African context might enable a more flexible view of what threats are securitised and by whom. Moreover, ST provides conceptual conditions as a basis to view the success of the speech act in context. At the practical level it is worth noting that, based on the findings, although a threat is not fully connected to existentialism, it may not necessarily indicate that the audience is not cognisant of its dangers and implications to national security. Confining the theoretical elements of ST might therefore be challenging in contexts that reflect newer threat sectors, which might have limited resources or revolving securitising actors such as a turnover of cabinet members and ministers relaying threat information.

The section that follows presents a summarised discussion of the indicators derived from the overall findings. The researcher presented a summarised version of the findings by emphasising the indicators used for the model in Figure 7.1. These indicators represent a summary of the findings derived from Phases 1 and 2 of the study.

8.4 Reiterating the research questions

This research employed two phases – one qualitative and the other quantitative. The semi-structured interviews in Phase 1 conducted at the SANDC allowed the researcher to obtain a contextual impression from a selected group of senior officers of their perceptions of cybersecurity in the workplace. Phase 2 focused on preparing the COQ, to explore the views of participants located at SAMA and the SANWC through focusing on four dimensions that related to various aspects of cybersecurity awareness. The dissertation commenced with three guiding research questions. Based on the information provided throughout the study and the findings presented, it was possible to provide informed answers to these research questions.

8.4.1 How do South African military officers conceptualise cybersecurity awareness?

RQ1 focused on gauging how South African military officers conceptualised cybersecurity awareness in the organisation. In answering this research question, the researcher considered several aspects that emerged from the findings that potentially answered the question. The findings indicated a lack of urgency by the organisation to address cybersecurity. This lack of urgency was regarded as an indication of how the participants from the SANDC, SANWC, and SAMA perceived a digital culture. Moreover, their perception of a digital culture sparked the participants’ use of their own technological devices and software rather than the organisation’s to perform their day-to-day tasks. The findings also showed that the SANDC, SANWC, and SAMA participants tended to conceptualise cybersecurity awareness as a factor that was still relatively new to the organisation. Minor differences emerged in how the participants from the SANDC and SAMA perceived junior officers practising online security behaviour. The findings also revealed that the practice of cybersecurity among SAMA participants did not have strong links with a lack of awareness in cyberspace. The data suggested that some SAMA participants were probably more comfortable with operating in cyberspace and still maintaining a sense of vigilance, although the majority of the SANDC and SANWC participants appeared to be apprehensive about this space and the integration of technology.

Overall, the findings suggested that the priority allocated to addressing cybersecurity in the organisation was limited. Some participants from SAMA and the SANWC indicated that the organisation needed to embrace a stricter position relating to cybersecurity. However, most participants indicated that cybersecurity education and awareness training should be presented to all military members. The majority of participants were aware of cyberthreats that could be harmful to the organisation. Few participants indicated they did not update themselves with information regarding cybersecurity. Moreover, some SAMA participants considered their online security behaviour as more relaxed and a minority of the SANWC participants indicated that they would use the Internet when necessary. It might have been possible that the misconception regarding the matter of cybersecurity could be linked to rank and exposure to cyberspace. Participants from the SANDC and SANWC expressed that they were more distrusting of junior colleagues’ security behaviour in cyberspace. Conversely, some SAMA participants were relaxed when sharing information with their colleagues and in using cyberspace. However, the majority of SAMA participants were aware of cyberthreats and exercised caution when sharing information in cyberspace.

In answering RQ1, it was clear that the premise of the conceptualisation of cybersecurity awareness was based on the following:

1) Most participants were vigilant of cyberthreats and cyberspace.
2) Most participants were aware of sharing information with their colleagues in the workplace.
3) Some participants were in favour of using their personal devices in the workplace.
4) Most participants indicated that there was a need for cybersecurity awareness training.

The aspects listed in answering RQ1 could explain why there was a difference in conception between the participants from the SANDC and SANWC as opposed to those from SAMA.

8.4.2 How do South African military officers perceive cybersecurity threats within the SANDF?

RQ2 focused on military officers' perception of cybersecurity threats. The researcher argues that the indicator awareness of online threats and perceived awareness of self in cyberspace should be applied in answering this research question. The findings showed that the participants located at the three military institutions took the necessary security precautions in securing themselves in cyberspace. The participants considered the domain of cyberspace to be dangerous and that they needed to adopt a sense of vigilance when navigating cyberspace. Hence, the findings suggested that most participants had the necessary awareness and that they were cognisant of the implications when a vulnerability could possibly be exploited. Cyberthreats and attacks therefore influenced military officers to adapt their online security behaviour regardless of whether it was in a personal or a professional setting. It was argued that the construction of threats essentially dealt with users' perception of what constituted the cyberthreat. The researcher asserted that the perception of risk information was impacted by the perception of digital safety and the availability of information that dealt with policies and guidelines. The identification and understanding of policies might assist military officers in interpreting security incidents and with using the necessary security tools to respond. Furthermore, the participants were also aware of their own security vulnerabilities. This awareness showed that, generally, military officers

(SANDC, SAMA, and SANWC) were informed of cyberthreats and that they might have the necessary knowledge to form adequate deductions of threats.

8.4.3 What are the perceptions of cybersecurity awareness through the lens of military officers?

RQ3 focused on the perceptions of cybersecurity awareness through the lens of South African military officers; thus focusing on the perceived role of cybersecurity. The findings showed that the participants regarded themselves as aware of cybersecurity threats but indicated that their knowledge of threats in the organisation was limited. The findings applicable to all three sample groups showed that their online security behaviour and information-sharing practices could be positively impacted by new threat information and training. Compliance with and integration of policies with operational activities might influence their security perceptions and awareness for the better. The link between compliance with guidelines and awareness of cybersecurity threats could be determined by how the participants integrated this into their work activities and applied vigilance in online security behaviour. This compliance with directives and guidelines showed that the participants were generally open to training and education in cybersecurity awareness. It should be noted that embedding cybersecurity was deemed to be an ongoing process that requires dedication. While some participants indicated that cybersecurity policies were present in the organisation, they believed that not all of their colleagues were aware of this, which could imply a difference in how security behaviour was practised. In addition, this underlined the reality of cybersecurity as an ongoing exercise to continuously fill the awareness voids.

The findings showed that some change regarding the manner in which policies and directives were communicated to military officers at all levels was necessary. This finding consequently raised questions about how guidelines and best practices were practised, as well as concerns about organisational governance. The findings indicated a strong sense that the guidelines were not clear, which explained why the participants conveyed that some of their colleagues were often unaware of cybersecurity guidelines. Unclear guidelines might therefore have had an impact on how military officers practised online security behaviour and adapted the ways in which they practised information sharing. In addition, the lack of understanding of policies might also have contributed to how technology was used, as expressed in the online behaviour of the military officers. The contextual aspect alongside the allocation of limited resources to the SANDF might have had a further impact on cybersecurity and preferred behaviours. In this regard, the participants pointed out that cybersecurity was in its infancy, which might indicate why the findings revealed that the senior management of the organisation was failing to prioritise cybersecurity. The cultivation of a digital culture in the organisation might have a positive impact on the security behaviour of the military officers, and in turn improve how these members of the military perceive cybersecurity.

8.5 Limitations of the study

This section discusses the limitations of the study. These limitations are as follows: (1) access to participants, (2) mitigation of bias, (3) missing data, and (4) challenges with sample size and the COQ.

8.5.1 Access to participants

The first sample recruitment site was identified as the SANDC. This site was earmarked as senior officers were attending a training course there. However, the primary recruitment site presented a myriad of challenges as the researcher had to conduct the interviews on-site and could not conduct interviews after hours owing to the restricted access to the military base on which the SANDC is located. The researcher mediated this challenge by creating a schedule for the participants once consent to conduct interviews had been obtained. Preceding this, at the initial briefing to which potential participants were invited to receive information about the nature and purpose of the research, a far greater number of military members attended and indicated their interest than who eventually participated. Nevertheless, after following up with the participants by calling them on their cellphones, some confirmed their interest in participating, while some potential participants indicated that they did not feel comfortable with participating in a study that was considered security sensitive. The researcher did not make a formal note of the verbal indications that the members gave regarding why they were no longer interested. As consent forms are generally signed at the start of an interview process and not prior to it, a participant is only regarded as engaged once the consent form has been signed. This did not present a problem. The researcher followed up with those who had shown an interest in participating in the study and scheduled interviews according to the participants' preferred date, location on-site, and time. In addition, of the 36 military officers who formed part of the SANDC cohort, only 10 indicated an interest in participating.

SAMA formed part of Phase 2, which primarily concerned the researcher administering the COQ. SAMA has a very full academic schedule that leaves little room for members to do anything else, including being interviewed for research purposes. Together with this, the researcher was not in the same province as the SAMA students. However, consultations took place with senior staff members at the institution to enquire whether it would be feasible to provide questionnaires to a large group of students. This arrangement received consent. The researcher arranged for SU lecturing assistants in the Department of Industrial Psychology, Faculty of Military Science, to assist with the collection of questionnaire data. In addition, the researcher constructed a training manual for the lecturing assistants, who were undergoing training in industrial psychology, to administer the COQ (see Appendix Q). This was done to guide the research assistants in the data-collection process, as well as with a view to handling the process ethically and to be able to respond to queries about questions that might require elaboration. The use of lecturing assistants allowed for financial and time constraints to be bridged and addressed in this study.

The participants at SAMA and the SANWC were all seated in one venue, which made it possible to gather all their responses in one session. This was beneficial as access to these sites and participants could be challenging, especially considering academic schedules and national military obligations. The researcher did not attend the completion of the COQ, which prevented interaction between the participants and the researcher. Exploring any supporting aspects such as body language and the way certain points on security were expressed were therefore limited due to the quantitative approach of Phases 1 and 2. Owing to the Likert-type order of certain items in the COQ, the respondents could rate questions based on their experience, and did not require asking deeper, more reflective questions. In addition, due to time constraints, the researcher could not pilot the COQ in a military sample. The piloting of the COQ could have resolved any problematic items that sought to assess the various constructs.

Accessing the data-collection site is crucial for a study to commence. Some challenges were experienced at the SANWC. Obtaining access approval from the Commandant at the training institution proved to be extremely challenging.

The researcher developed a call log and kept a trail record to show the difficulties with obtaining the necessary clearance to access the participants, who were senior military officers. Access to the sample population was obtained after interventions by academic representatives of SU, where the researcher was enrolled for his doctoral studies. Once the Commandant of the SANWC had granted permission, gaining access to the senior military officers who were attending a course was possible. After several months of liaising between SU and the SANWC, the researcher was finally able to brief the participants and to administer the COQ.

8.5.2 Mitigation of bias

In terms of addressing the element of bias in Phase 1 of the study, the researcher made use of a terminology list (see Appendix R) in case the participants needed clarity regarding terms related to cybersecurity. However, it is important to note that no participant in the process sought this assistance. It is also worth noting that the researcher acknowledges that bias can enter the process when providing the participant with a terminology list. Due to COVID-19 restrictions in place at the time, the researcher was unable to clarify or probe for additional information.

The researcher considered this terminology list as a precautionary measure in addressing clarification concerns. The researcher was aware of his own possible bias entering the construction of the qualitative component of the study. This awareness of potential bias entering the research process of Phase 1 was made possible with the use of a qualitative audit trail (see Appendix O) and a personal reflexive journal to ensure that all thoughts and ideas were captured. Palaganas et al. (2017) suggest that reflexivity is an ongoing process where introspection takes place and where the researcher acknowledges the role of subjectivity in the research process.

8.5.3 Missing data

One of the limitations that stemmed from the analysis of the COQ data was the amount of missing data. The amount of missing data presented in Chapter 6 may have an impact on the statistical power of the COQ. Due to COVID-19 restrictions in place at the time, the researcher was unable to re-establish contact with the SAMA and SANWC sample population groups as these sites were restricted during this period. The researcher therefore needed to work with the data that were collected during the pre-COVID-19 period. The limitation in this regard is that no interpersonal contact could be established to confirm some of the participants' responses. The researcher also notes that the missing data presented may not necessarily indicate a lack of cybersecurity awareness in the SAMA and SANWC sample population group. The amount of missing data in the study could be a factor to consider for future research on the construct of cybersecurity awareness. Furthermore, the focus of the study was on awareness and not on the level of knowledge regarding cybersecurity awareness among the participants. The COQ was designed to gauge the perception and consciousness of participants towards events. One of the design limitations of the COQ is that it does not assess the knowledge or level of education on cybersecurity. However, the perceptions of the four dimensions of the COQ were sufficient in answering the study's research questions.

8.5.4 Challenges with the sample size and the COQ

This study could be criticised for not extending the sample to include SANDF officers responsible for cybersecurity. While remaining cognisant of this, two main reasons were linked to the selected study sample at the SANDC, SAMA, and the SANWC. Firstly, the researcher focused on exploring the perceptions of cybersecurity; specialty in skills was thus not a key factor, nor was the study interested in interviewing cyber operators. Secondly, the researcher acknowledged that cybersecurity was an emerging domain in the SANDF. Exploring cybersecurity was therefore an important factor in establishing the foundation of how a cross-section of military officers conceptualised aspects of cybersecurity, related behaviour, and information-sharing practices. Furthermore, studying the perceptions relating to cybersecurity was appropriate as this was identified from the literature review as an upcoming domain. This exploratory study therefore provides an opportunity for further descriptive or explanatory research. Given the sample size of the study, the researcher cannot generalise the findings to the broader SANDF population, but this limitation creates opportunities for further research.

A practical criticism of the study possibly concerns the development of the COQ. The number of scale items in the COQ could have been reduced. However, because of the physical distance between locations and the researcher, and the once-off availability of sample sites for data collection owing to rigid COVID-19 restrictions, the researcher added additional items to the COQ for exploration. This assisted the researcher to make more in-depth deductions from the data that had been obtained.

8.6 Contributions of the study

This section addresses the contributions made by this study by focusing on (1) the information-sharing perceptions and practices among SANDF officers, (2) how the use of ST informed the case of cybersecurity in the South African context, and (3) using the COQ to explore the dimensions of cybersecurity.

8.6.1 Information sharing and cybersecurity practices among SANDF officers

This study added value to the armed forces context and cybersecurity domain in the South African military context by contributing to filling the void in the existing literature concerning cybersecurity awareness. As a result, this study presented a focus on the context of the armed forces and cybersecurity domains, which remain underdeveloped in South Africa.

The researcher focused on the perceptions of cybersecurity among South African military officers and on aspects related to behaviour and awareness. This study therefore acknowledged the unique role that the military officer (human element) performs in the cybersecurity chain. Furthermore, as cybersecurity advances up the South African national security agenda, the importance of the SANDF as a national security entity gains prominence. This study contributed to understanding the role of the SANDF and the human element as important actors in the securitisation process. This study further contributed to the gap that exists in cybersecurity awareness in the SANDF context by exploring various dimensions such as (1) information-sharing culture, (2) security orientation, (3) the view of cybersecurity, and (4) cybersecurity behaviour. The exploration of these dimensions allows for a better understanding of South African military officers’ contextual frame of cybersecurity in the SANDF. The findings of the study might also be considered to contribute as a baseline for practical interventions related to cybersecurity training and education in the SANDF. Views on the various dimensions offered a broad spectrum of information that could assist with forming a basis for a needs analysis of cyber. Furthermore, the study also contributed to the profile of what constituted cybersecurity awareness among senior and junior South African military officers.

8.6.2 How the use of ST informed the case of cybersecurity in the South African context

This study positioned itself within the security studies domain and explored the element of cybersecurity threats as a new conceptualisation of the security challenge entering the security debate. The findings of this study also contributed to the theoretical expansion of the security logic in ST and the view that the conceptualisation of threats might not necessarily be in sync with the status quo.

8.6.3 Using the COQ to explore the dimensions of cybersecurity

The unique contribution made by this study was that it explored the perceptions of cybersecurity awareness through the contextual lens of South Africa military officers by engaging in a mixed-methods approach and by using a sequential research design. The collection of data in this sequential process allowed the researcher to construct a picture of how military officers conceptualise the notion of security qualitatively. Providing the qualitative narrative of conceptualising cybersecurity enabled the researcher to develop an instrument that could capture the four dimensions of how cybersecurity is constructed in the organisation. The COQ allowed for a greater sample reach and the findings of the instrument were able to supplement the perceptions and views expressed in Phase 1 of the study. The methodological strategies employed in this study could be replicated in other contexts as the steps in Phases 1 and 2 were presented transparently. The evidence of these steps can also be traced in the attached appendices of this study.

The COQ contributed to the exploration of cybersecurity in the South African military context through potentially acting as a cybersecurity screening tool for the organisation, and especially senior management, to gauge where military members locate themselves in implementing cyber regulatory instructions and adopting cybersecurity behaviour. The COQ focused on the “here and now” and might provide valuable insight into how military officers consider securing information and engaging in certain security behaviours. Furthermore, the COQ offers an opportunity for the SANDF to enable the human factor to become more resilient in cyberspace. This could be done by perusing the factors that affect contextual issues, such as how existing information-sharing activities are performed and how cyberspace is perceived. Moreover, the COQ established the foundation for the identification of factors that concern cybersecurity awareness. In terms of improving the COQ, revising the scale items and reducing items might be considered. In addition, the COQ could be improved by focusing on a larger military population and adhering to processes not confined by COVID-19 restrictions to perform in-person data collection and follow-up. In addition, the COQ scale items could be improved by including multiple stakeholders from the private and security sector for additional input. The findings of the COQ showed that there were small differences between the scale items of the four dimensions. Additionally, the large amount of missing data may also have an impact on the development of the COQ. The researcher notes that survey fatigue may have been a consequence of the number of questions listed in the COQ. While the focus of this study was not to develop the COQ, the reliability showed good internal consistency, which indicates that certain construct items might be used as a foundation for further development.

8.7 Recommendations for future research

This section focuses on the study’s recommendations for future research on cybersecurity. The researcher acknowledges that there are four aspects to consider for future research, namely (1) the development of cybersecurity awareness screening tools, (2) exploring the validation of the COQ, (3) advancing cybersecurity education and training, and (4) policy development.

8.7.1 The development of cybersecurity awareness screening tools

The researcher submits that future research should be orientated towards the development of screening tools that are able to identify the cybersecurity awareness of military members. The use of screening tools may enable the organisation to gauge how military members perceive cyberthreats and how they adjust their security behaviour when confronted with online security challenges. Further development of the COQ may facilitate the screening of cybersecurity awareness in the SANDF. A follow-up study should thus be undertaken to explore the dimensions of the COQ to a military sample that has a wider range.

8.7.2 Exploring the validation of the COQ

While the focus of this study was not on the development of the COQ, the questionnaire served as a foundation for future development to explore factors that may govern cybersecurity behaviour and awareness in the military context. A recommendation for future research is thus to consider the construction of a statistical model, using structural equation modelling, to investigate multivariate causal relationships. This technique is but a step in the continuous validation of the COQ as an instrument for gauging cybersecurity behaviour among South African military officers. The COQ might thus serve as a starting point for determining factors that were strong predictors in the SANDF sample. In addition, the researcher recommends that future research should explore the COQ in contexts other than the military, to incorporate additional perspectives on security.

8.7.3 Advancing cybersecurity education and training

The findings showed that there was satisfactory knowledge of cybersecurity awareness in the organisation. This level of satisfactory awareness can be viewed in Dimension 2: security orientation among military officers (see Section 7.3.2), where it was shown that the participants were aware of threats and applied precautionary behaviour where possible. However, for a more in-depth view of cybersecurity behaviour, it might be necessary to focus on specific aspects unique to the organisation, such as directives that focus on online security. In addition, the COQ might assist by forming part of a training battery that might be presented to members of the military during the period prior to their exposure to training. The purpose of this proposed training battery would be to measure the pre- and post-cybersecurity behaviour of South African military members. Whereas the findings of the COQ did demonstrate that the participants were generally aware of cyberthreats, it did not assess specific threats and specific security behaviour. Future development in the workplace might therefore focus on cybersecurity awareness training by evaluating how members respond when confronted with online threats. The findings showed that cybersecurity awareness training should be available to each member of the military, regardless of their rank and level of functioning in the SANDF. The method through which cybersecurity awareness could be achieved might take the form of video and text-orientated content. In addition, as a practical initiative to bridge the skills gap and the need for cybersecurity training, the researcher recommends that cost-effective awareness training measures should be explored such as a Massive Open Online Course as a viable alternative to traditional education (Fianu et al., 2018). Such measures are available to help address the identified need for accessible cybersecurity training and education across all levels in the SANDF.

A gamification approach might also be considered as an alternative option for cybersecurity training in the organisation. This would be a more immersive and interactive approach, which would allow personnel to experience a simulated virtual environment that could replicate the contextual aspects in the physical domain. However, the researcher is mindful that gamification might be a platform that would appeal more to younger and more junior military than more senior military members. Based on the findings, it was evident that the junior participants from SAMA were more comfortable with using online platforms and maintaining security behaviour. In the final instance, cybersecurity awareness training was found to require more attention from the SANDF as the SANDF currently has only 100 trained cybersecurity operators (PMG, 2020). E-learning strategies might thus be considered to serve as a bridge between those who receive training and education and those who do not.

8.7.4 Policy development

Future cybersecurity initiatives should follow a more focused approach by highlighting the role of each security cluster more efficiently since the current allocation of responsibilities shows an overlap. This study did not analyse the policy on cybersecurity to make recommendations. Instead, it focused on the perceptions of South African military officers. Therefore, with knowledge on policy, the SANDF would be able to bridge the temporal gap in legislation and policy within internal directives. The findings suggested that the participants were generally aware of directives that related to elements of cybersecurity, such as information security in the workplace. This strengthened the argument that the directives offer ways to support existing policy and concepts of cybersecurity. The armed forces domain in South Africa should develop more comprehensive directives that focus on how better cybersecurity could be achieved at a level where all members are included and should not refer to the specialised roles concerning the approach to digital security. The findings showed that there is a need for better communication and implementation of policy on cybersecurity.

In addition, the SANDC findings indicated that uncertainty prevailed among senior officers about policy currently being employed. Future contributions to the development of a more integrated policy in the SANDF could perhaps be more direct and reward-based as this might assist in achieving compliance. Moreover, this might inspire military members to view compliance with policy and directives as beneficial. The SANWC and SAMA findings confirmed that knowledge of certain threats might assist in how online security behaviour is practised. A need emerged for synergy between directives issued in the organisation and the awareness required of military members at the unit level.

The time that legislation takes from inception until it is passed is considerable and requires dedicated attention. In terms of the findings in this regard, it is worth noting that the SAMA and SANWC respondents showed a definite preference for policy relating to cyber to be implemented in the organisation. Based on these findings, the researcher argues that knowledge of and compliance with policy were seen to have a beneficial impact on online security behaviour. Awareness of existing directives in the SANDF might therefore not only assist to bridge this gap between institution and practitioner but also positively influence the online security behaviour of users. The DoD, for example, might issue directives that focus on information security and the management of mobile device use in the organisation. The participants' views indicated that policies did not always reach everyone; the various mechanisms through which policy is disseminated in the organisation therefore need strengthening.

8.8 Reflection on the research study

This section focuses on the reflections of the researcher and personal pronouns are used to present the personal experience and views on this doctoral journey. The researcher engaged with this PhD research study on the perceptions of cybersecurity to explore how military officers embrace the notion of security in cyberspace. The topic is increasingly becoming relevant and requires development in the broader South African and military context. When reflecting on the PhD research study, the following aspects are worth noting and are presented in this reflection: (1) the SANDF as research context, (2) grappling with ST, and (3) finding my feet in a military orientated topic.

8.8.1 The SANDF as research context

I engaged with this study using a sequential design where I was able to interact physically with military officers in Phase 1 of the research (see Appendix O). However, there were some challenges in accessing the sample population groups in Phase 2 (see Section 8.5.1). The research context of this study was the SANDF. I had very little experience as an active military member within the organisation. I served as a civilian member for 12 months at the Military Psychological Institute, where my research interests were aligned to military science and psychology in the armed forces context. This PhD bridges the research gap in the organisation and aligns with the institutional goals of the SANDF. The organisation revealed in the South African Defence Review (RSA, 2015a) that cybersecurity is an element of concern that needs to be developed. My PhD was thus a means to address this gap and contribute to the organisation where my passion for military science was evoked. When reflecting on my PhD journey, the focus of cybersecurity started to actualise in 2018.

8.8.2 Grappling with ST

The theoretical component of this PhD was considered from an ST stance. I took the opportunity in my PhD to break away from the traditional psychological theories regarding behaviour and awareness. Instead, ST was an opportunity for me to explore my research interests and contribute a theoretical framework that is still emerging in the South African context. Reflecting on my theoretical stance for this study, I consider grappling with ST as one of the most challenging theoretical frameworks from a conceptual perspective, especially with cybersecurity being at the centre. ST not only challenged how my perspective of authority among actors is viewed, but it also required me to wrestle with the philosophical notions of power and speech acts. The selection of ST was the correct one, as I was able to contribute to theoretical knowledge by applying its facets to the South African military context.

8.8.3 Finding my feet in a military orientated topic

One of the main challenges in engaging with this topic was that I had limited experience in the SANDF. This limited period of serving in the SANDF may have impacted how I interpreted and understood some processes in the organisation.

The manner in which the participants expressed how security is conceptualised sometimes caused some confusion as I was for the larger part unfamiliar with the processes of securing information and the sharing practices in the organisation. As a result, I needed to become more familiar with the directives and policies of the organisation so that I was able to have a more grounded understanding of what military officers may experience in their day-to-day activities.

8.9 Conclusion

The role of cyberspace as a domain of warfare from an armed forces perspective could be significant for launching key strategic operations and maintaining freedom of action. This is achievable from a technical perspective, although an indeterminate limitation becomes prevalent when the human factor is introduced, which compromises the complexity and safety mechanisms of the former.

This study was conducted with the researcher highlighting the human factor as an important component in establishing cybersecurity and was therefore found worthy of further research. In this vein, information-sharing practices among SANDF officers from SAMA, the SANDC, and the SANWC revealed that there were clearly discernible differences in how officers approached the digital platforms. Although cybersecurity awareness in the organisation derived from human behaviour, altering undesirable behaviour did not receive the attention it deserves in the consideration of the complexity and dangers of cyberthreats and attacks.

This study showed that knowledge of and education in cybersecurity were necessary (and desired) for transforming not only organisational culture concerning how technology is embraced, but also how threats are perceived and eventually mitigated. The exploration of perceptions was important as what they pointed out would contribute to selecting ways and means for improved security behaviour in cyberspace. In addition, the researcher focused on the element of awareness instead of knowledge of cybersecurity due to the field being positioned as emerging in the South African and SANDF context. Contextual challenges also played their roles as the findings of this study, along with the literature review in Chapter 2, indicated budgetary constraints in the SANDF, which might have an impact on the resource allocation to the advancement of cybersecurity training in the organisation. On the other hand, contextual challenges also provided insight into the restrictions relating to cultivating a digital culture in the SANDF. The identified existing financial constraints, for example, could well be a major reason why cybersecurity awareness training and education have not featured prominently in the organisation. Furthermore, the use of outdated technologies might be due to the lack of resources.

Developing a cybersecurity culture in the SANDF could not be omitted from the core theme, namely awareness creation. The manner in which cybersecurity is framed is linked closely to key human practices applied in securing physical information; the practice of securing information and executing security behaviour should therefore be aligned. Hence, as derived from this study, the researcher concludes that a high level of uncertainty limits best practices in cybersecurity behaviour and the optimal implementation of guidelines in the SANDF, both of which require urgent resolution.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, *33*(3), 237–248.

Accenture. (2020). *Insight into the cyberthreat landscape in South Africa*. https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat- Landscape-Of-South-Africa-V5.pdf

Acharya, A., & Buzan, B. (2017). Why is there no non-Western international relations theory? Ten years on. *International Relations of the Asia-Pacific*, *17*(3), 341–370. DOI: 10.1093/irap/lcx006

Adams, J. (2012). Managing transport risks: What works? In R. Hillerbrand, P. Sandin, & M. Peterson. (Eds.), *Handbook of risk theory: Epistemology, decision theory, ethics, and social implications of risk* (pp. 239-264). Springer Science Business Media.

Adams, W. (2015). Conducting semi-structured interviews. In K. E. Newcomer, H. P. Hatry, & J. S. Wholey (Eds.), *Handbook of practical program evaluation* (4th ed., Chapter 19). Wiley Online Library. https://doi.org/10.1002/9781119171386.ch19

Adedolapo, A. A. (2016). *Bring your own device adoption in South African SMEs* [Unpublished master's dissertation]. University of Cape Town. https://open.uct.ac.za/bitstream/item/26232/thesis_com_2016_akin_adetoro_adedol apo.pdf?sequence=1

Adjei, J., Adams, S., Mensah, I., Tobbin, P., & Odei-Appiah, S. (2020). Digital identity management on social media: Exploring the factors that influence personal information disclosure on social media. *Journal of Sustainability*, *12*(23), 9994. https://doi.org/10.3390/su12239994

Adjei, J., Pearl, T., & Tobbin, P. (2020). Sense making of shared information: Perspective of relevance in WhatsApp. *Nordic and Baltic Journal of Information and Communications Technologies*, *1*, 159–184. DOI: 10.13052/nbjict1902-097X.2020.007

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018, March 16). *Assessing cybersecurity policy effectiveness in Africa via a cybersecurity liability index* [Conference presentation]. Forty-Sixth Research Conference On

Communication, Information and Internet Policy. https://doi.org/10.2139/ssrn.3142296

Aghatise, J. (2006). *Cybercrime definition*. http://www.researchgate.net/publication/265350281_Cybercrime_definition

Ahmad, F., & Huvila, I. (2019). Organizational changes, trust and information sharing: An empirical study. *Aslib Journal of Information Management*, *71*(5), 677–692.

Alam, T., Ullah, Z., AlDhaen, F. S., AlDhaen, E., Ahmad, N., & Scholz, M. (2021). Towards explaining knowledge hiding through relationship conflict, frustration, and irritability: The case of public sector teaching hospitals. *Sustainability, 13*, 12598. https://doi.org/10.3390/su132212598

Al-Dawod, F., & Stefanska, B. (2021). *The importance of risk awareness in cybersecurity among companies: A perspective on the role of top management* [Unpublished master's thesis]. Linköping University. https://www.diva-portal.org/smash/get/diva2:1571695/FULLTEXT01.pdf

Aldis, A., & Drent, M. E. (2008). *Common norms and good practices of civil-military relations in the EU*. Harmonie Papers.

Alharahsheh, H. H., & Pius, A. (2020). A review of key paradigms: Positivism vs interpretivism. *Global Academic Journal of Humanities and Social Sciences*, *2*(3), 39–43.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23. https://doi.org/ 10.3390/bdcc5020023

Alhojailan, M. I. (2012). Thematic analysis: A critical review of its process and evaluation. *West East Journal of Social Sciences*, *1*(1), 39–47. https://faculty.ksu.edu.sa/sites/default/files/ta_thematic_analysis_dr_mohammed_al hojailan.pdf

Al-Izki, F., & Weir, G. R. (2016). *Management attitudes toward information security in Omani public sector organizations* [Conference presentation]. First Cybersecurity and Cyber Forensics Conference, Computer and Information Sciences. https://pureportal.strath.ac.uk/en/publications/management-attitudes-toward- information-security-in-omani-public

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(2), 1–30. https://doi.org/10.1142/S0219649216500076

Allen, N. (2021, January 19). *Africa's evolving cyber threats*. Africa Center for Strategic Studies. https://africacenter.org/spotlight/africa-evolving-cyber-threats/

Almara'beh, H., Amer, E. F., & Sulieman, A. (2016). The effectiveness of multimedia learning tools in education. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(12), 761–764.

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., & Musa, A. (2018). *Understanding awareness of cybersecurity threat among IT employees* [Conference presentation]. Sixth International Conference on Future Internet of Things and Cloud Workshops. DOI: 10.1109/W-FiCloud.2018.00036

Alotaibi, M., Furnell, S., & Clarke, N. (2017). *Information security policies: A review of challenges and influencing factors* [Conference presentation]. Eleventh International Conference for Internet Technology and Secured Transactions. https://ro.ecu.edu.au/ecuworkspost2013/2981/

Alvi, M. H. (2016). *A manual for selecting sampling techniques in research*. Personal RePEc Archive. http://mpra.ub.uni-muenchen.de/70218/

Ames, H., Glenton, C., & Lewin, S. (2019). Purposive sampling in a qualitative evidence synthesis: A worked example from a synthesis on parental perceptions of vaccination communication. *BMC Medical Research Methodology*, *19*, 26. https://doi.org/10.1186/s12874-019-0665-4

Ancis, J. R. (2020). The age of cyber psychology: An overview*. Technology, Mind and Behaviour, 1*(1). https://doi.org/10.1037/tmb0000009

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35.

Anney, V. N. (2014). Ensuring the quality of the findings of qualitative research: Looking at trustworthiness criteria. *Journal of Emerging Trends in Educational Research and Policy Studies*, *5(*2), 272–281.

Antonsen, T., & Lundestad, E. (2019). Borgmann and the non-neutrality of technology. *Techné: Research in Philosophy and Technology, 23*(1), 83–103. DOI: 10.5840/techne201951497

Arendse, D., & Maree, D. (2019). Exploring the factors of the English Comprehension Test. *South African Journal of Psychology*, *49*(3), 376–390. DOI: 10.1177/0081246318805268

Armenakis, A. A., & Bedeian, A. G. (1999). Organizational change: A review of theory and research in the 1990s. *Journal of Management, 25*(3), 293–315. https://doi.org/10.1177/014920639902500303

Aschmann, M., Jansen van Vuuren, J., & Leenen, L. (2015). Towards the establishment of an African cyber-army. *Journal of Information Warfare*, *14*(3), 15–29.

Aschmann, M. J., Leenen, L., & Jansen van Vuuren, J. C. (2017, March 2–3). *The utilisation of the deep web for military counter terrorist operations* [Conference paper]. International Conference on Cyber Warfare and Security, Dayton, Ohio, USA.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report*, *13*, 195–201. http://www.sis.pitt.edu/jjoshi/courses/IS2621/Spring2014/Paper1.pdf

Ashraf, C. (2021). Defining cyberwar: Towards a definitional framework. *Defense & Security Analysis, 37*(3), 274–294. DOI: 10.1080/14751798.2021.1959141

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: Enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), 13–19. DOI: 10.1016/S1361-3723(09)70088-0

Atrews, R. (2020). Cyberwarfare: Threats, security, attacks, and impact. *Journal of Information Warfare*, *19*(4), 17–28. https://www.jstor.org/stable/27033642

August, T., Dao, D., & Niculescu, M. F. (2021). Economics of ransomware: Risk interdependence and large-scale attacks. *Management Science*, *2021*, 1–24. https://www.scheller.gatech.edu/directory/faculty/niculescu/pubs/August-Dao-Niculescu-2021-Econ-of-Ransomware.pdf

Austin, J. L. (1975). *How to do things with words* (2nd ed). Harvard University Press.

Aydindag, D. (2021). Copenhagen school and securitization of cyberspace in Turkey. *Propósitos y Representaciones*, *9*(1), 1–19. http://dx.doi.org/10.20511/pyr2021.v9nSPE1.e850

Babbie, E. R. (2010). *The practice of social research*. Wadsworth Cengage Learning.

Babbie, E. R., & Mouton, J. (2007). *The practice of social research* (11th ed.). Oxford University Press.

Bachmann, V., & Gunneriusson, H. (2014). Terrorism and cyber attacks as hybrid threats: Defining a comprehensive approach for countering 21st century threats to global risk and security. *Journal of Terrorism and Security Analysis*, *2014*, 26–36. https://dx.doi.org/10.2139/ssrn.2252595

Bada, M., & Nurse, J. R. (2019a). Chapter 4 – The social and psychological impact of cyber-attacks. In B. Benson, & McAlaney, J. (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

Bada, M., & Nurse, J. R. (2019b). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bada, M., & Sasse, A. M. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* Global Cyber Security Capacity Centre.

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van de Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks*.* *PloS One*, *14*(12), e0224216. https://doi.org/10.1371/journal.pone.0224216

Bălău, N., & Utz, S. (2017). Information sharing as strategic behaviour: The role of information display, social motivation and time pressure. *Behaviour & Information Technology*, *36*(6), 589–605.

Ball, A., Ramim, M. M., & Levy, Y. (2015). Examining users’ personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management*, *3*(1), 180–207.

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context. *European Journal of International Relations*, *11*(2), 171–201.

Balzacq, T. (2011). *Securitization theory: How security problems emerge and dissolve*. Routledge.

Balzacq, T. (2015). The “essence” of securitization: Theory, ideal type, and a sociological science of security. *International Relations*, *29*(1), 103–113. https://doi.org/10.1177/0047117814526606b

Bardwell, A., Sean, B., & Remuis, W. (2017). *Cybersecurity education for military officers*. Naval Postgraduate School.

Barrett, M., Marron, J., Yan Pillitteri, V., Boyens, J., Quinn, S., Witte, G., & Feldman, L. (2020). *Approaches for federal agencies to use the cybersecurity framework*. United States of America’s National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8170-upd

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *59*, 9–25.

Baxter, J., & Eyles, J. (1997). Evaluating qualitative research in social geography: Establishing “rigor” in interview analysis. *Transactions of the Institute of British Geographers*, *22*, 505–525. http://dx.doi.org/10.1111/j.0020-2754.1997.00505.x

Becton, J. B., Walker, H. J., & Jones-Farmer, A. (2014). Generational differences in behaviour. *Journal Applied Social Psychology*, *44*(3), 175–189. https://doi.org/10.1111/jasp.12208

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Nursing Plus Open*, *2*, 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Benson, J. C., & McCarthy, B. R. (2016). *Server-based and server-less BYOD solutions to support electronic learning* [Unpublished master’s thesis]. Naval Postgraduate School.

Berelson, B. (1952). *Content analysis in communication research*. Free Press.

Berg, B. L. (2001). *Qualitative research methods for the social sciences*. Allyn and Bacon.

Berman, E. A. (2017). An exploratory sequential mixed methods approach to understanding researchers’ data management practices at UVM: Integrated findings to develop research data services. *Journal of eScience Librarianship*, *6*(1), 1–25. https://doi.org/10.7191/jeslib.2017.1104

Bester, C. (2003). *The management of information inside the general support base concept of the South African National Defence Force* [Unpublished master's thesis]. Stellenbosch University. http://scholar.sun.ac.za/handle/10019.1/16475

Bester, P. (2016). Military psychology for conventional operations in Africa. In G. A. van Dyk (Ed.), *Military psychology for Africa* (pp. 1–37). African Sun Media.

Bester, P., & Du Plessis, A. (2014). Adaptable leaders for the South African army. In D. Lindsay, & D. Woycheshin (Eds.), *Adaptive leadership in the military context: International perspectives* (pp. 127–156). Canadian Defence Academy Press.

Bester, P., & Du Plessis, A. (2015). When military leaders differ from their political leaders: Overcoming leadership challenges. In D. Lindsay, & D. Woycheshin (Eds.), *Overcoming leadership challenges: International perspectives* (pp. 203–226). Canadian Defence Academy Press.

Bigelow, B. (2019). What are military cyberspace operations other than war? *In The Proceedings of the Eleventh International Conference on Cyber Conflict*, pp. 1-17. DOI: 10.23919/CYCON.2019.8756835

Bing, C., Menn, J., & Satter, R. (2021, March 16). Putin likely directed 2020 U.S. election meddling, U.S. intelligence finds. *Reuters*. https://www.reuters.com/article/usa- election-cyber-int-idUSKBN2B82PF

Bird, W., & Lubisi, N. (2021, October 3). Disinformation in a time of Covid-19: The electoral code of conduct. *Daily Maverick*. https://www.dailymaverick.co.za/article/2021-10-03-disinformation-in-a-time-of-covid-19-the-electoral-code-of-conduct/

Bitsch, V. (2005). Qualitative research: A grounded theory example and evaluation criteria. *Journal of Agribusiness*, *23*(1), 75–91. DOI: 0.22004/ag.econ.59612

Bogdan, R., Holotescu, C., Andone, D., & Grosseck, G. (2017, April 27–28). *How MOOCS are being used for corporate training* [Conference presentation]. Thirteenth International Scientific Conference eLearning and Software for Education, Bucharest, Romania. DOI: 10.12753/2066-026X-17-000

Bontea, S. T. (2017). *The cyber threat to military just-in-time logistics: Risk mitigation and the return to forward basing*. School of Advanced Military Studies. https://apps.dtic.mil/sti/pdfs/AD1038872.pdf

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly: Management Information Systems*, *39*(4), 837–864.

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495–499. DOI: 10.1080/0735648X.2019.1692426

Bote, D. (2019). *The South African national cyber security policy framework: A critical analysis* [Unpublished master's thesis]. North-West University.

Bourbeau, P. (Ed.). (2015). *Security: Dialogue across disciplines*. Cambridge University Press.

Bourbeau, P., Balzacq, T., & Cavelty, M. (2015). International relations: Celebrating eclectic dynamism in security studies. In P. Bourbeau (Ed.), *Security: Dialogue across disciplines* (pp. 111–136). Cambridge University Press.

Bourbeau, P., & Vuori, J. A. (2015). Security, resilience and desecuritization: Multidirectional moves and dynamics. *Critical Studies on Security, 3*(3), 253–268. https://doi.org/10.1080/21624887.2015.1111095

Bourdieu, P. (1994). *Language and symbolic power*. Harvard University Press.

Bowden, M. (2019, June 29). The worm that nearly ate the Internet: It infected 10 million computers. So why did cyber-geddon never arrive? *New York Times*. https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html

Bowen, P. W., Rose, R., & Pilkington, A. (2017). Mixed methods – theory and practice: Sequential, explanatory approach. *International Journal of Quantitative and Qualitative Research Methods*, *5*(2), 10–27.

Boyabatli, O., Leng, T., & Toktay, B. (2015). The impact of budget constraints on flexible vs. dedicated technology choice. *Management Science*, *62*(1), 225–244. https://doi.org/10.1287/mnsc.2014.209

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Sage Publications.

Brangetto, P., & Veenendaal, M. A. (2016). *Influence cyber operations: The use of cyberattacks in support of influence operations* [Conference presentation]. Eighth International Conference on Cyber Conflict. https://doi.org/10.1109/CYCON.2016.7529430

Brantly, A. (2021). Risk and uncertainty can be analysed in cyberspace. *Journal of Cybersecurity*, *7*(1), tyab001. https://doi.org/10.1093/cybsec/tyab001

Brantly, A., & Smeets, M. (2020). Military operations in cyberspace. In A. Sookermany (Ed.), *Handbook of military sciences* (pp. 1–16). Springer Link. https://link.springer.com/referenceworkentry/10.1007/978-3-030-02866-4_19-1

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Briggs, C. M. (2020). Climate change and hybrid warfare strategies. *Journal of Strategic Security*, *13*(4), 45–57. https://doi.org/10.5038/1944-0472.13.4.1864

Bronk, C. (2018). *Cyber warfare: Routledge handbook of defence studies*. Routledge.

Brown, V. J. (2014). Risk perception: It's personal. *Environmental Health Perspectives*, *122*(10), A276–A279. https://doi.org/10.1289/ehp.122-A276

Bruwer, N. (2016). Military psychology and peacekeeping operations. In G. A. van Dyk (Ed.), *Military psychology in Africa.* (pp 43–65). African Sun Media.

Bryan, A., & Volchenkova, K. (2016). Blended learning: Definition, models, implications for higher education. *Educational Sciences*, *8*(2), 24–30. DOI: 10.14529/ped160204

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press.

Bueger, C. (2015). What is maritime security? *Marine Policy*, *53*, 59–164. https://doi.org/10.1016/j.marpol.2014.12.005

Bueger, C., Larsen, J., & Schätzlein, M. (2019, June 20). *Towards a maritime security architecture for the Western Indian Ocean: A strategic review for the Contact Group on Piracy off the Coast of Somalia*. Report prepared for the 22nd CGPCS

Plenary in Balaclava, Mauritius. https://pure.diis.dk/ws/files/4019171/Strategic_Review_for_CGPCS_Final.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

Business Insider South Africa. (2019, July 24). *This startling graph shows how many Africans are now using the internet – far more than in North America, and on track to beat Europe*. https://www.businessinsider.co.za/internet-users-in-africa-2019-7

Business Insider South Africa. (2020, June 3). *Hackers on the dark web love South Africa – here's why we suffer 577 attacks per hour*. https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6

Business Tech. (2021, June 18). *South Africa to deploy military to help with Covid-19 third wave*. https://businesstech.co.za/news/government/499285/south- africa-to-deploy-military-to-help-with-covid-19-third-wave/

Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-Cold War era*. Longman.

Buzan, B. (2006). Will the 'global war on terrorism' be the new Cold War? *International Affairs*, *82*(6),1101–1118.

Buzan, B. (2008). The changing agenda of military security. In H. G. Brauch, U. O. Spring, C. Mesjasz, J. Grin, N. C. Behera, B. Chourou, P. Kameri-Mbote, & P. H. Liotta (Eds.), *Globalization and environmental challenges*. Hexagon Series on Human and Environmental Security and Peace (Vol. 3). Springer. https://doi.org/10.1007/978-3-540-75977-5_41

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.

Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press.

Buzan, B., & Wæver, O. (2009). Macro-securitisation and security constellations: Reconsidering scale in securitisation theory. *Review of International Studies*, *35*(2), 253–276. https://www.jstor.org/stable/20542789

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.

Camblor, M. P., & Alcover, C. M. (2019). Integrating distrust antecedents and consequences in organizational life. *Journal of Work and Organizational Psychology*, *35*(1), 17–26. https://doi.org/10.5093/jwop2019a3

Cascio, W. F., & Montealegre, R. (2016). How technology is changing work and organizations. *Annual Review of Organizational Psychology and Organizational Behavior*, *3*, 349–375.

Catanzaro, M. (1988). Using qualitative analytical techniques. *Nursing: Research Theory and Practice*, *8*(7), 437–456.

Cavelty, M. D. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse*. International Studies Review*, *15*, 105–122. DOI: 10.1111/misr.12023

Cavelty, M. D., & Wegner, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. DOI: 10.1080/13523260.2019.1678855

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication*, *20*, 133–155. https://doi.org/10.23962/10539/23572

Chandrasekhar, C., & Mee, P. (2021, May 3). *Why businesses and governments must fight cyber threats together*. World Economic Forum Global Agenda. https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/

Charrett, C. (2009). *A critical application of securitization theory: Overcoming the normative dilemma of writing security*. Working paper no. 2009/7. International Catalan Institute for Peace. https://dx.doi.org/10.2139/ssrn.1884149

Chaumba, J. (2013). The use and value of mixed methods research in social work. *Advances in Social Work*, *14*(2), 307–333. https://doi.org/10.18060/1858

Chinje, N. B., & Chinomona, R. (2015). Digital natives and information sharing on social media platforms: Implications for managers. *Journal of Contemporary Management*, *12*(1), 795–814. https://hdl.handle.net/10520/EJC178601

Chionis, D., & Karanikas, N. (2018). Differences in risk perception factors and behaviours amongst and within professionals and trainees in the aviation engineering domain. *Aerospace*, *5*, 1–23. DOI: 10.3390/aerospace5020062

Chow, S. L. (2002). Statistics and its role in psychological research. In *Encyclopaedia of life support systems: Methods in psychological research*. Eolss Publishers. https://web-archive.southampton.ac.uk/cogprints.org/2782/1/EOLSSsta.pdf

Cilliers, J. (2020). *Africa first: Igniting a growth revolution*. Jonathan Ball Publishers.

Cimpanu, C. (2021, May 19). Israel bombed two Hamas cyber targets. *The Record*. https://therecord.media/israel-bombed-two-hamas-cyber-targets/

Cisco. (2022). *Cisco annual internet report (2018–2023)* [White Paper]. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual- internet-report/white-paper-c11-741490.html

Clarke, V., & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *Psychologist*, *26*(2), 120–123. http://eprints.uwe.ac.uk/21155

Cohen, L., Manion, L., & Morrison, K. (2011). *Research methods in education* (7th ed.). Routledge.

Collier-Reed, B. I., Ingerman, A., & Berglund, A. (2009). Reflections on trustworthiness in phenomenographic research: Recognising purpose, context and change in the process of research. *Education as Change*, *13*(2), 339–355.

Collins Dictionary. (2022). Definition of 'lekker'. https://www.collinsdictionary.com/dictionary/english/lekker

Colomer, J. (2020) National sovereignty is over. *Central European Political Science Review*, *21*(81). https://www.researchgate.net/publication/345179576_National_Sovereignty_is_Over/link/5fa0406a299bf1b53e5a5a84/download

Comte, A. (1856). *A general view of positivism*. Smith Elder & Co.

Cornish, P. (2018). *Military operations in cyberspace*. Wilton Park Reports. https://www.researchgate.net/publication/330181733_Military_operations_in_cyberspace

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. http://doi.org/10.22215/timreview/835

Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Pearson Education.

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.). Sage Publications.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed). Sage Publications.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed). Sage Publications.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (2nd ed.). Sage Publications.

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021, November 15). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*, *27*, 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

Dando, C., & Tranter, C. (2016). Military and defence applications. In A. Attrill, & C. Fullwood (Eds.), *Applied cyber psychology: Practical applications of cyberpsychological theory and research* (pp. 197–215). Palgrave Macmillan.

Daniels, P. (2020, March 5). *Cyber security and the South African National Defence Force*. https://static.pmg.org.za/200311CYBER_SECURITY.pdf

D’Arcy, J., & Greene, J. (2014). Security culture and the employment relationship as drivers of employees’ security compliance. *Information Management and Computer Security*, *22*, 474–489. DOI: 10.1108/IMCS-08-2013-0057

Dearlove, R. (2010). National security and public anxiety: Our changing perceptions. In L. K. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 33–40). Oxford Handbooks.

Dearnley, C. (2005). A reflection on the use of semi-structured interviews. *Nursing Research*, *13*(1), 19–28. DOI: 10.7748/nr2005.07.13.1.19.c5997

Deeming, C. (2016). Rethinking social policy and society. *Social Policy and Society*, *15*(2), 159–175. DOI: 10.1017/S1474746415000147

Defence Web. (2016, April 19). *SA National Defence College in synch with the Defence Review*. https://www.defenceweb.co.za/sa-defence/sa-defence-sa-defence/sa-national-defence-college-in-synch-with-the-defence-review/

Defence Web. (2019, May 31). *Armscor cybersecurity unit up and operational.* https://www.defenceweb.co.za/cyber-defence/armscor-cybersecurity-unit-up-and-operational/

Deibert, R. J. (2002). Circuits of power: Security in the internet environment. In J. N. Rosenau, & J. P. Singh (Eds.), *Information technologies and global politics: The changing scope of power and governance* (pp. 115–142). State University of New York.

De Jager, L., & Smith, E. (2016). *Internet access spending and advertising: South African entertainment and media outlook: 2012–2016*. https://docplayer.net/5471461- Internet-access-spending-and-advertising.html

De Lange, M. (2012). *Guidelines to establish an e-safety awareness in South Africa* [Unpublished master's thesis]. Nelson Mandela Metropolitan University.

Demchak, C. (2016). Uncivil and post-Western cyber Westphalia: Changing interstate power relations of the cybered age. *The Cyber Defense Review*, *1*(1), 49–74.

De Moura, G., & Goldstein, T. (2021, June 17). *What the Biden–Putin summit reveals about future of cyber attacks – and how to increase cybersecurity*. World Economic Forum. https://www.weforum.org/agenda/2021/06/joe-biden-vladimir-putin-summit-cybersecurity/

Denning, D. (1999). *Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy*. Nautilus.

Dentlinger, L. (2018, May 18). Declining budget hampers effectiveness of the SANDF. *Eyewitness News.* https://ewn.co.za/2018/05/18/declining-budget-hampers-effectiveness-of-sandf

Dinesen, S. L., & Sæther, H. B. (2013). *Cyber security: Securitizing cyber threats in Denmark* [Unpublished master's thesis]. Copenhagen Business School.

Dixon, O. C. (2008). *Warrior women: A qualitative content analysis of the perceptions of the experiences of Native American women professors in the academy*

[Unpublished doctoral dissertation]. University of San Francisco. https://www.academia.edu/11027034/Warrior_Women_A_Qualitative_Content_Analysis_of_the_Perceptions_of_the_Experiences_of_Native_American_Women_in_the_Academy

Djozo, K., Dimitrovska, A., & Angelevski, S. (2015). The impact of military education on the quality of decision making in military leaders. In *Proceedings of the International Scientific Conference, Researching Security – Approaches, concepts and policies*, pp. 65–79. https://www.researchgate.net/publication/328392256_THE_IMPACT_OF_MILITARY_EDUCATION_ON_THE_QUALITY_OF_DECISION_MAKING_IN_MILITARY_LEADERS

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1675404. DOI: 10.1080/23311886.2019.1675404

Dlamini, Z., & Modise, M. (2012, March 22–23). *Cyber security awareness initiatives in South Africa: A synergy approach* [Conference presentation]. Seventh International Conference on Information Warfare and Security, University of Washington, Seattle. http://hdl.handle.net/10204/5941

Dobbie, M. F., & Brown, R. R. (2014). A framework for understanding risk perception, explored from the perspective of the water practitioner. *Risk Analysis*, *34*(2), 294–308. DOI: 10.1111/risa.12100

Dobronravova, I. (2009). The true democracy and the true self-organization, triple C – Cognition, communication and co-operation. *Open Access Journal for a Global Sustainable Information Society*, *7*(1), 25–28.

Dong, K., Ali, R. F., Dominic, P. D., & Ali, S. E. (2021). The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability*, *13*, 2800. https://doi.org/10.3390/su13052800

Dönges, H. E., & Hofmann, S. C. (2018). Defence as security. In D. J. Galbreath, & J. R. Deni (Eds.), *Routledge handbook of defence studies* (pp. 29–39). Routledge.

Dos Santos, M. C. (2018). Identity and discourse in securitisation theory. *Contexto Internacional*, *40*(2), 229–248. http://dx.doi.org/10.1590/S0102-8529.2018400200003

Douzet, F. (2014). Understanding cyberspace with geopolitics. *Hérodote*, *1-2*(152-153), 3–21. https://doi.org/10.3917/her.152.0003

Downe-Wambolt, B. (1992). Content analysis: Method, applications and issues. *Health Care for Women International*, *13*, 313–321. https://doi.org/10.1080/07399339209516006

Doyle, H. (2015, August 27). New tools, new vulnerabilities: The emerging cyber-terrorism dyad. *The Cyber Defence Review*. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136007/new-tools-new-vulnerabilities-the-emerging-cyber-terrorism-dyad/

Ďulík, M., & Ďulík, J. R. (2019). Cyber security challenges in future military battlefield information networks. *Advances in Military Technology*, *14*(2), 263–277. DOI: 10.3849/aimt.01248

Du Plessis, C. (2020, July 28). Military doctors unhappy with 'WhatsApp deployment'. *Daily Maverick*. https://www.dailymaverick.co.za/article/2020-07-28-military-doctors- unhappy-with-whatsapp-deployment/

Du Plessis, C. (2021, July 23). Pegasus spying scandal: Rwanda targeted South Africa's Ramaphosa. *The Africa Report*. https://www.theafricareport.com/111202/pegasus-spying-scandal-rwanda-targeted-south-africas-president-ramaphosa/

Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: A South African context. *Acta Criminologica: Southern African Journal of Criminology*, *31*(3), 111–131.

Duvenage, P. (2019). *A conceptual framework for cyber counterintelligence* [Doctoral dissertation]. University of Johannesburg. http://hdl.handle.net/10210/400987

Edelmann, V. (2020). *Cyberattacks: A threat that unites military and civilian actors?* European Army Interoperability Centre. https://finabel.org/cyberattacks-a-threat-that-unites-military-and-civilian-actors/

Eggers, W., Turley, M., & Kishnani, P. K. (2018). *The future of regulation: Principles for regulating emerging technologies*. Deloitte Insights. https://www2.deloitte.com/content/dam/insights/us/articles/4538_Future-of-regulation/DI_Future-of-regulation.pdf

Egloff, F. J. (2015). Cybersecurity and the age of privateering: A historical analogy. *Cybersecurity Studies Programme: Working Paper Series*, *1*, 1–15. https://www.politics.ox.ac.uk/sites/default/files/2022-03/201503-CTGA-Egloff%20F-cybersecurityandtheageofprivateering.pdf

Egloff, F. J., & Cavelty, M. (2021). Attribution and knowledge creation assemblages in cybersecurity politics. *Journal of Cybersecurity*, *7*(1), 1–12. https://doi.org/10.1093/cybsec/tyab002

Elvin, G., & Johansson, E. (2017). *The impact of organizational culture on information security during development and management of IT systems: A comparative study between Japanese and Swedish banking industry* [Abstract]. Uppsala University. https://www.diva-portal.org/smash/get/diva2:1112265/FULLTEXT01.pdf

Eroukhmanoff, C. (2018). Securitisation theory: An introduction. In S. McGlinchey, R. Walters, & C. Scheinpflug (Eds.), *International relations theory* (pp. 1–4). E-International. https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/

Ertan, A., Crossland, G., & Heath, C. (2018). *Everyday cyber security in organisations*. https://www.researchgate.net/publication/340938936_Cyber_Security_Behaviour_In_Organisations/citation/download

Eysenck, M. W., & Keane, M. T. (2015). *Cognitive psychology. A student's handbook* (7th ed.). Psychology Press. https://doi.org/10.4324/9781315778006

Ezeokafor, E., & Kaunert, C. (2018). Securitization outside of the West: Conceptualizing the securitization – Neo-patrimonialism nexus in Africa. *Global Discourse*, *8*(2), 1–17. http://dx.doi.org/10.1080/23269995.2017.1412619

Fadia, A., Nayfeh, M., & Noble, J. (2020). *Follow the leaders: How governments can combat intensifying cybersecurity risks*. McKinsey and Company. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/

follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

Falco, E., Zambrano-Verratti, J., & Kleinhans, R. (2019). Web-based participatory mapping in informal settlements: The slums of Caracas, Venezuela. *Habitat International*, *94*(3), 1–20. https://doi.org/10.1016/j.habitatint.2019.102038

Farmer, T., Robinson, K., Elliot, S., & Eyles, J. (2006). Developing and implementing a triangulation protocol for qualitative health research. *Qualitative Health Research*, *16*(3), 377–394. https://doi.org/10.1177/1049732305285708

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019, April 27). The impact of age, gender, and educational level on the cybersecurity behaviours of tertiary institution students: An empirical investigation of Malaysian universities. *Journal of Physics Conference Series*, *2019*, 1339. https://doi:10.1088/1742-6596/1339/1/012098

Felix, J. (2020, September 2). No money to modernise current SANDF equipment, Parliament hears. *News24*. https://www.news24.com/news24/southafrica/news/no-money-to-modernise-current-sandf-equipment-parliament-hears-20200902

Feng, G. C. (2014). Intercoder reliability indices: Disuse, misuse, and abuse. *Quality & Quantity*, *48*, 1803–1815. https://doi.org/10.1007/s11135-013-9956-8

Ferrer, R., & Klein, W. M. (2015). Risk perceptions and health behavior. *Current Opinion in Psychology*, *5*, 85–89. https://doi.org/10.1016/j.copsyc.2015.03.012

Fianu, E., Blewett, C., Ampong, G. O., & Ofori, K. S. (2018). Factors affecting MOOC usage by students in selected Ghanaian universities. *Education Sciences*, *8*(2), 70. https://doi.org/10.3390/educsci8020070

Fichman, R. G., Dos Santos, B. L., & Zheng, Z. (2014). Digital innovation as a fundamental and powerful concept in the information systems curriculum. *MIS Quarterly*, *38*(2), 329–353.

Finlay, L. (2002). "Outing" the researcher: The provenance, process, and practice of reflexivity. *Qualitative Health Research*, *12*(4), 531–545. https://doi.org/10.1177/104973202129120052

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioural Decision Making*, *13*(1), 1–17. http://dx.doi.org/10.1002/(SICI)1099-0771(200001/03)13:1<1::AIDBDM333>3.0.CO;2-S

Floyd, R. (2007). Towards a consequentialist evaluation of security: Bringing together the Copenhagen and the Welsh schools of security studies. *Review of International Studies*, *33*(2), 327–350. https://doi.org/10.1017/S026021050700753X

Floyd, R. (2020). Securitisation and the function of functional actors. *Critical Studies on Security*, *9*(2), 81–97. DOI: 10.1080/21624887.2020.1827590

Forster, T., & Heinzel, M. (2021). Reacting, fast and slow: How world leaders shaped government responses to the COVID-19 pandemic. *Journal of European Public Policy*, *28*(8), 1299–1320. DOI: 10.1080/13501763.2021.1942157

Fouad, N. (2019). *The peculiarities of securitising cyberspace: A multi-actor analysis of the construction of cyber threats in the US (2003–2016)* [Conference presentation]. Eighteenth European Conference on Cyber Warfare and Security. https://www.researchgate.net/publication/334291099_The_Peculiarities_of_Securitising_Cyberspace_A_Multi-Actor_Analysis_of_the_Construction_of_Cyber_Threats_in_the_US_2003-2016

Fox, N. J. (2008). Post positivism. In L. M. Given (Ed.), *The SAGE encyclopedia of qualitative research methods* (pp. 659–664). Sage Publications.

Foxcroft, C., & Roodt, G. (2007). *Introduction to psychological assessments in the South African context* (4th ed.). Oxford University Press.

Fraenkel, J. R., & Wallen, N. E. (1996). *How to design and evaluate research in education*. McGraw-Hill.

Friedman, A. A., & West, D. M. (2010). Privacy and security in cloud computing. *Issues in Technology Innovation*, *3*, 1–13.

Furman, S., Theofanos, M., Choong, Y., & Stanton, B. (2012). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, *10*(2), 40–49. http://dx.doi.org/10.1109/MSP.2011.180

Gálik, S., & Tolnaiová, S. G. (2019). Cyberspace as a new existential dimension of man. In E. Abu-Taieh, A. E. Mouatasim, & I. H. Hadid (Eds.), *Cyberspace*. IntechOpen. https://doi.org/10.5772/intechopen.88156

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. *Automatika*, *58*(3), 273–286. DOI: 10.1080/00051144.2017.1407022

Gallarotti, G. M. (2011). Soft power: What it is, why it's important, and the conditions for its effective use. *Journal of Political Power*, *4*(1), 25–47. DOI: 10.1080/2158379X.2011.557886

Galletta, D., & Polak, P. (2003). An empirical investigation of antecedents of Internet abuse in the workplace. In *Proceedings of the Second Annual Workshop on HCI Research in MIS*, pp. 47–51. https://www.researchgate.net/publication/303152376_An_empirical_investigation_of_antecedents_of_internet_abuse_in_the_workplace

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber attacks: Social, political, economic, and cultural*. IEEE Technology & Society Magazine*, *30*(1), 28–38.

Garcia, A. (2017). A proposed South African army future deployment strategy concept system: The capstone concept and the operating concept. *South African Army Journal*. https://www.researchgate.net/publication/322078326_A_PROPOSED_SOUTH_AFRICAN_ARMY_FUTURE_DEPLOYMENT_STRATEGY_CONCEPT_SYSTEM_THE_CAPSTONE_CONCEPT_AND_THE_OPERATING_CONCEPT

Garg, V., & Camp, L. J. (2015). Cars, condoms, and Facebook. In Y. Desmedt (Ed.), *Information security* (pp. 280–289). Springer International Publishing. DOI: 10.1007/978-3-319-27659-5_20

Gazula, M. B. (2017). *Cyber warfare conflict analysis and case studies* [Unpublished master's thesis]. Massachusetts Institute of Technology.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *Journal of Information Systems in Developing Countries*, *80*(6), 1–17.

Geers, K. (2011). *Strategic cybersecurity.* CDD COE Publications.

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2014). *World War C: Understanding nation-state motives behind today's advanced cyber attacks*.

https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf

Georgieva, I. (2020). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy*, *41*(1), 33–54. DOI: 10.1080/13523260.2019.1677389

Gerber, J. (2017, December 13). Leaked SANDF document details powers of 'control officer' during state of emergency. *Mail & Guardian*. https://mg.co.za/article/2017-12-13-leaked-sandf-document-details-powers-of-control-officer-during-state-of- emergency/

Ghazvini, A., & Shukur, Z. (2016). Awareness training transfer and information security content development for healthcare industry. *International Journal of Advanced Computer Science and Applications*, *7*(5). DOI: 10.14569/IJACSA.2016.070549

Gökçe, K. G., & Dogerlioglu, O. (2019). "Bring your own device" policies: Perspectives of both employees and organizations. *Knowledge Management & E-Learning*, *11*(2), 233–246. https://doi.org/10.34105/j.kmel.2019.11.012

Gomez, M. A. (2017). Victory in cyberspace. *IAFOR Journal of Politics, Economics & Law*, *4*(1), 40–51. DOI: 10.22492/ijpel.4.1.04

Gonzalez-Manzano, L., De Fuentes, J. M., Ramos, C., Sanchez, A., & Quispe, F. (2022). Identifying key relationships between nation-state cyberattacks and geopolitical and economic factors: A model. *Security and Communication Networks*, *2022*, 5784674. https://doi.org/10.1155/2022/5784674

Goodwin, C., & Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., Massagli, A., McKay, A., McKitrick, P., Neutze, J., Storch, T., & Sullivan, K. (2015). *A framework for cybersecurity Information sharing and risk reduction*. Microsoft. https://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf

Goran, J., LaBerge, L., & Srinivasan, R. (2017, July 20). Culture for a digital age. *McKinsey Quarterly*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/culture-for-a-digital-age

Grabner-Kräuter, S. (2018). Cybersecurity. In R. B. Kolb (Ed.), *The SAGE encyclopaedia of business ethics and society* (Vol. 1, pp. 808-812). Sage Publications. http://dx.doi.org/10.4135/9781483381503.n286

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, *2*, 105–112. DOI: 10.1016/j.nedt.2003.10.001

Gray, D. E. (2009). *Doing research in the real world*. Sage Publications.

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis*, *11*(3), 255–274. https://doi.org/10.3102/01623737011003255

Griffiths, J. (2017). *Cyber security as an emerging challenge to South African national security* [Unpublished master's thesis]. University of Pretoria.

Grobler, M., & Dlamini, Z. (2012). Global cyber trends a South African reality. In *Proceedings of the International Information Management Corporation*. http://researchspace.csir.co.za/dspace/bitstream/handle/10204/5989/Grobler2_2012.pdf?sequence=1&isAllowed

Grobler, M., & Jansen van Vuuren, J. (2012). Collaboration as proactive measure against cyber warfare in South Africa. *African Security Review*, *21*(2), 61–73. DOI: 10.1080/10246029.2012.654803

Grobler, M., Jansen van Vuuren, J., & Zaaiman, J. (2013). Preparing South Africa for cybercrime and cyber defense. *Systemics, Cybernetics and Informatics*, *11*(7), 32–41. http://hdl.handle.net/10204/7140

Groenewald, T. (2004). A phenomenological research design illustrated. *International Journal of Qualitative Methods*, *3*(1), 42–55. https://doi.org/10.1177%2F160940690400300104

Guba, E. G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Technology Research and Development*, *29*(2), 75–91. https://doi.org/10.1007/BF02766777

Guba, E. G., & Lincoln, Y. S. (1989). What is this constructivist paradigm anyway? In E. G. Guba, & Y. S. Lincoln (Eds.), *Fourth generation evaluation* (pp. 79–90). Sage Publications,

Guion, L. A. (2002). *Triangulation: Establishing the validity of qualitative studies.* Institute of Food and Agricultural Studies, University of Florida Extension. https://scholar.google.co.za/scholar?cluster=2671080152376884768&hl=en&as_sdt=0,5&as_vis=1

Gunnarsson, K. (2018). *"Out of sight, out of mind": A qualitative study of the interrelated character of workplace attitudes and the within-couple division of parental leave* [Unpublished master's thesis]. Stockholm University.

Gupta, R., Bhardwaj, G., & Singh, G. (2019). *Employee perception and behavioural intention to adopt BYOD in organizations* [Conference presentation]. International Conference on Automation, Computational and Technology Management. https://www.researchgate.net/publication/335991746_Employee_Perception_and_Behavioral_Intention_to_Adopt_BYOD_in_the_Organizations

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Helyion*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hama, H. (2017). State security, societal security, and human security. *Jadavpur Journal of International Relations*, *21*(1), 1–19. DOI: 10.1177/0973598417706591

Hammarstrand, J., & Fu, T. (2015). *Information security awareness and behaviour of trained and untrained home users in Sweden* [Unpublished bachelor's thesis]. University of Borås. https://www.diva-portal.org/smash/get/diva2:950568/FULLTEXT01.pdf

Hansen, L. (2011). Theorizing the image for security studies: Visual securitization and the Muhammad cartoon crisis. *European Journal of International Relations*, *17*(1), 51–74. https://doi.org/10.1177/1354066110388593

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Harris, L., & Brown, G. (2010). Mixing interview and questionnaire methods: Practical problems in aligning data. *Practical Assessment Research & Evaluation, 15*, Article 1. http://pareonline.net/pdf/v15n1.pdf

Harwood, T., & Garry, T. (2003). An overview of content analysis. *The Marketing Review*, *3*, 479–498. DOI: 10.1362/146934703771910080

Hayes, J. (2009). Identity and securitization in the democratic peace: The United States and the divergence of response to India and Iran's nuclear programs. *International Studies Quarterly*, *53*, 977–999.

Heale, R., & Forbes. D. (2013). Understanding triangulation in research. *Evidence-Based Nursing*, *16*, 98. DOI: 10.1136/eb-2013-101494

Heartherly, C. J., & Melendez, I. (2019). Every soldier a cyber warrior: The case for cyber education in the United States Army. *Cyber Defence Review*, *4*(1), 63–74. https://www.jstor.org/stable/26623067

Heinecken, L. (2011). A diverse society, a representative military? The complexity of managing diversity in the South African armed forces. *South African Journal of Military Studies*, *37*(1), 25–49. DOI: 10.5787/37-1-58

Heinecken, L. (2017). Conceptualizing the tensions evoked by gender integration in the military: The South African case. *Armed Forces & Society*, *43*(2), 202–220. https://doi.org/10.1177/0095327X16670692

Heinecken, L., Gueli, R., & Neethling, A. (2005). Defence, democracy and South Africa's civil-military gap. *South African Journal of Military Studies*, *33*(1), 119–140.

Heinecken, L., & Visser, D. (2008). Officer education at the South African Military Academy: Social science but no sociology? *Armed Forces & Society*, *35*(1), 145–161. https://www.jstor.org/stable/48608838

Herjavec Group. (2019). *Official annual cybercrime report*. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Hinsenveld, N. H. (2015). *An overview of the "safety and security" cluster in Twente* [Unpublished bachelor's thesis]. University of Twente.

Hirsch Ballin, E., Dijstelbloem, H., & De Goede, P. (2020). The extension of the concept of security. In E. Hirsch Ballin, H. Dijstelbloem, & P. de Goede (Eds.), *Security in an interconnected world: A strategic vision for defence policy* (pp. 13–40). Springer. https://doi.org/10.1007/978-3-030-37606-2

Hjalmarson, O. (2013). *The securitization of cyberspace: How the web was won* [Unpublished bachelor's thesis]. Lund University.

Hlase, E. (2018). *The securitisation of cyberspace in South Africa: The tension between national security and civil liberties* [Unpublished master's thesis]. University of Pretoria.

Holland, R. (1999). Reflexivity. *Human Relations*, *52*(4), 463–484. https://doi.org/10.1007/978-3-319-60747-4_17

Holsti, O. (1968). Content analysis. In G. Lindzey, & E. Aronson (Eds.), *The handbook of social psychology* (2nd ed., Chapter 16). Addison-Wesley.

Hong, Y., & Goodnight, T. (2020). How to think about cyber sovereignty: The case of China. *Chinese Journal of Communication*, *13*(1), 8–26. DOI: 10.1080/17544750.2019.1687536

Hosken, G. (2016, July 13). SA's top military secrets stolen. *Business Live*. https://www.businesslive.co.za/rdm/technology/2016-07-13-sas-top-military-secrets-stolen/

Huang, D. L., Raua, P. L., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221–232. DOI: 10.1080/01449290701679361

Huntington, S. (1957). *The soldier and the state: The theory and politics of civil-military relations*. Belknap of Harvard University Press.

Huth, P., Bennett, D., & Gelpi, C. (1992). System uncertainty, risk propensity, and international conflict among the great powers. *Journal of Conflict Resolution*, *36*, 478–517. http://www.jstor.org/stable/174344

Huysmans, J. (1998). Revisiting Copenhagen: Or, on the creative development of a security studies agenda in Europe. *European Journal of International Relations*, *4*(4), 479–505.

Huysmans, J. (2006). *The politics of insecurity: Fear, migration and asylum in the EU*. Routledge. https://doi.org/10.4324/9780203008690

IBM Corporation. (2016). *Statistical Package for the Social Sciences version 24*. IBM Corp.

Idahosa, M. (2020). *Strategies for implementing successful IT security systems in small businesses* [Unpublished doctoral dissertation]. Walden University. https://scholarworks.waldenu.edu/dissertations/8546/

Inria. (2019, September 4). *Inria white book no. 03: Current challenges and Inria's research directions*. https://files.inria.fr/dircom/extranet/LB_cybersecurity_WEB.pdf

International Telecommunications Union (ITU). (2021). *Global cybersecurity index 2021*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Internet World Stats. (2022, July 20). *Internet users statistics for Africa*. https://www.internetworldstats.com/stats1.htm

Irandoost, D. H. (2018, March 3). Cybersecurity: A national security issue? *E-International Relations*. https://www.e-ir.info/2018/05/03/cybersecurity-a-national-security-issue/

Izuakor, C. (2016, February 19–21). *Understanding the impact of cybersecurity risks on safety* [Conference presentation]. Second International Conference on Information Systems Security and Privacy, Rome, Italy. DOI: 10.5220/0005796805090513

Jabar, T., & Singh, M. (2022). Exploration of mobile device behavior for mitigating advanced persistent threats: A systematic literature review and conceptual framework. *Sensors*, *22*, 1–38.

Jacob, J., Peters, M., & Yang, A. T. (2020). Interdisciplinary cybersecurity: Rethinking the approach and the process. In K. K. Choo, T. Morris, & G. Peterson (Eds.), *National cyber summit research track: Advances in intelligent systems and computing* (Vol. 1055). Springer. https://doi.org/10.1007/978-3-030-31239-8_6

Jacobs, Y. (2021a, January 7). WhatsApp new privacy policy: Everything you need to know. *IOL*. https://www.iol.co.za/technology/mobile/whatsapp-new-privacy-policy-everything-you-need-to-know-fc0adae4-f7b2-4a22-a834-4c6408b3d53c

Jacobs, Y. (2021b, July 1). POPIA: What it means for WhatsApp groups. *IOL*. https://www.iol.co.za/technology/mobile/popia-what-it-means-for-whatsapp-groups-2c2f9edf-3f87-4f62-b9ff-bda53d703de8

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex and Intelligent Systems*, *7*, 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

Jalkanen, J. (2019). *Is the human the weakest link in information security? Systematic literature review* [Unpublished master's thesis]. University of Jyväskylä. https://jyx.jyu.fi/bitstream/handle/123456789/64186/URN%3ANBN%3Afi%3Ajyu-201905242795.pdf

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. DOI: 10.1016/j.jcss.2014.02.005

Janse van Rensburg, W. (2019). *Twenty years of democracy: An analysis of parliamentary oversight of the military in South Africa since 1994* [Unpublished doctoral dissertation]. Stellenbosch University.

Jansen, J., & Van Schaik, P. (2016). Understanding precautionary online behavioral intentions: A comparison of three models. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance*, pp. 1–11. https://research.tees.ac.uk/en/publications/understanding-precautionary-online-behavioural-intentions-a-compa-3

Jansen van Vuuren, J. C., Leenen, L., Phahlamohlaka, J., & Zaaiman, J. (2013). *Development of a South African cybersecurity policy implementation framework* [Conference presentation]. International Conference on Cyber Security and Warfare, Denver, Colorado, USA. https://www.researchgate.net/publication/266145673

Jansen van Vuuren, J. C., Leenen, L., & Zaaiman, J. J. (2014). *Using an ontology as a model for the implementation of the National Cybersecurity Policy Framework for South Africa* [Conference presentation]. International Conference on Cyber Warfare & Security, Denver, Colorado, USA. https://researchspace.csir.co.za/dspace/handle/10204/7869

Jibril, A. B., Kwarteng, M., Chovancová, M., & Denanyoh, R. (2020). Customers' perception of cybersecurity threats – Toward e-banking adoption and retention: A conceptual study. In *Proceedings of the Fifteenth International Conference on Cyber Warfare and Security*, pp. 270–276. https://publikace.k.utb.cz/handle/10563/1009676?locale-attribute=en

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, *1*(2), 112–133. https://doi.org/10.1177/1558689806298224

Jupillat, N. (2015). Armed attacks in cyberspace: The unseen threat to peace and security that redefines the law of state responsibility. *University of Detroit Mercy Law Review*, *92*(2), 115–130. https://ssrn.com/abstract=2772798

Kacała, T. (2015). Military leadership in the context of challenges and threats existing in the information environment. *Journal of Corporate Responsibility and Leadership*, *2*(1), 9–22. https://apcz.umk.pl/JCRL/article/view/JCRL.2015.001

Kacała, T. (2020). The perception of information and its role in exercising military leadership. *Journal of Corporate Responsibility and Leadership*, *6*(4), 23–41. DOI: 10.12775/JCRL.2019.013

Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan.

Kandeh, A., Botha, R., & Futcher, L. (2018). Enforcement of the Protection of Personal Information Act: Perspective of data management professionals. *SA Journal of Information Management*, *20*(1), 1–9. https://doi.org/10.4102/sajim.v20i1.917

Kapur, S. (2018). From Copenhagen to Uri and across the line of control: India's "surgical strikes" as a case of securitisation in two acts. *Global Discourse*, *8*(1), 62–79.

Kapur, S., & Mabon, S. (2018). The Copenhagen School goes global: Securitisation in the non-West. *Global Discourse*, *8*(1), 1–4. DOI: 10.1080/23269995.2018.1424686

Karaman, M., Çatalkaya, H., & Aybar, C. (2016). Institutional cybersecurity from the military perspective. *International Journal of Information Security Science*, *5*(1), 1–7. https://www.researchgate.net/publication/299533127_Institutional_Cybersecurity_from_Military_Perspective

Kärkkäinen, A. (2015). *Developing cyber security architecture for military networks using cognitive networking* [Unpublished doctoral dissertation]. Aalto University. http://urn.fi/URN:ISBN:978-952-60-6454-3

Karpavičiūtė, L. (2017). Securitization and Lithuania's national security change. *Lithuanian Foreign Policy Review*, *36*(1), 9–33. DOI: 10.1515/lfpr-2017-0005

Kaushik, V., & Walsh, C. A. (2019). Pragmatism as a research paradigm and its implications for social work research. *Social Sciences*, *8*(9), 255. https://doi.org/10.3390/socsci8090255

Kavanagh, C. (2019). *New tech, new threats, and new governance challenges: An opportunity to craft smarter responses?* Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP_Camino_KavanaghNew_Tech_New_Threats.pdf

Kemp, S. (2022, February 15). Digital 2022: South Africa. *Data Reportal*. https://datareportal.com/reports/digital-2022-south-africa

Khan, N. A., Brohi, S. N., & Zaman, N. (2020, December 5). Ten deadly cybersecurity threats amid COVID-19 pandemic. *TechRxiv*. https://doi.org/10.36227/techrxiv.12278792.v1

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2022). Cyber-security and risky behaviours in a developing country context: A Pakistani perspective. *Security Journal*, 2022. https://doi.org/10.1057/s41284-022-00343-4

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 2021. https://doi.org/10.1016/j.cose.2021.102267

Kiboi, B. (2015). *Cyber security as an emerging* threat *to Kenya's national security* [Unpublished master's thesis]. University of Pretoria.

Kivunja, C. (2018). Distinguishing between theory, theoretical framework, and conceptual framework: A systematic review of lessons from the field. *International Journal of Higher Education*, *7*(6), 44–53. DOI: 10.5430/ijhe.v7n6p44

Kohl, U. (2018).Territoriality and globalization (2018). In S. Allen, D. Costelloe, M. Fitzmaurice, P. Gragl, & E. Guntrip (Eds.), *Oxford handbook on jurisdiction in international law* (27 pages). Oxford University Press. https://ssrn.com/abstract=3259358

Kolini, F., & Janczewski, L. (2015). Cyber defense capability model: A foundation taxonomy. In *CONF-IRM 2015 Proceedings*. https://aisel.aisnet.org/confirm2015/32

Kolton, M. (2017). Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence. *Cyber Defence Review*, *2*(1), 119–154. http://www.jstor.org/stable/26267405

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research – Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. DOI: 10.1080/13814788.2017.1375092

Kortjan, N. (2013). *A cyber security awareness and education framework for South Africa* [Unpublished master's thesis]. Nelson Mandela Metropolitan University. http://hdl.handle.net/10948/d1014829

Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity*, *5*(1), 1–11. https://doi.org/10.1093/cybsec/tyz007

Krickeberg, M. (2016). The internet as a slippery object of state security: The problem of physical border insensitivity, anonymity and global interconnectedness. *Interstate – Journal of International Affairs*, *2*, 1–2. http://www.inquiriesjournal.com/a?id=1344

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology*. Sage Publications.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. DOI: 1016/j.cose.2010.08.001

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. DOI: 10.1080/1097198X.2019.1603527

Kvale, S. (1996). *Interview views: An introduction to qualitative research interviewing*. Sage Publications.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management and Computer Security*, *18*(1), 4–13. DOI: 101108/09685221011035223

Lacy, M. J., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*, 100–115.

Lacy, S., Watson, B. R., Riffe, D., & Lovejoy, J. (2015). Issues and best practices in content analysis. *Journalism & Mass Communication Quarterly*, *92*(4), 791–811. https://doi.org/10.1177/1077699015607338

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioural aspects of cybersecurity. *Cybersecurity*, *3*, 10. https://doi.org/10.1186/s42400-020-00050-w

Laitinen, K., & Sivunen, A. (2019). Enablers of and constraints on employees' information sharing on enterprise social media. *Information Technology and People*, *34*(2), 642–665. DOI: 10.1108/ITP-04-2019-0186

Larsen, J. (2020). Maritime security changing tack: A window on shifting configurations of power projection at sea. In E. R. Lucas, S. Rivera-Paez, T. Crosbie, & F. F Jensen (Eds.), *Maritime security: Counter-terrorism lessons from maritime piracy and narcotics interdiction* (pp. 170–183). IOS Press.

Larsen, M. H., & Lund, M. S. (2021). Cyber risk perception in the maritime domain: A systematic literature review. *IEEE Access*, *9*, 144895–144905. DOI: 10.1109/ACCESS.2021.3122433

Larsen, M. H., Lund, M. S., & Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research*, *3*, 100065. https://doi.org/10.1016/j.martra.2022.100065

Le, N. T., & Hoang, D. B. (2016, December 9–11). *Can maturity models support cyber security?* [Conference presentation]. Thirty-fifth International Performance Computing and Communications Conference, Las Vegas, Nevada, USA.

Leenen, L., Aschmann, M., Grobler, M., & Van Heerden, A. (2018). *Facing the culture gap in operationalising cyber within a military context* [Conference presentation]. Thirteenth International Conference on Cyber Warfare and Security, Washington, D.C., USA. http://toc.proceedings.com/38822webtoc.pdf

Leenen, L., & Jansen van Vuuren, J. (2019, February 28). *Framework for the cultivation of a military cybersecurity culture* [Conference presentation]. Fourteenth International Conference on Cyber Warfare and Security. Stellenbosch, South Africa.

Lehto, M. (2015). Phenomena in the cyber world. In M. Lehto, & P. Neittaanmäki (Eds.), *Cyber security: Analytics, technology and automation* (Vol. 78, pp. 3–29). Springer. https://doi.org/10.1007/978-3-319-18302-2_1

Lehto, M., & Henselmann, G. (2020). Non-kinetic warfare – The new game changer in the battle space. In B. K. Payne, & H. Wu (Eds.), *Proceedings of the 15th*

International Conference on Cyber Warfare and Security (pp. 316–325). Academic Conferences International. https://doi.org/10.34190/ICCWS.20.033

Leiter, A. (2020). Cyber sovereignty: A snapshot from a field in motion. *Harvard International Law Journal Frontiers*, *61*, 1–6. https://harvardilj.org/wp-content/uploads/sites/15/leiter-PDF-format.pdf

Lejaka, T. K., Da Veiga, A., & Loock, M. (2019). Cyber security awareness for small, medium and micro enterprises in South Africa. In *Proceedings of Conference on Information Communications Technology and Society*, pp. 1–6. DOI: 0.1109/ICTAS.2019.8703609

Lewis, J. A. (2006). *Cybersecurity and critical infrastructure protection.* Centre for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-rotection

Lewis, J. A., & Timlin, K. (2011). *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization.* United Nations Institute for Disarmament Research, Centre for Strategic and International Studies. https://unidir.org/publication/cybersecurity-and-cyberwarfare-preliminary-assessment-national-doctrine-and

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments*. Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lichtman, M. (2014). *Qualitative research for the social sciences*. Sage Publications. https://dx.doi.org/10.4135/9781544307756

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage Publications.

Liou, D. K., Chih, W. H., Hsu, L. C., & Huang, C. Y. (2016). Investigating information sharing behavior: The mediating roles of the desire to share information in virtual communities. *Information Systems and e-Business Management*, *14*, 187–216. https://doi.org/10.1007/s10257-015-0279-2

Lo, C. Y., & Thomas, N. (2018). The macro securitization of antimicrobial resistance in Asia. *Journal of International Affairs*, *72*(6), 567–583. DOI: 10.1080/10357718.2018.1534939

Loeb, S. J., Dynarski, S. M., McFarland, D. A., Morris, P., Reardon, S. F., & Reber, S. J. (2017). *Descriptive analysis in education: A guide for researchers*. National

Center for Education Evaluation and Regional Assistance. http://ies.ed.gov/ncee/

Louw, G. M. (2013). *South African defence policy and capability: The case of the South African National Defence Force* [Unpublished master's thesis]. Stellenbosch University. http://hdl.handle.net/10019.1/85766

Lucke, R. J. (2016, September 7–10). *How securitization theory can benefit from psychology findings* [Conference presentation]. ECPR General Conference, Prague, Czech Republic; Panel: Advances in Political Psychology: Methodological and Theoretical Contributions. https://opus4.kobv.de/opus4-uni-passau/frontdoor/deliver/index/docId/621/file/Lucke_Robin_Securitization_Psychology.pdf

Mabon, S. (2018). Existential threats and regulating life: Securitization in the contemporary Middle East. *Global Discourse*, *8*(1), 42–48. DOI: 10.1080/23269995.2017.1410001

MacArthur, V., & Conlan, O. (2012). *Addressing the challenges of survey fatigue for lifelong user modelling* [Conference presentation]. Twelfth IEEE International Conference on Advanced Learning Technologies. DOI: 10.1109/ICALT.2012.196

Mack, N., Woodsong, Y., MacQueen, K. M., Guest, G., & Namey, E. (2005). *Qualitative research methods: A data collector's field guide*. Family Health International, U.S. Agency for International Development.

MacNamara, C. (2019). *Power in cyberspace — How states operate in the digital domain* [Unpublished bachelor's degree]. Queens University. DOI: 10.13140/RG.2.2.29879.27048

Makhathini, T. N., & Van Dyk, G. (2018). Organisational climate, job satisfaction, and leadership style influences on organisational commitment among South African soldiers. *Journal of Psychology in Africa*, *28*(1), 21–25. DOI: 10.1080/14330237.2018.1438834

Malatji, M., Marnewick, A. L., & Von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability*, *13*(1), 291. https://doi.org/10.3390/su13010291

Mandrup, T. (2009). South Africa and the SADC stand-by force. *Scientia Militaria: South African Journal of Military Studies*, *37*(2), 1–24. DOI: 10.5787/37-2-66

Mange, T. (2019). *Knowledge management practices in local government: The case of the City of Johannesburg* [Master's thesis]. Stellenbosch University.

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. *Journal of Strategic Security*, *8*(5), 85–98. http://dx.doi.org/10.5038/1944-0472.8.3S.1478

Mannheim, K. (1952). The problem of generations. In P. Kecskemeti (Ed.), *Essays on the sociology of knowledge* (pp. 276–320). Routledge and Kegan Paul.

Mansell, R. (2016). Power, hierarchy and the internet: Why the internet empowers and disempowers. *Global Studies*, *9*(2), 19–25.

Marivate, V., & Combrink, H. (2020). Use of available data to inform the COVID-19 outbreak in South Africa: A case study. *Data Science Journal*, *19*(19), 1–7. DOI: 10.5334/dsj-2020-019

Marouf, L. (2015). Employee perception of the knowledge sharing culture in Kuwaiti companies: Effect of demographic characteristics. *Ibres*, *24*(2), 103–118.

Martin, G. (2020, March 12). Uncontrolled use of social networks a security risk for the SANDF. *Defence Web.* https://www.defenceweb.co.za/sa-defence/sa-defence-sa-defence/uncontrolled-use-of-social-networks-a-security-risk-for-the-sandf/

Martin, S. (2014). *Human perception: A comparative study of how others perceive me and how I perceive myself* [Unpublished bachelor's thesis]. Linnaeus University.

Mashiane, T., Dlamini, Z., & Mahlangu, T. (2019, February 28–March 1). *A rollout strategy for cybersecurity awareness campaigns* [Conference presentation]. Fourteenth International Conference on Cyber Warfare and Security, Stellenbosch University, Stellenbosch, South Africa.

Mashiloane, M. W., Mafini, C., & Pooe, R. D. (2018). Supply chain dynamism, information sharing, inter-organisational relationships and supply chain performance in the manufacturing sector. *Acta Commercii – Independent Research Journal in the Management Sciences*, *18*(1), 1–15. https://hdl.handle.net/10520/EJC-1033056e7b

May, R., Angel, E., & Ellenberger, H. (Eds.). (1958)*. Existence: A new dimension in psychiatry and psychology.* Basic Books/Hachette Book Group. https://doi.org/10.1037/11321-000

Mayring, P. (2002). Qualitative content analysis: Research instrument or mode of interpretation? In M. Kiegelmann (Ed.), *The role of the researcher in qualitative psychology* (pp. 139–148). Ingeborg Huber.

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *Journal of Computer Engineering*, *17*(3), 17–24. DOI: 10.9790/0661-17361724

McCain, N. (2021, July 21). Ramaphosa one of 14 world leaders targeted in Pegasus spyware case report. *News24.* https://www.news24.com/news24/southafrica/news/ramaphosa-one-of-14-world-leaders-targeted-in-pegasus-spyware-case-report-20210721

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156.

McDonald, M. (2008). Securitization and the construction of security. *European Journal of International Relations*, *14*(4), 563–587. https://doi.org/10.1177/1354066108097553

McDonald, N., Corrigan, S., Daly, C., & Cromie, S. (2000). Safety management systems and safety culture in aircraft maintenance organisations. *Safety Science*, *34*(1–3), 151–176. https://doi.org/10.1016/S0925-7535(00)00011-4

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 10021006. DOI: 10.1080/0142159X.2018.1497149

McMahon, C. (2020). In defence of the human factor. *Frontiers in Psychology*, *11*, 1390. DOI: 10.3389/fpsyg.2020.01390

Mendoza, D. K. (2017). The vulnerability of cyberspace: The cyber crime*. Journal of Forensic Science & Criminal Investigation*, *2*(1), 555576. https://juniperpublishers.com/jfsci/pdf/JFSCI.MS.ID.555576.pdf

Merriam, S. B. (1985). The case study in educational research: A review of selected literature. *Journal of Educational Thought*, *19*(3), 204–217. http://www.jstor.org/stable/23768608

Messick, S. (1995). Validity of psychological assessment: Validation of inferences from persons' responses and performances as scientific inquiry into score meaning. *American Psychologist*, *50*(9), 741–749. https://doi.org/10.1037/0003-066X.50.9.741

Mihaela, C. S. (2020). Current security threats in the national and international context. *Accounting and Management Information Systems*, *19*(1), 351–378. http://dx.doi.org/10.24818/jamis.2020.02007

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Sage Publications.

Mitrovic, Z., Veljkovic, I., Whyte, G., & Thompson, K. (2014, November 3–5). *Introducing BYOD in an organisation: The risk and customer services viewpoints* [Conference presentation]. First Namibia Customer Service Awards & Conference, Windhoek, Namibia. https://ir.nust.na/xmlui/bitstream/handle/10628/522/Veljkovic%20%26%20Whyte.%20Introducing%20BYOD%20in%20an%20organisation%20-%20the%20risk%20and%20customer%20services%20viewpoints.pdf?sequence=1&isAllowed=y

Mkhonza, L., & Letsoalo, A. (2017). *Understanding the skills gaps in the public service sector*. Public Service Sector Education and Training Authority. https://pseta.org.za/wp-content/uploads/2018/05/Understanding-the-Skills-Gaps-in-the-Public-Service-Sector.pdf

Modiba, M. M. (2020). *A digital transformation framework for South African financial service providers* [Unpublished doctoral dissertation]. North-West University.

Mohammad, R. (2014). *A description of the lived experiences of young adults who grew up in religiously heterogeneous households* [Unpublished master's thesis]. Stellenbosch University.

Molwantwa, D. M. (2019). *Aligning the constitutional rights of citizens with cybersecurity measures in South Africa* [Unpublished master's thesis]. North-West University. https://www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

Montesh, M., & Basdeo, V. (2012). The role of the South African National Defence Force in policing. *Scientia Militaria: South African Journal of Military Studies*, *40*(1), 71–94.

Mousa, S. (2019). Cyber security: Exploring awareness among university students at a public educational institution. *International Journal of Innovative Research and Knowledge*, *5*, 88–97.

Moussa, M. (2015). *Monitoring employee behavior through the use of technology and issues of employee privacy in America*. SAGE Open. https://doi.org/10.1177/2158244015580168

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers Psychology*, *12*, 561011. DOI: 10.3389/fpsyg.2021.561011

Moustakas, C. E. (1994). *Phenomenological research methods.* Sage Publications.

Mukiibi, H. (2019). Cyber security in Africa: The boring technology story that matters. XRDS: *Crossroads, The ACM Magazine for Students*, *26*, 56–59. DOI: 10.1145/3368077

Mulazzani, F., & Sarcia, S. A. (2011). *Cyber security on military deployed networks* [Conference presentation]. Third International Conference on Cyber Conflict, Talinn, Estonia. https://ccdcoe.org/uploads/2018/10/CyberSecurityOnMilitaryDeployedNetworks-Mulazzani-Sarcia.pdf

Murire, O. T., Flowerday, S., Strydom, K., & Fourie, C. J. (2021). Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. *Journal of Transdisciplinary Research Southern Africa*, *17*(1), a909. https://doi. org/10.4102/td.v17i1.909

Mutimer, D. (1997). Beyond strategy: Critical thinking and the new security studies. In C. A. Snyder (Ed.), *Contemporary security studies* (p. 90). Macmillan.

Myre, G. (2022, April 26). How does Ukraine keep intercepting Russian military communications? Special series: Ukraine invasion explained. *NPR*. https://www.npr.org/2022/04/26/1094656395/how-does-ukraine-keep-intercepting-russian-military-communications

Nævestad, T. O., Meyer, F. S., & Honerud, H. J. (2018, June 17–21). Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security. In S. Haugen, A. Barros, C. van Gulijk, T. Kongsvik., & J. E. Vinnem (Eds.), *Safety* *and reliability – Safe societies in a changing world*: *Proceedings of ESREL*, Trondheim, Norway. CRC Press. https://doi.org/10.1201/9781351174664

Naidoo, K. (2020). *Innovation, digital platform technologies and employment: An overview of key issues and emerging trends in South Africa.* Southern Centre for Inequality Studies, University of the Witwatersrand. https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/scis/documents/9%20Naidoo%20emerging%20trends%20in%20South%20Africa.docx.pdf

National Institute of Standards and Technology. (2011). *Managing information security risk: Organization, mission, and information system view*. United States Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Nelwamondo, M., & Njenga, J. (2021). Approaches for enhancing information sharing between government and communities in Western Cape. *South African Journal of Information Management*, *23*(1), 1–9. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1560-683X2021000100035

Netolická, V., & Mareš, M. (2018). Arms race “in cyberspace” — A case study of Iran and Israel. *Comparative Strategy*, *37*(5), 414–429. DOI: 10.1080/01495933.2018.1526568

Neuendorf, K. A. (2002). *The content analysis guidebook*. Sage Publications.

Ngcobo, B. (2020). *Cyber defence strategy* [PowerPoint slides]. Cyber Command: South African Defence Intelligence. https://static.pmg.org.za/200311CYBER.pdf

Nielsen, S. (2016). The role of the U.S. military in cyberspace. *Journal of Information Warfare*, *15*(2), 27–38. https://www.jstor.org/stable/26487529

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology*, *7*(2), 61–73.

North, M. S., & Fiske, S. T. (2012). An inconvenienced youth? Ageism and its potential intergenerational roots*.* *Psychological Bulletin*, *138*(5), 982–997. DOI: 10.1037/a0027843

Ntsaluba, N. (2017). *Cybersecurity policy and legislation in South Africa* [Unpublished master’s thesis]. University of Pretoria.

Nunnally, J. C., & Bernstein, I. H. (1994). The assessment of reliability. *Psychometric Theory*, *3*, 248–292.

Nye, J. (2021). Soft power: The evolution of a concept. *Journal of Political Power*, *14(1),* 196–208. DOI: 10.1080/2158379X.2021.1879572

O’Brien, T. C., & Tropp, L. R. (2015). Psychology: The phenomenology of human security. In P. Bourbeau (Ed.), *Security: Dialogue across disciplines* (pp. 137–155). Cambridge University Press.

O’Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: Debates and practical guidelines. *International Journal of Qualitative Methods*, January 2020. https://doi.org/10.1177/1609406919899220

Painter, C. (2018). The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. *The Foreign Service Journal*, June 2018. https://afsa.org/diplomacy-cyberspace

Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity. *A Review: Decision Analysis*, *16*(3), 157–237. https://doi.org/10.1287/deca.2018.0387

Palaganas, E. C., Sanchez, M. C., Molintas, M. P., & Caricativo, R. D. (2017). Reflexivity in qualitative research: A journey of learning. *The Qualitative Report*, *22*(2), 426–438. https://doi.org/10.46743/2160-3715/2017.2552

Palinkas, L., Horwitz, S., & Green, C., Wisdom, J., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health*, *42*(5), 533–544. DOI: 10.1007/s10488-013-0528-y

Paliszkiewicz, J., Svanadze, S., & Jikia, M. (2017). The role of knowledge management processes on organizational culture. *Online Journal of Applied Knowledge Management*, *5*(2), 29–44. https://doi.org/10.36965/OJAKM.20175(2)29-44

Papazoglou, G. (2019). Society and culture: Cultural policies driven by local authorities as a factor in local development – The example of the Municipality of Xanthi, Greece. *Heritage*, *2*(3), 2625–2639. https://doi.org/10.3390/heritage2030161

Parahoo, K. (2006). *Nursing research: Principles, process, and issues*. Palgrave Macmillan.

Parliamentary Monitoring Group (PMG). (2020, March 11). *Cyber warfare policy: Department of Defence briefing minutes.* https://pmg.org.za/committee-meeting/30014/

Parliamentary Monitoring Group (PMG). (2022, May 11). *Report of the Portfolio Committee on Defence and Military Veterans on Budget Vote 26.* https://pmg.org.za/tabled-committee-report/4982/

Parusheva, S. (2019). Digitalization and digital transformation in construction: Benefits and challenges. Information and communication technologies in business and education. In *Proceedings of the International Conference Dedicated to the 50th Anniversary of the Department of Informatics*, pp. 126–134.

Patil, B. V., & Joshi, M. J. (2014). Usages of selected antivirus software in different categories of users in selected districts. *Journal of Environmental Science, Computer Science and Engineering & Technology*, *3*(2), 6769–6973.

Patino, C. M., & Ferreira, J. C. (2018). Inclusion and exclusion criteria in research studies: Definitions and why they matter. *Jornal Brasileiro de Pneumologia*, *44*(2), 84. DOI: 10.1590/S1806-37562018000000088

Patrick, A. (2021, July 7). Military doctors were right: WhatsApp is not right for orders to deploy. *Times Live*. https://www.timeslive.co.za/news/south-africa/2021-04-22- military-doctors-were-right-whatsapp-is-not-right-for-orders-to-deploy/

Patrick, H., Van Niekerk, B., & Fields, Z. (2016). Security-information flow in the South African public sector. *Journal of Information Warfare*, *15*(4), 68–85. https://www.jstor.org/stable/26487552

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage Publications.

Petit, J. (2022, March 22). 5 social engineering attacks to watch out for. *Tripwire: The State of Security*. http://www.tripwire.com/state-of-security/security-awareness/5- social-engineering-attacks-to-watch-out-for/

Philipsen, L. (2018). Performative securitization: From conditions of success to conditions of possibility. *Journal of International Relations and Development*, *23*, 139–163. https://doi.org/10.1057/s41268-018-0130-8

Pierce, G., Cleary, P., Holland, C., & Rabrenovic, G. (2018). Security challenges in the 21st century: The changing nature of risk, security and sustainability. In M.

Hoffman (Ed.), *Advances in cross-cultural decision making: Advances in intelligent systems and computing* (pp. 180–190). Springer. https://doi.org/10.1007/978-3-319-60747-4_17

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *African Journal of Information and Communication*, *28*, 1–21. https://doi.org/10.23962/10539/32213

Pillow, W. (2003). Confession, catharsis, or cure? Rethinking the uses of reflexivity as methodological power in qualitative research. *International Journal of Qualitative Studies in Education*, *16*(2), 175–196. DOI: 10.1080/0951839032000060635

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Franco Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*, 371–390. https://doi.org/10.1007/s10111-021-00683-y

Potgieter, P. (2018). The awareness behaviour of students on cyber security awareness by using social media platforms: A case study at Central University of Technology. *Proceedings of the Fourth International Conference on the Internet, Cyber Security and Information Systems*, *12*, 272–280.

Pram Gad, U., & Lund Petersen, K. (2011). Concepts of politics in securitization studies. *Security Dialogue*, *42*(4–5), 315–328. https://doi.org/10.1177/0967010611418716

Prevezianou, M. F. (2021). Beyond ones and zeros: Conceptualizing cyber crises. *Risk, Hazards and Crisis in Public Policy*, *12*(1), 51–72. https://doi.org/10.1002/rhc3.12204

Public-Private Analytical Exchange Programme. (2019). *Commodification of cyber-capabilities: A grand cyber-arms bazaar.* https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf

Pucetaite, R., Lamsa, A. M., & Novelskaite, A. (2010). Building organizational trust in a low-trust societal context. *Baltic Journal of Management*, *5*(2), 197–217. DOI: 10.1108/17465261011045124

Rahman, M. M., Arif, M. T., Luke, F., Letchumi, S., Nabila, F., Ling, C. W., Chin, E. S., & Baharin, N. (2020). Factors affecting internet use among university students in Sarawak, Malaysia: An empirical study. *International Journal of Community Medicine and Public Health*, *7*, 848–854. http://dx.doi.org/10.18203/2394-6040.ijcmph20200933

Ramluckan, T., Van Niekerk, B., & Leenen, L. (2020). Cybersecurity and information warfare research in South Africa: Challenges and proposed solutions. *Journal of Information Warfare*, *19*(1), 80–95.

Rauf, A. (2019). *The importance of human factor in cybersecurity* [Abstract]. National University of Sciences and Technology. https://www.researchgate.net/publication/332539716_The_Importance_of_Human_Factor_in_Cybersecurity/citation/download

Rawoot, I., Van Heerden, A., & Parker, L. (2017). Operational forces soldiers' perceptions of attributes and skills for career success. *South African Journal of Industrial Psychology*, *43*(1), 1–9. DOI: 10.4102/sajip.v43i0.1440

Republic of South Africa (RSA). (1950). *Population Registration Act 30 of 1950*. Government Printer. http://psimg.jstor.org/fsi/img/pdf/t0/10.5555/al.sff.document.leg19500707.028.020.030_final.pdf

Republic of South Africa (RSA). (1996). *Constitution of the Republic of South Africa Act 108 of 1996*. Government Printer.

Republic of South Africa (RSA). (2000). *Promotion of Access to Information Act 2 of 2000*. Government Printer.

Republic of South Africa (RSA). (2002a). *Electronic Communications and Transactions Act 25 of 2002*. Government Printer.

Republic of South Africa (RSA). (2002b). *Defence Act 42 of 2002*. Government Printer.

Republic of South Africa (RSA). (2010). Department of Defence. *South African military security awareness learning manual.* Government Printer.

Republic of South Africa (RSA). (2011a). Department of Defence. *Instruction DODI/CMI/00008/2001: Policy, process and procedures on information and communications systems security in the Department of Defence (Edition 4)*. Government Printer.

Republic of South Africa (RSA). (2011b). Department of Defence. *Instruction DOD/CMIS/R/318/1/P: Policy on the use of cellular telephones in the Department of Defence (Edition 4)*. Government Printer.

Republic of South Africa (RSA). (2011c). Department of Defence. *Instruction POL&PLAN NO/00022/1999: Policy on the disclosure of defence information.* Government Printer.

Republic of South Africa (RSA). (2013a). Department of Defence. *Instruction DODI/CMI/00011/2001: Policy on electronic mail in the Department of Defence.* Government Printer.

Republic of South Africa (RSA). (2013b). *Protection of Personal Information Act 4 of 2013*. Government Printer.

Republic of South Africa (RSA). (2015a). Department of Defence. *South African defence review*. https://static.pmg.org.za/170512review.pdf

Republic of South Africa (RSA). (2015b). State Security Agency. *National cybersecurity policy framework (NCPF).* Government Printer.

Republic of South Africa. (2016). *Cybercrimes and Cybersecurity Bill of 2017*. https://www.gov.za/sites/default/files/gcis_document/201703/b6-2017cybercrimes170221a.pdf

Republic of South Africa (RSA). (2017a). Department of Defence. *Budget vote 2017/2018*. https://www.gov.za/speeches/minister-nosiviwe-mapisa-nqakula-defence-and-military-veterans-dept-budget-vote-201718-25

Republic of South Africa (RSA). (2017b). Department of Telecommunications and Postal Services. *Baseline study on the cybersecurity readiness: A report of the Department of Telecommunications and Postal Services*. https://www.cybersecurityhub.gov.za/images/docs/Cyber-Readiness-Report.pdf

Republic of South Africa (RSA). (2018). Department of Defence. *Budget vote 2018/2019*. https://www.gov.za/speeches/minister-nosiviwe-mapisa-nqakula-defence-dept-budget-vote-201819-18-may-2018-0000

Republic of South Africa (RSA). (2020a). *Cybercrimes Act 19 of 2020.* Government Printer.

Republic of South Africa. (2020b). Department of Defence. *Annual report 2020/2021*. https://www.gov.za/sites/default/files/gcis_document/202110/defenceannualreport202021.pdf

Republic of South Africa (RSA). (2021). Department of Defence and Military Veterans. *Budget vote 2021/22*. https://www.gov.za/speeches/minister-nosiviwe-mapisa-nqakula-defence-and-military-veterans-dept-budget-vote-202122-18

Republic of South Africa (RSA). (2022). Department of Defence. *Budget vote 2022/23*. https://www.gov.za/speeches/minister-thandi-modise-defence-dept-budget-vote-202223-24-may-2022-0000

Reva, D. (2020, 28 October). Africa can’t risk a major maritime cyber-attack. *Daily Maverick*. https://www.dailymaverick.co.za/article/2020-10-28-africa-cant-risk-a- major-maritime-cyber-attack/

Reva, D. (2021, 29 July). *Cyber-attacks expose the vulnerability of South African ports.* Institute for Security Studies. https://issafrica.org/iss-today/cyber-attacks-expose- the-vulnerability-of-south-africas-ports

Rhee, H. S., Ryu, Y., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*, 221–232. DOI: 10.1016/j.cose.2011.12.001

Rice, A., & Kitchel, T. (2016). Deconstructing content knowledge: Coping strategies and their underlying influencers for beginning agriculture teachers*. Journal of Agricultural Education*, *57*(3), 208–222. DOI: 10.5032/jae.2016.03208

Rishi, S., Stanley, B., & Gyimesi, K. (2008). *Automotive 2020: Clarity beyond the chaos*. IBM Institute for Business Value, IBM Global Business Services.

Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation*, *35*(1), 22–31.

Rivadeneira Zambrano, F. R., & Rodríguez Rafael, G. D. (2018). Bring your own device (BYOD): A survey of threats and security management models. *International Journal of Electronic Business*, *14*(2), 146–170. DOI: 10.1504/IJEB.2018.10016225

Romaniuk, S. N. (2018). Copenhagen School. In *The SAGE encyclopaedia of surveillance, security and privacy.* Sage Publications. http://dx.doi.org/10.4135/97814833599 22.n95

Roomaney, R., & Coetzee, B. (2018). Introduction to and application of mixed methods research designs. In S. Kramer, S. Laher, A. Fynn, & H. H. Jansen van Vuuren (Eds.), *Online readings in research methods* (Chapter 4). Psychological Society of South Africa. https://www.psyssa.com/wp-content/uploads/2018/10/ORIM-Chapter-4-Introduction-to-and-application-of-mixed-methods-research-designs_by-Roomaney-Coetzee.pdf

Saban, K. A., Rau, S., & Wood, C. A. (2021). SME executives' perceptions and the information security preparedness model. *Information and Computer Security*, *29*(2), 263–282. https://doi.org/10.1108/ICS-01-2020-0014

Salahdine, F., & Kaabouch, N. (2019) Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Sapriel, C. (2021). Managing stakeholder communication during a cyber crisis. *Cyber Security: A Peer-Reviewed Journal*, *4*(4), 380–387.

Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). *Human vulnerabilities in security systems*. Human Factors Working Group, Cyber Security. https://pdfs.semanticscholar.org/38b4/36a07f78056a82df1e9228b87ca145f09f9c.pdf

Savolainen, R. (2017). Information need as trigger and driver of information seeking: A conceptual analysis. *Aslib Journal of Information Management*, *69*(1), 2–21. https://doi.org/10.1108/AJIM-08-2016-0139

Sayler, K. M. (2020). *Artificial intelligence and national security.* Congressional Research Service report. https://sgp.fas.org/crs/natsec/R45178.pdf

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), Article 8. https://doi.org/10.15394/jdfsl.2017.1476

Schneier, B. (2013, March 14). Rhetoric of cyber war breeds fear—and more cyber war. *The Irish Times*. https://www.schneier.com/essays/archives/2013/03/rhetoric_of_cyber_wa.html

Schneier, B. (2015). Data and Goliath: *The hidden battles to collect your data and control your world*. W.W. Norton & Company.

Schneier, B. (2018, November 2). *Schneier on security: How to punish cybercriminals*. https://www.schneier.com/blog/archives/2018/11/ how_to_punish_c.html

Schneier, B. (2019, November 12). *Internet governance: We must bridge the gap between technology and policymaking – Our future depends on it*. World Economic Forum. https://www.weforum.org/agenda/2019/11/we-must-bridge-the-gap-between-technology-and-policy-our-future-depends-on-it/

Schwarz, K. J. (2016). *The securitization of cyberspace through technification* [Unpublished master's thesis]. Virginia Polytechnic Institute and State University.

Shea, J. (2018). Cyberspace as a domain of operations: What is NATO's vision and strategy? *Marine Corps University Journal*, *9*(2), 133–150. https://doi.org/10.21140/mcuj.2018090208

Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, *1*, 81–93. https://doi.org/10.1007/s41111-016-0002-6

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Journal of Education and Information*, *22*, 63–75.

Siart, B., Pflüger, S., & Wallner, B. (2016). Pulling rank: Military rank affects hormone levels and fairness in an allocation experiment. *Frontiers in Psychology*, *7*, 1750. https://doi.org/10.3389/fpsyg.2016.01750

Sigholm, J. (2016). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1), 1–37. https://doi.org/10.1515/jms-2016-0184

Sileyew, K. J. (2019). Research design and methodology. In E. Abu-Taieh, A. E. Mouatasim, & I. H. Al (Eds.), *Cyberspace*. IntechOpen. https://doi.org/10.5772/intechopen.85731

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. Oxford University Press.

Singh, U., & Srivastava, K. B. L. (2016). Organizational trust and organizational citizenship behaviour. *Global Business Review*, *17*(3), 594–609. https://doi.org/10.1177/0972150916630804

Sithole, T. G. (2019). *Assessing cyber resilience of public sector information systems: A South African perspective* [Unpublished master's thesis]. University of Pretoria. http://hdl.handle.net/2263/72687

Sitkin, S. B., & Roth, N. L. (1993). Explaining the limited effectiveness of legalistic "remedies" for trust/distrust. *Organization Science*, *4*, 367–392. https://doi.org/10.1287/orsc.4.3.367

Sjöberg, L., Moen, B., & Rundmo, T. (2004). *Explaining risk perception: An evaluation of the psychometric paradigm in risk perception research*. Norwegian University of Science and Technology, C Rotunde Publikasjoner.

Skagerlund, K., Forsblad, M., Slovic, P., & Västfjäll, D. (2020). The affect heuristic and risk perception – Stability across elicitation methods and individual cognitive abilities. *Frontiers in Psychology*, *11*, 970. https://doi.org/10.3389/fpsyg.2020.00970

Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*, *12*(3), 90–113. https://www.airuniversity.af.edu/

Smith, C. (2021, July 30). Transnet to lift force majeure for port terminals. *News24*. https://www.news24.com/fin24/companies/transnet-to-lift-force-majeure-for-port-terminals-20210730

Smith, C., & Palazzo, A. (2016). *Coming to terms with the modern way of war: Precision missiles and the land component of Australia's joint force*. Australian land warfare concept series (Vol. 1, 2016). https://researchcentre.army.gov.au/sites/default/files/160819_-_concept_-_lw_-_australian_land_warfare_concept_series_1_-_unclas_0.pdf

Soeters, J., & Goldenberg, I. (2019). Information sharing in multinational security and military operations. Why and why not? With whom and with whom not? *Defence Studies*, *19*(1), 37–48. DOI: 10.1080/14702436.2018.1558055

Sohrabi Safa, N., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behaviour*, *57,* 442–451. http://dx.doi.org/10.1016/j.chb.2015.12.037

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, *5*(3), 392–412. https://doi:10.1080/23738871.2020.1820546

Souppaya, M., & Scarfone, K. (2013). *Guide to malware incident prevention and handling for desktops and laptops*. National Institute for Standards and Technology: Special publication, revision 1. http://dx.doi.org/10.6028/NIST.SP.800-83r1

South African Government. (2013, October 15). *Minister inaugurates National Cyber Security Advisory Council*. https://www.gov.za/minister-inaugurates-national-cyber-security-advisory-council

South African National Space Agency (SANSA). (2019). *New SANSA app to improve SANDF secure communications*. https://www.sansa.org.za/2019/08/13/new-sansa-app-to-improve-sandf-secure-communications/

Spencer, L., & Ritchie, J. (2012). In pursuit of quality. In D. Harper, & A. R. Thompson (Eds.), *Qualitative research methods in mental health and psychotherapy: A guide for students and practitioners* (pp. 227–242). Wiley-Blackwell.

Stampnitzky, L., & Mattson, G. (2015). Sociology and security. In F. Bourbeau (Ed.), *Security: Dialogue across disciplines* (Chapter 5). Cambridge University. https://wrdtp.ac.uk/wp-content/uploads/2019/02/Stampnitzky-and-Mattson-Sociologies-in-Insecurity.pdf

Statista. (2022a, July 16). *Global digital population as of April 2022*. https://www.statista.com/statistics/617136/digital-population-worldwide/

Statista. (2022b, July 8). *Share of internet users in Africa as of January 2022, by country*. https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/

Stępka, M. (2022). Securitisation as the work of framing. In *Identifying security logics in the EU policy discourse* (pp. 33–61). IMISCOE research series. Springer. https://doi.org/10.1007/978-3-030-93035-6_3

Stevens, C. (2020). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*, *41*, 129–152. https://doi:10.1080/13523260.2019.1675258

Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge University Press.

Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations*, *13*(3), 357–383. https://doi.org/10.1177/1354066107080128

Šulović, V. (2010). *Meaning of security and the theory of securitization*. Policy Documentation Centre. http://pdc.ceu.hu/archive/00006385/

Sutherland, E. (2017). Governance of cybersecurity – The case of South Africa. *The African Journal of Information and Communication*, *20*, 83–112. https://doi.org/10.23962/10539/23574

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226–231. https://doi.org/10.4212/cjhp.v68i3.1456

Sverdlov, L. (2020, February 13). Israeli cyber-company uncovers Hamas campaign against PA. *The Jerusalem Post*. https://www.jpost.com/arab-israeli-conflict/gaza-news/israeli-cyber-company-uncovers-hamas-campaign-against-pa-617421

Swedberg, R. (2018). On the uses of exploratory research and exploratory studies in social science. In C. Elman, J. Gerring, & J. Mahoney (Eds.), *The production of knowledge*: *Enhancing progress in social science* (pp. 17–41). Cambridge University Press.

Taha, N., & Dahabiyeh, L. (2020). College students' information security awareness: A comparison between smartphones and computers. *Education and Information Technologies*, *26*, 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches*. Sage Publications.

Tashakkori, A., & Teddlie, C. (2008). Introduction to mixed method and mixed model studies in the social and behavioural science. In V. L. Plano Clark, & J. W. Creswell (Eds.), *The mixed methods reader* (pp. 7–26). Sage Publications.

Techopedia. (2017, January 19). *Open-source tools: What does open-source tools mean?* https://www.techopedia.com/definition/3295/open-source-tools

Techopedia. (2019, February 5). *Cyberattack: What does it mean?* https://www.techopedia.com/definition/24748/cyberattack

Techopedia. (2022, April 25). *Cyberthreat: What does cyberthreat mean?* https://www.techopedia.com/definition/25263/cyberthreat

Teddlie, C., & Tashakkori, A. (2008). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioural sciences*. Sage Publications.

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2*, 5–8. https://doi.org/10.1016/S1353-4858(12)70013-2

Tkachuk, N. (2018). Countering cyber threats to national security: Ukraine defends its cyber infrastructure in the face of attacks from Russia. *Per Concordiam*, *2*, 44–47.

Tobin, G. A., & Begley, C. M. (2004). Methodological rigour within a qualitative framework. *Journal of Advanced Nursing*, *48*, 388–396. http://dx.doi.org/10.1111/j.1365-2648.2004.03207.x

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys*, *51*(2), 1–27. http://doi.acm.org/10.1145/3172869

Toyana, M. (2021, July 27). Transnet ports division declares force majeure on container terminals after cyberattack. *Daily Maverick*. https://www.dailymaverick.co.za/article/2021-07-27-transnet-ports-division-declares-force-majeure-on-container-terminals-after-cyber-attack/

Trim, P. R., & Lee, Y. I. (2021). The global cyber security model: Counteracting cyber attacks through a resilient partnership arrangement. *Big Data & Cognitive Computing*, *5*(3), 32. https://doi.org/10.3390/bdcc5030032

Tsagourias, N., & Buchan, R. J. (2018). Automatic cyber defence and the laws of war. *German Yearbook of International Law*, 60, 203–237.

Tsfati, Y., & Cohen, J. (2013). Perceptions of media and media effects: The third person effect, trust in media and hostile media perceptions. In E. Scharrer (Ed.), *Blackwell's international companion to media studies: Media effects/media psychology* (pp. 128–146). Wiley-Blackwell.

Tshwane, T. (2020, March 23). SANDF on standby to assist in Covid-19 mitigation efforts. *Moneyweb*. https://www.moneyweb.co.za/news/south-africa/sandf-on-standby-to-assist-in-covid-19-mitigation-efforts/

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computer and Security Journal*, *109*(C), 102387. https://doi.org/10.1016/j.cose.2021.102387

United Nations (UN). (2018, February 18). *From nuclear threat to cyberwar, unity must prevail over division in tackling global challenges, Secretary-General tells Security Forum* [Press release]. https://www.un.org/press/en/2018/sgsm18900.doc.htm

United States Army Joint Chiefs of Staff. (2018). *Joint publication on cyber operations*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Uslaner, E. M. (2002). *The moral foundations of trust*. Cambridge University Press.

Van den Berg, B., & Keymolen, E. (2017). Regulating security on the Internet: Control versus trust. *International Review of Law, Computers & Technology*, *31*(2), 188–205. DOI: 10.1080/13600869.2017.1298504

Van der Waag-Cowling, N. (2013). *A study of research in the Faculty of Military Science* [Unpublished master's thesis]. Stellenbosch University.

Van der Waag-Cowling, N. (2017). South Africa and the cyber warfare threat: A strategic overview. In *Civil-military cooperation and international collaboration in cyber operations*. Institute for Leadership and Strategic Studies: Symposium monograph series. University of North Georgia Press. https://web.ung.edu/media/university-press/ILSS%20Monograph%202017.pdf

Van Heerden, R., Von Solms, S., & Mooi, R. (2016). Classification of cyber attacks in South Africa. In Institute of Electrical and Electronics Engineers (IEEE) (Ed.), *IST-Africa Week Conference* (pp. 1–16). IEEE. https://doi.org/10.1109/ISTAFRICA.2016.7530663

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Van Niekerk, B., & Maharaj, M. (2013). Social media and information conflict. *International Journal of Communication*, *7*, 1162–1184.

Van Ooijen, M. (2020). *Cyber securitization or cyberization of conflict? On the militarization of cyber security in Estonia* [Unpublished master's thesis]. Utrecht University.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L. Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *57*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Van Vuuren, R. (2018). Information warfare as future weapon of mass disruption. *Journal of Futures Studies*, *23*(1), 77–94. https://www.airitilibrary.com/Publication/alDetailedMesh?docid=10276084-201809-201811150002-201811150002-77-94

Van't Wout, C. (2019, February 28–March 1). *Develop and maintain a cybersecurity organisational culture* [Conference presentation]. Fourteenth International Conference on Cyber Warfare and Security, Stellenbosch, South Africa. http://hdl.handle.net/10204/11345

Veerasamy, N. (2021, February 25–26). *Cyber threats focusing on Covid-19 outbreak* [Conference presentation]. International Conference on Cyber Warfare and Security, Tennessee, USA. http://hdl.handle.net/10204/11926

Veerasamy, N., Mashiane, T., & Pillay, K. (2019, February 28–March 1). *Contextualising cybersecurity readiness in South Africa* [Conference presentation]. Fourteenth International Conference on Cyber Warfare and Security, Stellenbosch, South Africa. http://hdl.handle.net/10204/11247

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-device risk management model: A case study from a South African organisation. *The Electronic Journal of Information Systems Evaluation*, *22*(1), 1–14.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, A. M. (2019). Cyber security education is as essential as "the three R's". *Heliyon*, *5*(12), e02855, https://doi:10.1016/j.heliyon.2019.e02855

Verizon. (2018, July 20). Data breach report: Studies in cyber crime. *Data Breach Digest*. https://www.verizon.com/business/resources/reports/2018-data-breach-digest.pdf

Vermeulen, J. (2016, February 12). Anonymous hacks SA government database. *MyBroadband*. https://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html

Vermooten, N. (2018). *Variance in employee engagement among public school teachers in the Western Cape province: An exploratory study* [Unpublished doctoral dissertation]. Stellenbosch University.

Vourvachis, P., & Woodward, T. (2015). *Content analysis in social and environmental reporting research: Trends and challenges (Version 1)*. Loughborough University. https://hdl.handle.net/2134/19623

Vreÿ, F., & Solomon, H. (2020). *COVID-19 as a security threat: Some initial perspectives*. Research brief. Security Institute for Governance and Leadership in Africa. https://www.ufs.ac.za/docs/default-source/coronavirus-covid-19-sars-cov-2/brief-7-covid19.pdf?sfvrsn=a0979721_2

Wæver, O. (1995). Securitization and desecuritization. In R. Lipschutz (Ed.), *On security* (pp. 48–86). Columbia University Press.

Wæver, O. (1998). Insecurity, security, and asecurity in the West European non-war community. In E. Adler, & M. Barnett (Eds.), *Security communities* (pp. 69–118). Cambridge University Press.

Wæver, O., Lemaitre, P., & Tromer, E. (Eds.). (1989). *European polyphony: Beyond East-West confrontation*. MacMillan.

Walaza, M., Loock, M., & Kritzinger. E. (2019, December 2–5). The South African ICT security awareness framework for education. In *Innovative Technologies and Learning: Proceedings of Second International Conference* (pp. 330–339). Springer-Verlag. https://doi.org/10.1007/978-3-030-35343-8_35

Walters, P. (2012). *The risks of using portable devices.* United States Department of Homeland Security. https://www.cisa.gov/uscert/sites/default/files/publications/RisksOfPortableDevices.pdf

Watson, S. (2011). The “human” as referent object? Humanitarianism as securitization. *Security Dialogue*, *42*(1), 3–20. https://doi.org/10.1177/0967010610393549

Watt, D. (2007). On becoming a qualitative researcher: The value of reflexivity. *The Qualitative Report*, *12*(1), 82–101. http://www.nova.edu/ssss/QR/QR12-1/watt.pdf

Weber, R. P. (1990). *Basic content analysis* (2nd ed.). Sage Publications.

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict & Terrorism*, *28*, 129–149. DOI: 10.1080/10576100590905110

Weiner, M. R., Monin, J. K., Mota, N., & Pietrzak, R. H. (2016). Age differences in the association of social support and mental health in male U.S. veterans: Results from the national health and resilience in veterans study. *American Journal of Geriatric Psychiatry*, *24*(4), 327–336. https://doi.org/10.1016/j.jagp.2015.11.007

Welch, C. (2011, November 16). Cyberspace attacks could provoke military response, says Defense Department. *The Verge*. https://www.theverge.com/2011/11/16/2566450/us-dod-cyberspace-attacks-risk-military-response

Whitney, L. (2021, October 13). Dark web: Many cybercrime services sell for less than $500. *Tech Republic*. https://www.techrepublic.com/article/dark-web-many-cybercrime- services-sell-for-less-than-500/

Williams, M. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly*, *47*(4), 511–531.

Williams, M. C. (2007). *Culture and security: Symbolic power and the politics of international security*. Routledge.

Wilson, C. (2015). Cybersecurity in the 21st century: Applying cyber threat intelligence. *Journal of the Colloquium for Information Systems Security Education*, *3*(1), 1–19. https://cisse.info/journal/index.php/cisse/article/view/32

Winkler, I. (2017, June 22). Back to basics: 7 elements of a successful security awareness program. *CSO Online*. https://www.csoonline.com/article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html

Wirtz, J. (2017). Life in the “gray zone”: Observations for contemporary strategists. *Defense & Security Analysis*, *33*(2), 106–114. https://doi.org/10.1080/14751798.2017.1310702

Yeboah-Boateng, E. O., & Boaten, F. E. (2016). Bring-your-own-device: An evaluation of associated risks to corporate information security. *International Journal of Information Technology & Engineering*, *4*(8), 12–30. https://arxiv.org/abs/1609.01821

Zangirolami-Raimundo, J., Echeimberg, J.O., & Leone, C. (2018). Research methodology topics: Cross-sectional studies. *Journal of Human Growth and Development*, *28*(3), 356–360. http://dx.doi.org/10.7322/jhgd.152198

Zhang, Y., & Wildemuth, B. M. (2005). Qualitative analysis of content. *Human Brain Mapping*, *30*(7), 2197–2206.

Zheng, D. E., & Lewis, J. A. (2015). *Cyber threat information sharing: Recommendations for congress and the administration*. Report Centre for Strategic and International Studies: Strategic Technologies Programme.

Zheng, W. (2009). The knowledge-inducing culture: An integrative framework of cultural enablers of knowledge management. *Journal of Information and Knowledge Management*, *8*(3), 213–227.

Zukic, A. (2020). *Assessing the role of the military in national cybersecurity efforts* [Unpublished master's thesis]. U.S. Army Command and General Staff College.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior*:* A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.

Zygmont, C. S. (2014). *A phenomenographical study of the qualitative variation of adventure wilderness programme experiences among adolescent high school participants in the Western Cape* [Unpublished doctoral dissertation]. Stellenbosch University.

APPENDICES

APPENDIX A: INFORMATION SHEET FOR SEMI-STRUCTURED INTERVIEWS

UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvennoot • your knowledge partner

Who am I? Hello, I am Kyle Bester from the University of Stellenbosch.

What am I doing? I am conducting research at the Faculty of Military Science to explore cybersecurity in the organisation, with a particular focus on exploring the views and perceptions of members. In order to continue with the research, we need your inputs so that we may improve our knowledge base of cybersecurity. It is hoped that this research may be published by dissertation in order to extend our knowledge base on cybersecurity.

Your participation: I will ask you to participate in an interview, which will not be more than 60 minutes. When participating in the interview, it would be appreciated if you could be honest and elaborate as far as possible. This interview is however not compulsory and will not affect you in any manner. It is entirely up to you how many questions you answer, but it would be appreciated if you did attempt to answer most of it. If you feel that you do not want to participate in this interview, it is your right and you will not be disadvantaged in any manner.

Please understand that your participation is entirely voluntary. You alone decide whether or not you want to take part. If you choose not to take part, you will not be affected in any way whatsoever. If you agree to take part, you may refuse to answer any question or stop at any time. If you do this there will also be no penalties and you will not be prejudiced in any way. If you agree to participate, we ask you to answer to the best of your ability and encourage you to answer as many questions as you feel comfortable with.

Confidentiality: On the interview schedule, it requires you to complete your age, race, gender and region. This information is only used to explain the sample for research purposes and there is no need for any identifying information, such as names or ID numbers/force numbers. This information will only be observed by the principal researcher and only he will have access to the data. You can be assured that you as an individual will not be linked to any publication or analysed information. Your information will therefore always remain confidential. All identifying information such as the audio recordings and consent forms will be kept in a locked filing facility and access to this is restricted, thus it will not be made available to others. These details will be destroyed once the project has been completed.

Risks/discomforts: There are no risks when participating in the interview and the questions in the interview are all related to exploring cybersecurity.

Benefits: There are no immediate benefits to you from taking part in this study. However, this study will be helpful in assisting the SANDF in the understanding of cybersecurity from the views of members employed in the organisation. Focusing on participant views and perception will allow one to see how security is framed, prioritised and understood. Furthermore, by exploring the views and perceptions of participants', this study will also ascertain what the political and social implications are for cybersecurity from the views of members. Note, participation is out of free will and without payment. Your participation is important and we thank you for this. In order to comply with the ethical requirements of the study, I will ensure that I receive a signed and dated copy of the Participant Information Leaflet and Informed Consent form.

If you have any concerns: If you have any questions or concerns about the research or participating in this study, please feel free to contact the researcher Kyle Bester (+27 76 737 6654; 19079346@sun.ac.za) and/or his supervisor, Dr Michelle Nel (+27 22 702 3131; nel@ma2.sun.ac.za).

APPENDIX B: CONSENT TO PARTICIPATE IN RESEARCH INTERVIEW

UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvennoot • your knowledge partner

TITLE: Perceptions on cybersecurity among South African military officers

You are asked to take participate in a research study conducted by Mr Kyle John Bester, from Faculty of Military Sciences at Stellenbosch University. The results obtained will contribute to the completion of a doctoral degree in Industrial Psychology. You were selected as a possible participant in this study because you are a South African National Defence Force officer.

PURPOSE OF THE STUDY

The main purpose for undertaking this study is due to the . significant gap which exists with regard to knowledge production on the perceptions of cybersecurity among South African military officers. More specifically, the study focuses on the human element within the emerging field of inquiry namely cybersecurity. Expanding on this, the proposed study also seeks to explore how cybersecurity measures are able to deal with cyberthreats that have increased due to the increased digitalisation and interconnectedness of actors. The researcher therefore seeks to explore the views of South African military officers on cybersecurity. The proposed outcome of the study is to understand the nature of cybersecurity within the South African National Defence Force by gauging the views of officers.

WHAT WILL BE ASKED OF ME?

If you volunteer to participate in this study, you would be required to do the following:

INTERVIEW

You will be asked to voluntarily participate in an interview to explore your views and perceptions on cybersecurity within the military. You will be required to answer questions related to cybersecurity posture; views on security; security orientation and cybersecurity in the organisation. You will be requested to answer all questions. However, if you do not want to answer a question it is in your right to do so. Note that there are no right or wrong responses; we are merely interested in your personal views and perceptions on cybersecurity. Your responses will remain anonymous and your confidentiality will be protected. You will require approximately 60 minutes when participating in the interview.

POSSIBLE RISKS AND DISCOMFORTS

There are no potential risks envisaged in this study. The interview will also require approximately 60 minutes of your time.

POSSIBLE BENEFITS TO PARTICIPANTS AND/OR TO THE SOCIETY

Participation in the research study will provide you with an opportunity to reflect on the factors (i.e., information-sharing culture, security orientation; view on cybersecurity and cybersecurity posture) that may play a role in how your views and perception on cybersecurity can have an impact on the organization

PAYMENT FOR PARTICIPATION

No payment will be made to participants for partaking in this study.

PROTECTION OF YOUR INFORMATION, CONFIDENTIALITY AND IDENTITY

Any information you share with me during this study and that could possibly identify you as a participant will be protected. This will be done by providing you with a pseudonym or unique number which will only be known by the principle researcher. Only the researcher will have access to the information you shared during the data-collection process. Furthermore, your information will be stored in a safe location, which will only be known by the researcher. After the research study has been completed the data will be deleted.

During the interview process your information will be audio-recorded. As a voluntary participant you have the opportunity to refuse to be recorded. Furthermore, as a participant you will also have an opportunity to review and edit the information recorded. Only the principle researcher Mr Kyle Bester will have access to these recordings. These audio- recordings will be used for educational purposes and will be erased once the research study has been completed. The results of this study will be published in the form of a completed dissertation, but confidentiality will be maintained. No names or identifying information will be published.

PARTICIPATION AND WITHDRAWAL

You can choose whether to be in this study or not. If you volunteer to be in this study, you may withdraw at any time without consequences of any kind. You may refuse to answer any question and still remain in the study. The investigator may withdraw you from this research if circumstances arise which warrant doing so.

RESEARCHER'S CONTACT INFORMATION

If you have any questions or concerns about the research or participating in this study, please feel free to contact the researcher Kyle Bester (+27 76 737 6654; 19079346@sun.ac.za) and/or his supervisor, Dr Michelle Nel (+27 22 702 3131; nel@ma2.sun.ac.za).

RIGHTS OF RESEARCH PARTICIPANTS

You may withdraw your consent at any time and discontinue participation without penalty. You are not waiving any legal claims, rights or remedies because of your participation in this research study. If you have questions regarding your rights as a research participant, contact Ms Maléne Fouché [mfouche@sun.ac.za; 021 808 4622] at the Division for Research Development.

APPENDIX C: CONSENT TO PARTICIPATE IN CYBERSECURITY ORIENTATION QUESTIONNAIRE

UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvennoot • your knowledge partner

TITLE: Perceptions on cybersecurity among South African military officers

You are asked to take participate in a research study conducted by Mr Kyle John Bester, from Faculty of Military Sciences at Stellenbosch University. The results obtained will contribute to the completion of a doctoral degree in Industrial Psychology. You were selected as a possible participant in this study because you are a South African National Defence Force officer.

PURPOSE OF THE STUDY

The main purpose for undertaking this study is due to the due to the significant gap which exists with regard to knowledge production on the perceptions of cybersecurity among South African military officers. More specifically, the study focuses on the human element within the emerging field of inquiry namely cybersecurity. Expanding on this, the proposed study also seeks to explore how cybersecurity measures are able to deal with cyberthreats that have increased due to the increased digitalisation and interconnectedness of actors. The researcher therefore seeks to explore the views of South African military officers on cybersecurity. The proposed outcome of the study is to understand the nature of cybersecurity within the South African National Defence Force by gauging the views of officers.

WHAT WILL BE ASKED OF ME?

If you volunteer to participate in this study, you would be required to do the following:

QUESTIONNAIRE

You will be asked to complete a questionnaire to explore your views and perceptions on cybersecurity within the defence force. You will be required to rate each question on a Likert scale ranging from 1 to 5. There are no right or wrong responses; we are merely interested in your personal opinions. Your responses will remain anonymous and your confidentiality will be protected. You will require approximately 15-20 minutes when completing this questionnaire.

POSSIBLE RISKS AND DISCOMFORTS

There are no potential risks envisaged in this study. The questionnaire will also require approximately 20 minutes of your time to complete.

POSSIBLE BENEFITS TO PARTICIPANTS AND/OR TO THE SOCIETY

Participation in the research study will provide you with an opportunity to reflect on the factors (i.e., information-sharing culture, security orientation; view on cybersecurity and cybersecurity posture) that may play a role in how your views and perception on cybersecurity can have an impact on the organization

PAYMENT FOR PARTICIPATION

No payment will be made to participants for partaking in this study.

PROTECTION OF YOUR INFORMATION, CONFIDENTIALITY AND IDENTITY

Any information you share with me during this study and that could possibly identify you as a participant will be protected. This will be done by providing you with a pseudonym or unique number which will only be known by the principle researcher. Only the principle researcher Mr Kyle Bester will have access to the information you shared during the data-collection process. Furthermore, your information will be stored in a safe location, which will only be known by the researcher. After the research study has been completed the data will be deleted. The results of this study will be published in the form of a completed dissertation, but confidentiality will be maintained. No names or identifying information will be published.

PARTICIPATION AND WITHDRAWAL

You can choose whether to be in this study or not. If you volunteer to be in this study, you may withdraw at any time without consequences of any kind. You may refuse to answer any question and still remain in the study. The investigator may withdraw you from this research if circumstances arise which warrant doing so.

RESEARCHER’S CONTACT INFORMATION

If you have any questions or concerns about the research or participating in this study, please feel free to contact the researcher Kyle Bester (+27 76 737 6654; 19079346@sun.ac.za) and/or his supervisor, Dr Michelle Nel (+27 22 702 3131; nel@ma2.sun.ac.za).

RIGHTS OF RESEARCH PARTICIPANTS

You may withdraw your consent at any time and discontinue participation without penalty. You are not waiving any legal claims, rights or remedies because of your participation in this research study. If you have questions regarding your rights as a research participant, contact Ms Maléne Fouché [mfouche@sun.ac.za; 021 808 4622] at the Division for Research Development.

APPENDIX D: SEMI-STRUCTURED INTERVIEW GUIDE

UNIVERSITEIT·STELLENBOSCH·UNIVERSITY
jou kennisvennoot • your knowledge partner

Biographical Information:

Age:

Race:

Gender:

Region:

Questions: Information-sharing culture:

- In your opinion, what information would you brand as sensitive?
- What is the best way in your view on how to protect such information?
- In your opinion, do you feel that information shared at work merits the classification of being sensitive?
- How do you feel about government information being saved on a personal data-storage device?
- Do you consider the use of a personal data-storage device such as USB / hard drive crucial to your everyday work activity?
- What other electronic devices are you using to store your information?
- What in your opinion is the best way to store such sensitive information?
- How often would you make use of public/open access Wi-Fi with your personal or work computer?
- Do you feel secured when accessing those networks?
- In your opinion, if you could rank your information from low importance to a higher level of importance, which would you classify as crucial to you?
- What is your opinion on sharing information on work activity (Posting pictures with their uniform revealing rank; or posting information that links to their duties at work)?

- Have you ever encountered an information-sharing policy within the organisation?
- In your opinion should the organisation adopt a stricter policy on information sharing?

Questions: Security orientation

- Are you a security conscious individual? Explain.
- What are your views on information security within the organisation?
- How do you secure information at your organisation?
- What does the term “security” mean for you?
- In your opinion is there a culture of cybersecurity within the organisation?
- How would you describe this culture of cybersecurity within the organisation?
- How often do you share organizational information with colleagues?
- What is your opinion on sensitive information that is being shared with colleagues’?
- Are you aware of technology that may be prone to hacking in your workplace?
- What is your perception on browsing websites that are unprotected on your work devices?
- What are your thoughts on downloading documents from the Internet on your work device?
- How do you feel about state documents that contain sensitive information being taken home on personal devices?
- How do you assess your cybersafety?
- Do you have software that can be used to safeguard against cyberthreats?

Questions: View on cybersecurity

- What is your view on cybersecurity?
- What is cyberspace/Internet in your opinion?
- What does this mean for you?

- What are your views on cyberthreats?
- What cyberattacks are you aware of?
- What is your understanding on cyberthreats/attacks?
- What are your thoughts on equipping all military officers with the technical skills to combat cyberthreats?
- Given the importance of cyberthreats pose, why do you think there is a lack of awareness of cyber-related issues in the organisation?
- How would you describe the nature of communication on cybersecurity that is taking place in the organization?
- In your opinion, should there be collaboration between cyber commands and units?
- Do you feel that the guidelines concerning cybersecurity currently under review are limiting your work?
- Do you consider this a space that needs to be controlled by the armed forces or other state-affiliated actors?
- How would you approach this domain of warfare?
- Do you feel that cyber space should be monitored at work?
- How would you regulate the use of the Internet at work?
- What is your opinion on national security and how would cyberattacks compromise it?
- Do you feel that members of the organisation should be informed about these threats and attacks?
- Do you feel that there should be more awareness regarding cybersecurity?
- In your opinion what tools can be used in the organisation to increase cyber awareness?
- What are your perspectives on cyber-related issues and its impact on the organisation?

Questions: Cybersecurity posture in the organisation

- What are your perceptions regarding the Internet?
- Do you feel that being cyber conscious will have an impact on your interaction with colleagues and peers?
- How would you describe your posture in cyberspace?
- What are your feelings towards online behaviour?
- Does this have an effect on how you interact with others at your workplace?
- In your view what is the ideal way to manage cybersecurity in the workplace?
- What information in your opinion is acceptable to be shared in the workplace?
- How would you describe your online behaviour when navigating the intranet?
- Is this behaviour or cyber posture similar to how you would navigate the Internet in your personal capacity via your personal devices?
- What is your view on using open-source tools/software in the military context?
- What is your view on new technologies being introduced in the organisation that may have potential risks?
- Are you aware of any units that are using open-source software to manage sensitive information?
- How do you feel about this?
- What in your opinion is the idea way to manage sensitive information in the workplace?
- In your opinion, how would you regulate and monitor others' Internet and intranet usage?
- In your view, should there be more education regarding Internet usage and behaviour?
- What in your opinion should be added to a cyber-related education programme for military officers?
- Do you feel that the organisation should support for active monitoring of governmental devices?
- What is your view on the information security team in your organisation?

End, Thank You

APPENDIX E: THE CYBERSECURITY ORIENTATION QUESTIONNAIRE

UNIVERSITEIT·STELLENBOSCH·UNIVERSITY
jou kennisvennoot • your knowledge partner

INSTRUCTIONS:

1. The following statements are about cybersecurity within the organisation.
2. Please read each statement carefully and indicate your answer by making a cross in the relevant block of how much you agree or disagree with the statement.

   For example: I share information easily with people.

Strongly Agree	**[✓ Agree]**	**Disagree**	**Strongly Disagree**

3. There is no right or wrong answer.
4. Please give your honest response for all the items.
5. Please answer ALL the questions.
6. Please ONLY mark ONE option for the different answer options given.

SECTION A: BIOGRAPHICAL INFORMATION:

Nationality:

South African	**Other**

Age: __________

Race:

White	African	Coloured	Indian	Other

Gender:

Male	**Female**

Province:

Eastern Cape	
Northern Cape	
Gauteng	
North West	
Free State	
Western Cape	
Mpumalanga	
Limpopo	
KwaZulu-Natal	

What Arm of Service are you from:

SAAF	**NAVY**	**ARMY**	**SAMHS**

How many years are you in the SANDF: ____________________________

What is your current rank in the SANDF: ____________________________

SECTION 1: INFORMATION-SHARING CULTURE

1. **Read** all the questions clearly and take note of **ALL** the **answer options given (Strongly Disagree, Disagree, Agree, and Strongly Agree).**
2. You may **NOT** mark more than one **OPTION.**

No.	Statements	Strongly Disagree	Disagree	Agree	Strongly Agree
1	I feel that it is safe to share information on social media.				
2	I feel that my personal information is important.				
3	I feel passwords are enough to protect my personal information stored on my work computer/laptop.				
4	I feel that using a storage device (USB) is the best way to store information.				
5	I change my passwords on my laptops, cellphone and computer on a regular basis.				
6	I feel safe using free Wi-Fi from public places.				
7	I sometimes connect my cellphone or laptop to a public Wi-Fi connection.				
8	I feel comfortable posting about my personal life on social media.				
9	I feel comfortable posting information about my work place activities on social media.				
10	I feel that my work should have more cybersecurity awareness campaigns.				
11	I have read about an information-sharing policy at my work place.				
12	I feel that my work place should implement an information- sharing policy.				
13	I am aware of guidelines at my work place promoting cybersafety.				

SHORT QUESTIONS

1. Read ALL the questions clearly and PLEASE provide honest answers for ALL the questions.

No.	Short Opinion Questions	Answers
14	What would you consider to be sensitive information?	
15	How would you describe the culture of cybersecurity within your work place?	
16	Do you share work information with colleagues on a regular basis? And why?	
17	How do you feel about sharing sensitive information with your colleagues?	

SECTION 2: SECURITY ORIENTATION

1. **Read** all the questions clearly and take note of **ALL** the **answer options given (Strongly Disagree, Disagree, Agree, and Strongly Agree).**
2. You may **NOT** mark more than one **OPTION.**

No.	Statements	Strongly Disagree	Disagree	Agree	Strongly Agree
18	When I use the Internet, I am aware of the dangers of cyberthreats/attacks.				
19	I feel that information security is important in my work place.				
20	When I feel unsafe using the Internet, I decide to log out.				
21	I sometimes save my personal information on my work laptop or computer.				
22	I know of technology that can be used to hack computers in my work place.				
23	I update myself with cybersecurity issues.				
24	I sometimes try to include cybersafety guidelines in my work place.				
25	I know of colleagues that have had their personal or work laptops/computers hacked.				

SHORT QUESTIONS

1. Read ALL the questions clearly and PLEASE provide honest answers for ALL the questions.

No.	Short Opinion Questions	Answers
26	What do you think of cybersecurity?	
27	How would you describe your behaviour on the Internet?	
28	How do you feel about your behaviour when using Internet websites?	

SECTION 3: VIEWS ON CYBERSECURITY

1. **Read** all the questions clearly and take note of **ALL** the **answer options given (Strongly Disagree, Disagree, Agree, and Strongly Agree).**
2. You may **NOT** mark more than one **OPTION.**

No.	Statements	Strongly Disagree	Disagree	Agree	Strongly Agree
29	I feel that the Internet is safe to use.				
30	I am aware of the cyberthreats that are affecting the work place.				
31	I am aware of cyberattacks that has happened in my work place.				
32	I feel that all my work colleagues should learn the skills that can help them fight cyberthreats at work.				
33	I feel that the cybersecurity guidelines at my organisation will not limit the duties and tasks of military officers.				
34	I feel that there is a need for the military to control cyberspace.				
35	I feel that all Internet activity at my work place should be monitored to prevent cyberthreats.				
36	I feel that monitoring the Internet at my work will change the way how people think of cybersecurity.				
37	I feel that all my colleagues are informed of cyberthreats or attacks at our work place.				
38	I feel that the organisation pays attention to cyberthreats and attacks in the country.				
39	I feel that cyberspace is a new space to carry out warfare.				
40	I feel that my work colleagues are aware of the cybersecurity guidelines at our work place.				
41	I am aware of my colleagues that are knowledgeable about cybersecurity.				
42	I am aware of the consequences of cyberthreats for the organisation and the country.				
43	I feel that cyberthreats cannot harm the work place.				
44	I feel that all officers in my work place should be aware of the effects of cyberthreats.				

SECTION 4: CYBERSECURITY POSTURE IN THE ORGANISATION

1. **Read** all the questions clearly and take note of **ALL** the **answer options given (Strongly Disagree, Disagree, Agree, and Strongly Agree).**
2. You may **NOT** mark more than one **OPTION.**

No.	Statements	Strongly Disagree	Disagree	Agree	Strongly Agree
45	I feel that I behave the same on the Internet when I am at home or at work.				
46	I feel that knowing about cyberthreats may change how I communicate with others.				
47	I feel that using free software to fight cyberthreats and attacks at my work place is unsafe.				
48	I feel that my work place should develop their own software to fight cyberthreats and attacks.				
49	I feel that a cyber education programme for all members will increase cybersecurity at my work place.				
50	I feel that education and training will help to change the security behaviour of members at my work place.				
51	I feel that cyber-related education should be included in some of the work training programmes.				

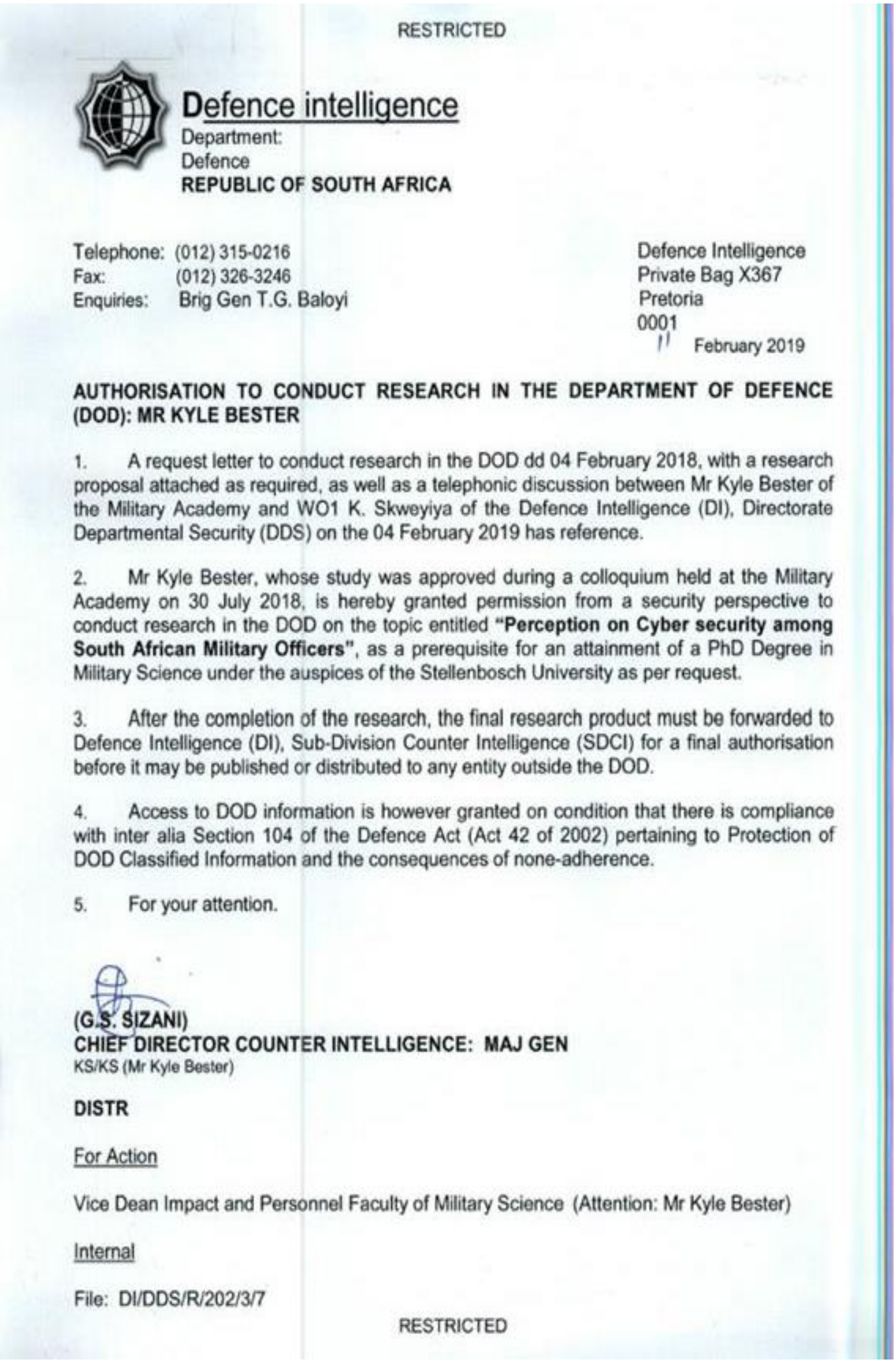
SHORT QUESTIONS

1. Read **ALL** the questions clearly and **PLEASE** provide honest answers to **ALL** the questions.

No.	Short Opinion Questions	Answers
52	Does cybersecurity affect how you interact with others at your workplace?	
53	What do you feel is the best way to manage cybersecurity in your work place?	

THANK YOU FOR PARTICIPATING IN THIS STUDY!!

APPENDIX F: DEFENCE INTELLIGENCE CLEARANCE



RESTRICTED

Defence intelligence
Department:
Defence
REPUBLIC OF SOUTH AFRICA

Telephone: (012) 315-0216
Fax: (012) 326-3246
Enquiries: Brig Gen T.G. Baloyi

Defence Intelligence
Private Bag X367
Pretoria
0001
11 February 2019

AUTHORISATION TO CONDUCT RESEARCH IN THE DEPARTMENT OF DEFENCE (DOD): MR KYLE BESTER

1. A request letter to conduct research in the DOD dd 04 February 2018, with a research proposal attached as required, as well as a telephonic discussion between Mr Kyle Bester of the Military Academy and WO1 K. Skweyiya of the Defence Intelligence (DI), Directorate Departmental Security (DDS) on the 04 February 2019 has reference.

2. Mr Kyle Bester, whose study was approved during a colloquium held at the Military Academy on 30 July 2018, is hereby granted permission from a security perspective to conduct research in the DOD on the topic entitled **"Perception on Cyber security among South African Military Officers"**, as a prerequisite for an attainment of a PhD Degree in Military Science under the auspices of the Stellenbosch University as per request.

3. After the completion of the research, the final research product must be forwarded to Defence Intelligence (DI), Sub-Division Counter Intelligence (SDCI) for a final authorisation before it may be published or distributed to any entity outside the DOD.

4. Access to DOD information is however granted on condition that there is compliance with inter alia Section 104 of the Defence Act (Act 42 of 2002) pertaining to Protection of DOD Classified Information and the consequences of none-adherence.

5. For your attention.

(G.S. SIZANI)
CHIEF DIRECTOR COUNTER INTELLIGENCE: MAJ GEN
KS/KS (Mr Kyle Bester)

DISTR

For Action

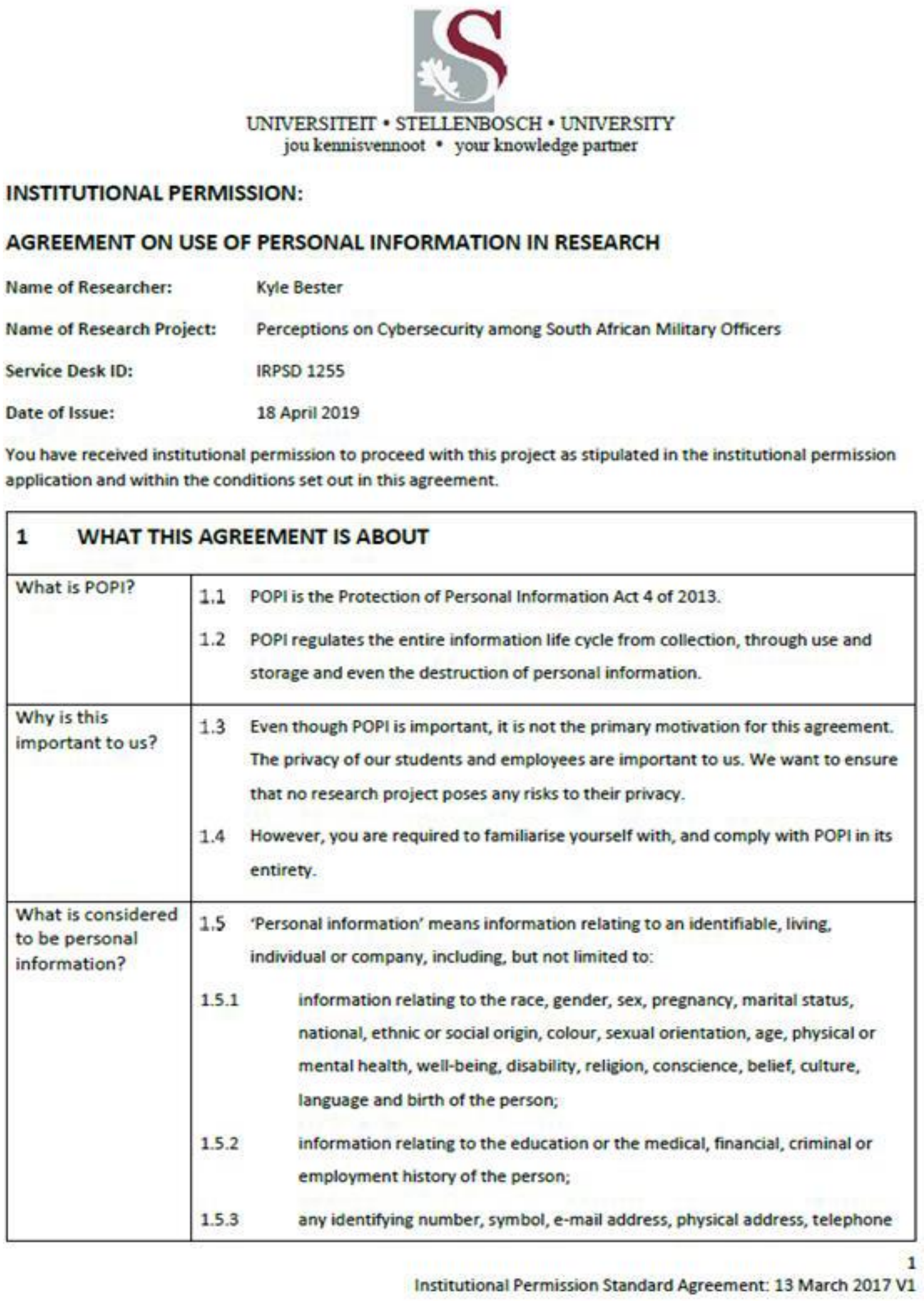
Vice Dean Impact and Personnel Faculty of Military Science (Attention: Mr Kyle Bester)

Internal

File: DI/DDS/R/202/3/7

RESTRICTED

APPENDIX G: INSTITUTIONAL PERMISSION



UNIVERSITEIT • STELLENBOSCH • UNIVERSITY
jou kennisvennoot • your knowledge partner

INSTITUTIONAL PERMISSION:

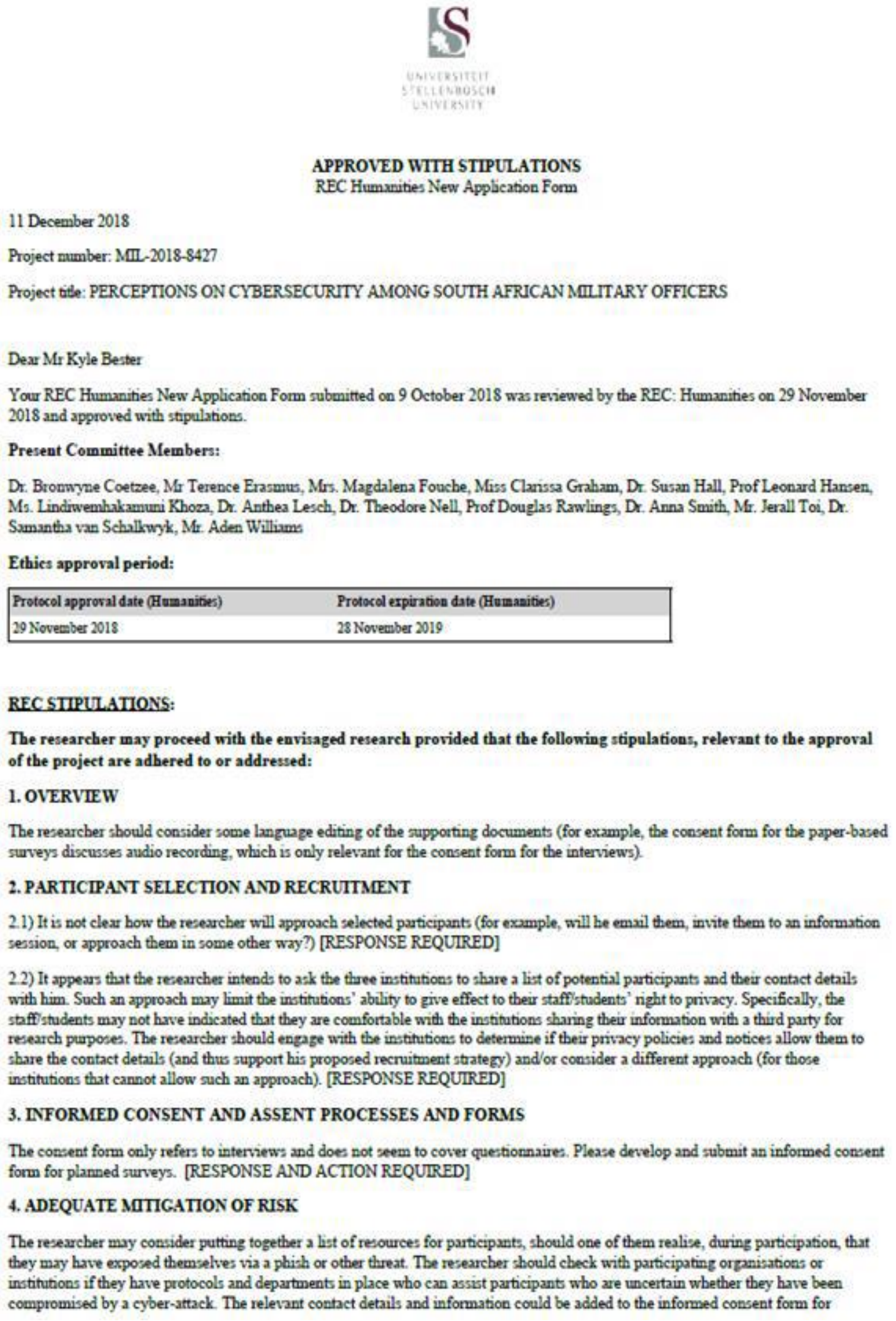
AGREEMENT ON USE OF PERSONAL INFORMATION IN RESEARCH

Name of Researcher:	Kyle Bester
Name of Research Project:	Perceptions on Cybersecurity among South African Military Officers
Service Desk ID:	IRPSD 1255
Date of Issue:	18 April 2019

You have received institutional permission to proceed with this project as stipulated in the institutional permission application and within the conditions set out in this agreement.

1 WHAT THIS AGREEMENT IS ABOUT	
What is POPI?	1.1 POPI is the Protection of Personal Information Act 4 of 2013. 1.2 POPI regulates the entire information life cycle from collection, through use and storage and even the destruction of personal information.
Why is this important to us?	1.3 Even though POPI is important, it is not the primary motivation for this agreement. The privacy of our students and employees are important to us. We want to ensure that no research project poses any risks to their privacy. 1.4 However, you are required to familiarise yourself with, and comply with POPI in its entirety.
What is considered to be personal information?	1.5 'Personal information' means information relating to an identifiable, living, individual or company, including, but not limited to: 1.5.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; 1.5.2 information relating to the education or the medical, financial, criminal or employment history of the person; 1.5.3 any identifying number, symbol, e-mail address, physical address, telephone

APPENDIX H: UNIVERSITY ETHICS CLEARANCE LETTER



UNIVERSITEIT
STELLENBOSCH
UNIVERSITY

APPROVED WITH STIPULATIONS
REC Humanities New Application Form

11 December 2018

Project number: MIL-2018-8427

Project title: PERCEPTIONS ON CYBERSECURITY AMONG SOUTH AFRICAN MILITARY OFFICERS

Dear Mr Kyle Bester

Your REC Humanities New Application Form submitted on 9 October 2018 was reviewed by the REC: Humanities on 29 November 2018 and approved with stipulations.

Present Committee Members:

Dr. Bronwyne Coetzee, Mr Terence Erasmus, Mrs. Magdalena Fouche, Miss Clarissa Graham, Dr. Susan Hall, Prof Leonard Hansen, Ms. Lindiwemhakamuni Khoza, Dr. Anthea Lesch, Dr. Theodore Nell, Prof Douglas Rawlings, Dr. Anna Smith, Mr. Jerall Toi, Dr. Samantha van Schalkwyk, Mr. Aden Williams

Ethics approval period:

Protocol approval date (Humanities)	Protocol expiration date (Humanities)
29 November 2018	28 November 2019

REC STIPULATIONS:

The researcher may proceed with the envisaged research provided that the following stipulations, relevant to the approval of the project are adhered to or addressed:

1. OVERVIEW

The researcher should consider some language editing of the supporting documents (for example, the consent form for the paper-based surveys discusses audio recording, which is only relevant for the consent form for the interviews).

2. PARTICIPANT SELECTION AND RECRUITMENT

2.1) It is not clear how the researcher will approach selected participants (for example, will he email them, invite them to an information session, or approach them in some other way?) [RESPONSE REQUIRED]

2.2) It appears that the researcher intends to ask the three institutions to share a list of potential participants and their contact details with him. Such an approach may limit the institutions' ability to give effect to their staff/students' right to privacy. Specifically, the staff/students may not have indicated that they are comfortable with the institutions sharing their information with a third party for research purposes. The researcher should engage with the institutions to determine if their privacy policies and notices allow them to share the contact details (and thus support his proposed recruitment strategy) and/or consider a different approach (for those institutions that cannot allow such an approach). [RESPONSE REQUIRED]

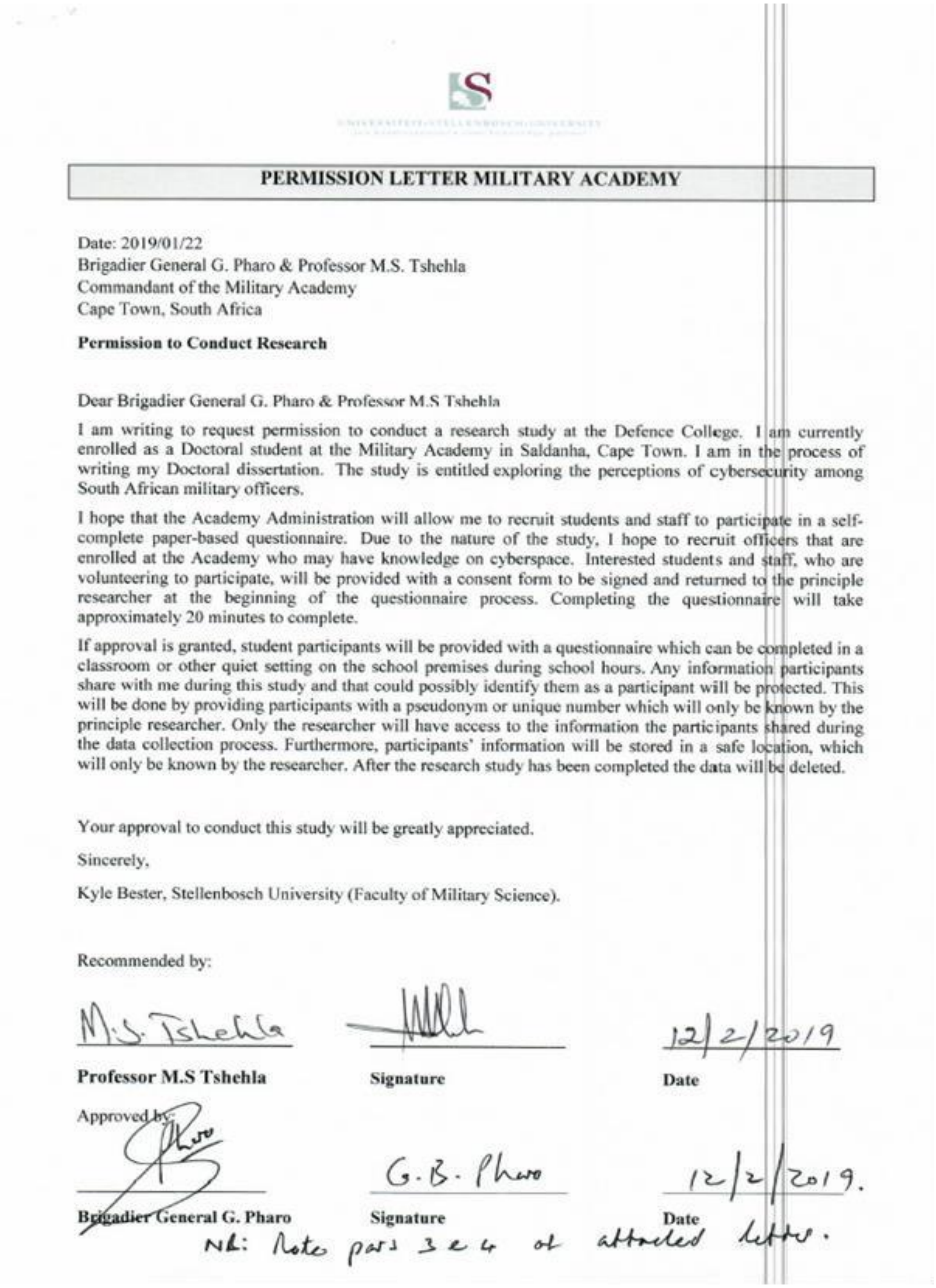
3. INFORMED CONSENT AND ASSENT PROCESSES AND FORMS

The consent form only refers to interviews and does not seem to cover questionnaires. Please develop and submit an informed consent form for planned surveys. [RESPONSE AND ACTION REQUIRED]

4. ADEQUATE MITIGATION OF RISK

The researcher may consider putting together a list of resources for participants, should one of them realise, during participation, that they may have exposed themselves via a phish or other threat. The researcher should check with participating organisations or institutions if they have protocols and departments in place who can assist participants who are uncertain whether they have been compromised by a cyber-attack. The relevant contact details and information could be added to the informed consent form for

APPENDIX I: PERMISSION LETTER FROM THE SOUTH AFRICAN MILITARY ACADEMY



PERMISSION LETTER MILITARY ACADEMY

Date: 2019/01/22
Brigadier General G. Pharo & Professor M.S. Tshehla
Commandant of the Military Academy
Cape Town, South Africa

Permission to Conduct Research

Dear Brigadier General G. Pharo & Professor M.S Tshehla

I am writing to request permission to conduct a research study at the Defence College. I am currently enrolled as a Doctoral student at the Military Academy in Saldanha, Cape Town. I am in the process of writing my Doctoral dissertation. The study is entitled exploring the perceptions of cybersecurity among South African military officers.

I hope that the Academy Administration will allow me to recruit students and staff to participate in a self-complete paper-based questionnaire. Due to the nature of the study, I hope to recruit officers that are enrolled at the Academy who may have knowledge on cyberspace. Interested students and staff, who are volunteering to participate, will be provided with a consent form to be signed and returned to the principle researcher at the beginning of the questionnaire process. Completing the questionnaire will take approximately 20 minutes to complete.

If approval is granted, student participants will be provided with a questionnaire which can be completed in a classroom or other quiet setting on the school premises during school hours. Any information participants share with me during this study and that could possibly identify them as a participant will be protected. This will be done by providing participants with a pseudonym or unique number which will only be known by the principle researcher. Only the researcher will have access to the information the participants shared during the data collection process. Furthermore, participants' information will be stored in a safe location, which will only be known by the researcher. After the research study has been completed the data will be deleted.

Your approval to conduct this study will be greatly appreciated.

Sincerely,

Kyle Bester, Stellenbosch University (Faculty of Military Science).

Recommended by:

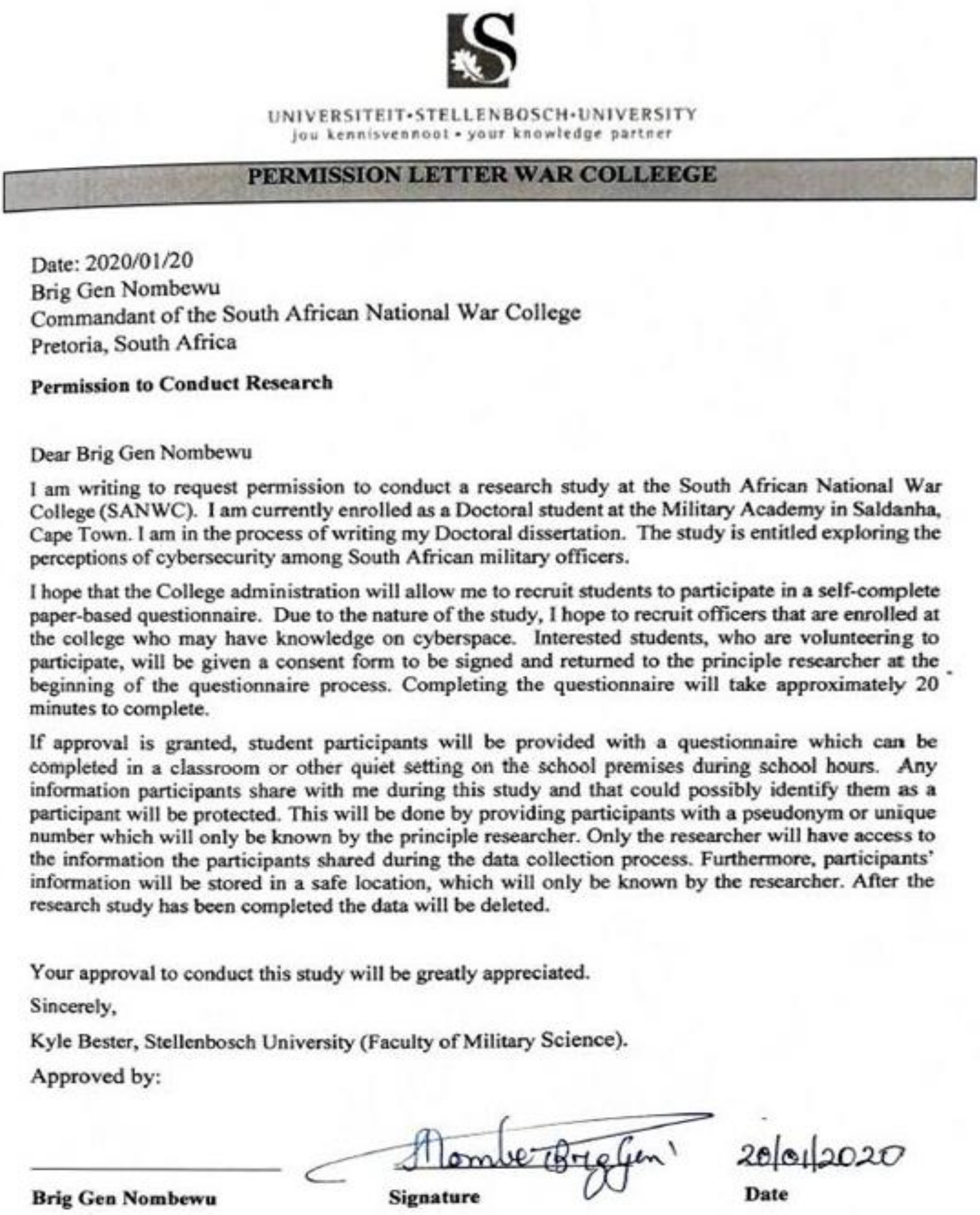
M.S. Tshehla		12/2/2019
Professor M.S Tshehla	**Signature**	**Date**

Approved by:

	G.B. Pharo	12/2/2019.
Brigadier General G. Pharo	**Signature**	**Date**

NB: Note pars 3 & 4 of attached letter.

APPENDIX J: PERMISSION LETTER FROM THE SOUTH AFRICAN NATIONAL WAR COLLEGE



UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvennoot • your knowledge partner

PERMISSION LETTER WAR COLLEEGE

Date: 2020/01/20
Brig Gen Nombewu
Commandant of the South African National War College
Pretoria, South Africa

Permission to Conduct Research

Dear Brig Gen Nombewu

I am writing to request permission to conduct a research study at the South African National War College (SANWC). I am currently enrolled as a Doctoral student at the Military Academy in Saldanha, Cape Town. I am in the process of writing my Doctoral dissertation. The study is entitled exploring the perceptions of cybersecurity among South African military officers.

I hope that the College administration will allow me to recruit students to participate in a self-complete paper-based questionnaire. Due to the nature of the study, I hope to recruit officers that are enrolled at the college who may have knowledge on cyberspace. Interested students, who are volunteering to participate, will be given a consent form to be signed and returned to the principle researcher at the beginning of the questionnaire process. Completing the questionnaire will take approximately 20 minutes to complete.

If approval is granted, student participants will be provided with a questionnaire which can be completed in a classroom or other quiet setting on the school premises during school hours. Any information participants share with me during this study and that could possibly identify them as a participant will be protected. This will be done by providing participants with a pseudonym or unique number which will only be known by the principle researcher. Only the researcher will have access to the information the participants shared during the data collection process. Furthermore, participants' information will be stored in a safe location, which will only be known by the researcher. After the research study has been completed the data will be deleted.

Your approval to conduct this study will be greatly appreciated.

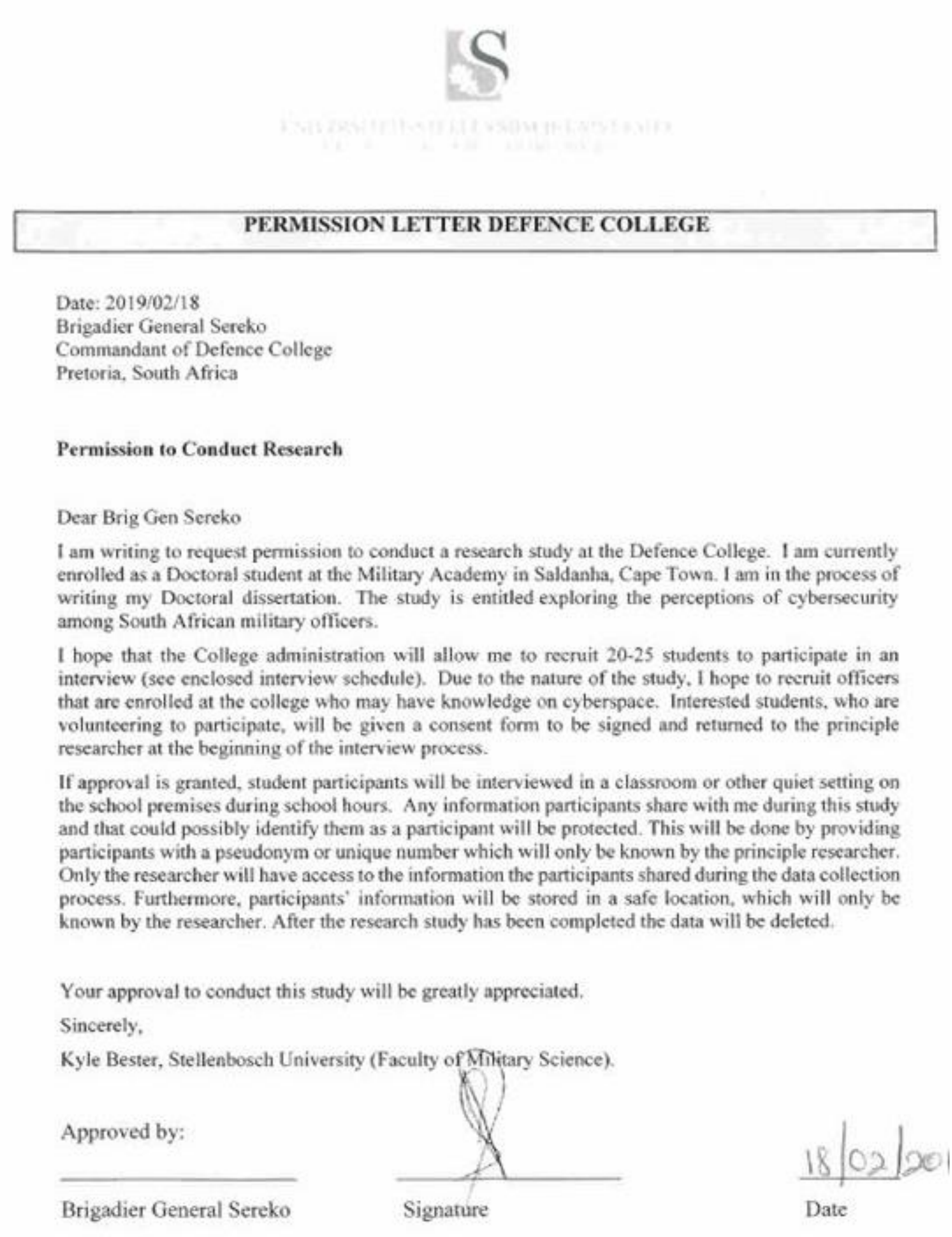
Sincerely,

Kyle Bester, Stellenbosch University (Faculty of Military Science).

Approved by:

	Nombe Brig Gen	20/01/2020
Brig Gen Nombewu	**Signature**	**Date**

APPENDIX K: PERMISSION LETTER FROM THE SOUTH AFRICAN NATIONAL DEFENCE COLLEGE



PERMISSION LETTER DEFENCE COLLEGE

Date: 2019/02/18
Brigadier General Sereko
Commandant of Defence College
Pretoria, South Africa

Permission to Conduct Research

Dear Brig Gen Sereko

I am writing to request permission to conduct a research study at the Defence College. I am currently enrolled as a Doctoral student at the Military Academy in Saldanha, Cape Town. I am in the process of writing my Doctoral dissertation. The study is entitled exploring the perceptions of cybersecurity among South African military officers.

I hope that the College administration will allow me to recruit 20-25 students to participate in an interview (see enclosed interview schedule). Due to the nature of the study, I hope to recruit officers that are enrolled at the college who may have knowledge on cyberspace. Interested students, who are volunteering to participate, will be given a consent form to be signed and returned to the principle researcher at the beginning of the interview process.

If approval is granted, student participants will be interviewed in a classroom or other quiet setting on the school premises during school hours. Any information participants share with me during this study and that could possibly identify them as a participant will be protected. This will be done by providing participants with a pseudonym or unique number which will only be known by the principle researcher. Only the researcher will have access to the information the participants shared during the data collection process. Furthermore, participants' information will be stored in a safe location, which will only be known by the researcher. After the research study has been completed the data will be deleted.

Your approval to conduct this study will be greatly appreciated.

Sincerely,

Kyle Bester, Stellenbosch University (Faculty of Military Science).

Approved by:

		18/02/201
Brigadier General Sereko	Signature	Date

APPENDIX L: CONTENT ANALYSIS SHEET PROCESS INDICATING MEANING UNITS, CODES, CATEGORIES, AND THEMES FOR PHASE 1

Main theme 1: Knowledge production and training focusing on cybersecurity awareness					
Sub-theme 1.1: Awareness and knowledge of cyber space and its associated dangers					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
I think the organisation should enforce a policy more if there is one and to check and make a presentation during war period once a month to say like that there were 7 violations on Facebook and counter-M should look at this to create that awareness on rules and order within cyberspace" (2)	Awareness of cyberthreats and attacks	Violations in cyberspace	Awareness construction	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness
"Like I said being a human and pushing the military away from the normal human being, uhm which is from a personal capacity uhm I don't think that I take it that seriously, but in my work environment I take it very seriously and I know the consequence and implications. But from a personal view people or hackers can build a personal profile of you and putting it out there and that's why I don't belong to Facebook or have a Facebook Profile, but I am on WhatsApp as it is more commonly used. So you can see my profile, but it doesn't say anything more on me. One thing that I do use is LinkedIn which is what I use for jobs and linking with other professionals in my field and sharing information and creating a network. I also see a lot of my other colleagues on LinkedIn that is of national security value in the sense that this information can be used either against or for. And you can use cyberattacks to get this information which is another	I do not take it that seriously in my personal capacity, but in my professional capacity I consider security to be important	Violations in cyberspace	Awareness construction	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness

Main theme 1: Knowledge production and training focusing on cybersecurity awareness					
Sub-theme 1.1: Awareness and knowledge of cyber space and its associated dangers					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
form of warfare in my opinion and if you are not aware of it you may see your downfall" (1)					
People are being caught out for violating certain cybersecurity procedures it's usually kept quiet, I think we should make it visible and expose those that are not violating the organisation's trust and procedures.	Awareness of cybersafety procedures	Violating organisation trust	Absence of awareness procedures	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness
There are many formal presentations that have taken place regarding the awareness of cyberthreats and that are why when we speak about cybersecurity it's hyperlinked to something and it's not a stand- alone topic. And as the department of defence we should be more advanced than everybody else in the society, because if we cannot do that all nonsense ends up in the DoD (3)	Awareness of policy regarding cybersafety measures	Awareness initiatives	Awareness construction	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness
My understanding is that we should be able to function and share information without external stakeholders who are intending to interfere with our daily activities in the military when it comes to information…This should come through basic training, so that we can be taught this subject at every course you come in contact with. The topic of cybersecurity should be considered a must at every course you are attending and should continue throughout your training as an officer (6)	We should be able to share information without people interfering in operational activities and this information should be available at basis training	Awareness through education	Awareness construction	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness
We do awareness campaigns during the officer commanding periods that we have, counter-intelligence presents then uhm with collaboration with SITA we schedule information security courses	Awareness of policies that are related to information security	Awareness through education	Awareness construction	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness

Main theme 1: Knowledge production and training focusing on cybersecurity awareness					
Sub-theme 1.1: Awareness and knowledge of cyber space and its associated dangers					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
"No, I am not security conscious because we are not taught, because the department is not strict on us or telling us to follow the guidelines or even bringing in awareness on that factor" *(p6)*	Awareness of rules and guidelines in the DoD regarding procedures	Lack of seriousness	Absence of awareness procedures	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness
The way we structured our security cluster and how we interact with other stakeholders, uhm all I can say is that people always wake up after the incident. We are reactive as South Africans and we are supposed to be proactive. We are reactive in everything and that's the reason why some of us don't see cyberthreats as a threat. The military should control cyberspace and should be on top (p3)	Some officers are proactive in taking security measures	Proactive measures	Measures to secure information in cyberspace	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness
Cybersecurity has been around for the last decade or so, uhm in the military context uhm we have good plans, and policies, but implementation is the issue. But I think because we haven't had an attack or a threat we don't really take it seriously. Yes I am aware that we have some computers stolen, many of them 30 or 40 computers were from HQ and they contained information that was sensitive and that could be the link of why they wanted to take it (3) which is working quite well because after a certain time they just don't do maintenance on those old computers. They are actually forcing the units to purchase new computers and dispose of the old (9)	Cyberthreats not considered real or important	Lack of seriousness	Challenges of implementation in the organisation	Awareness and knowledge of cyber space and its associated dangers	Knowledge production and training focusing on cybersecurity awareness

Sub-theme 1.2: The establishment of cybersecurity awareness among military members					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
I Think that all officers are aware of it uhm I don't remember the course name but uhm we have the basic and advance course in our unit that deals with the security of information (1)	Security courses are available at certain units	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness
I would say it's limited due to the DoD scaling down over the years and still scaling down. And obviously you have the lack of expertise and lack of knowledge and because we change people every 3-6 years and you have a different person with a different background in how they deal with things.	Knowledge regarding cybersecurity is unevenly spread	Challenges in accessing knowledge	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness
This should come through basic training, so that we can be taught this subject at every course you come in contact with. The topic of cybersecurity should be considered a must at every course you are attending and should continue throughout your training as an officer" (6).	Training on cybersecurity should start at a basic level	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness
The DoD needs to equip all members with skills, and remember if you do you're planning then you will see that whatever you say and do can be used against you. For example cellphone of today are like computers, I mean I can say something and tomorrow the person can record it and then tomorrow it's on twitter and on Facebook, which means people think cybersecurity is something like it came out of the sky, and cellphones are considered an instrument that can be used to breach security (10)	Equipping all members with skills	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness
"uhm what we should add is to change the training material and not to just talk about documents but to	Training of members through	Training of members	Training of members to	The establishment of cybersecurity	Knowledge production and

Sub-theme 1.2: The establishment of cybersecurity awareness among military members					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
make young officers and non-commissioned officers aware of the consequences and trends of what currently Is happening in cyberspace and security domain you know" (4)	the changing of training material		create cyber awareness	awareness among military members	training focusing on cybersecurity awareness
"I think cybersecurity should form part of a course to sensitise people to the threats and guidelines of best practices. If you go on formative or on a NCO course there should be a lecture on cybersecurity for your own personal good and for the work" (9)	Cybersecurity should form part of a training course to sensitise members	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Cybersecurity awareness in the organisation
"uhm what we should add is to change the training material and not to just talk about documents but to make young officers and non-commissioned officers aware of the consequences and trends of what currently Is happening in cyberspace and security domain you know. And what's the point of me learning this at higher HQ and it's not filtered down. I am the one securing information, but there is limited information about this at the lower levels. And they are the ones who use Internet and electronic devices the most" (4)	Changing of training material and making awareness available for all	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Cybersecurity awareness in the organisation
There are challenges within our domain. I do feel like just because there is a lack we should continue to inform and teaching youngsters in the organisation as well as the senior personnel about the consequences of information sharing and cybersecurity (1).	Training regarding this should start with junior officers	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness
"I think so and I portray that as well. But in one case you know some people leave nothing to their subordinates and if it's mine then it's mine. If it's intellectual property then it can be shared so I'm more like that. so if I do things I make It available to people	Making training and information available for members	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness

Sub-theme 1.2: The establishment of cybersecurity awareness among military members					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
and I am one of those people that support cybersecurity because I know how damaging it can be" (5)					
This should come through basic training, so that we can be taught this subject at every course you come in contact with. The topic of cybersecurity should be considered a must at every course you are attending and should continue throughout your training as an officer	Training should commence by looking at basic training	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness
"Uhm I believe it should start with basic training as a package of awareness, lectures can also create awareness, let's take a simple example we need to start bottom up approach where we create awareness at a junior level and that awareness needs to take place at that level. A person coming into the DoD can be given this foundation" (10)	Bottom-up approach should be used in cybersecurity awareness	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness
It should be an intervention where one should have training on a monthly basis and deliver education as technology is moving quickly	Regular awareness sessions should be held with officers at units	Training of members	Training of members to create cyber awareness	The establishment of cybersecurity awareness among military members	Knowledge production and training focusing on cybersecurity awareness

Main theme 2: Challenges of trust with technology and members					
Sub-theme 2.1: Vigilance among members of the organisation owing to differences in how cyberspace is approached					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
Well uhm I don't think we have information security. You know neh once a decision is made by the council; the whole DoD knows it and the minutes are published. Before its being communicated to you the rumours are starting to surface (12)	Members are becoming weary of the computers at their units	Trust in technology	Distrust in one another	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members
"Yes, because then officers and non-commissioned officers wont abuse the resources of the organisation and browse on sites that are unprotected and might be harmful to the DoD network (15)	Members do not trust each other due to misuse	Trust in each other	Distrust in one another	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members
"I would make it more visible, if people are being caught out for violating certain cybersecurity procedures it's usually kept quiet, I think we should make it visible and expose those that are not violating the organisation's trust and procedures. If military personnel can see those that have loose lips that can sink ships, then surely this will scare them" (5)	Exposing those that violate trust	Trust in each other	Distrust in one another	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members
"I don't have a problem with the Internet in the DoD because it assists a lot in the research we do. It gives you access to other scholars and their works and a lot of other things. However, people start to misuse the Internet in the DoD and are not security aware" (10).	Members are abusing organisational resources	Trust in each other	Distrust in one another	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members
I do feel that they should share information on what happened on Facebook for example and state that they have detected this and that it's wrong, and	Members are unsure what to do	Trust in the organisation	Distrust in policies	Vigilance among members of the organisation owing	Challenges of trust with technology and members

Main theme 2: Challenges of trust with technology and members					
Sub-theme 2.1: Vigilance among members of the organisation owing to differences in how cyberspace is approached					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
because of the lack of knowledge about a command like this uhm, you kind of don't know what's allowed and what's not allowed. And you don't want to start a name- and-shame campaign but yeah we don't know" (5)	in terms of information sharing			to differences in how cyberspace is approached	
Uhm just the normal antivirus called Kaspersky. So your personal preference plays a role and the programme must show me that it works. MacAfee doesn't remove all the viruses in my experience and it doesn't pick up all the viruses (14)	Members are weary of antivirus challenges within the DoD	Trust in technology	Distrust in DoD computers	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members
I am using Kaspersky and I think currently it's one of good tools to use, I won't say it's the best, you also have to have malware protection as well. Because this malware can also damage the system (10)	Unofficial software is being used to protect against viruses	Trust in technology	Distrust in DoD computers	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members
My personal information is all on the H drive because that goes directly onto the server, the D drive I use specifically for the webpage so that information is just restricted and then on the T- drive I don't like putting things on because it's a sharing thing, sometimes I have to put my PMDS there as an example so when they are done they can just remove it and call me immediately. And if you go on to the T drive now there is a lot of peoples CV's and personal photos which is considered personal and that is a lack of awareness on our side because we don't adhere to the policy and yes (16)	Members do not want to use the military system to store information due to concerns of information being lost or hacked	Trust in technology	Distrust in DoD computers	Vigilance among members of the organisation owing to differences in how cyberspace is approached	Challenges of trust with technology and members

Sub-theme 2.2: The uncertainty of cybersecurity best practices and protocols in the organisation					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Main theme**
How can we regulate something we don't have knowledge on? First let us get the knowledge on cybersecurity and create awareness. I mean let's get the policy and then get the strategy and thereafter decide to monitor and control (12)	Knowledge on creating cybersecurity awareness	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
Yes, I am aware of such a policy. Uhm I feel it's good because there is a big problem with the amount of military personnel using social media and what they post on there as there's no restriction. There is no watchdog, however there is an instruction" (4)	There is limited enforcement of information sharing online	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
"How do you control that because now we need to get everyone who has DoD laptops to sign and out? It becomes a tedious exercise, and yeah it goes about the trust for me, let's say if I say to people this is sensitive stuff that we are dealing with they need to take it the way I take it. I think, that is the only way to be safe which is to instil integrity into our people so that they can understand that we are dealing with sensitive information. Like when we deal with ammunition, they must take it like we are dealing with ammunition. We should take the people to court who transgress and look into the policy of how to do things, but it's like crime, you can regulate it, but they will still commit it. They must find it in themselves to get this integrity and by reporting when they take information home on their laptops or USB's. I mean the DoD can give it to away to them, because it in any case gets taken home" (3)	How do you control security as everyone needs laptops so they are choosing to use their own devices to store sensitive information	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members

Sub-theme 2.2: The uncertainty of cybersecurity best practices and protocols in the organisation					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Main theme**
For instance we had a case where a person was hijacked and in the policy it does state that you must look after your stuff and where you must put it, but it doesn't stipulate certain things, so that policy must be updated and I know it's a lot of work but there are people who are tasked and paid to do this, to keep it relevant to the current technology. I mean it's very old though some of the information there is really old. And they can start by removing MacAfee because I don't feel it's secure (16)		Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
The enforcement of the policies are just not right and I was never allowed as a junior officer to just take a file home and work at home, yet it happens now so there's no information security regulating the content being taken out of the unit and being worked on. Protocol has changed over time" (12)	Shifting policies overtime remains inconsistent	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
"I personally think that the policy is restrictive. However, it is the application of commanders that is the problem. I do feel that Non-commissioned officers should be going on course to inform them about the dangers of sharing information and how we should go about storing this information, but also what information we should not be sharing. So, yes I think it is within our domain to protect this information going out" (1)	The application of the policy from higher up is considered the challenge	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
Let me say there are not really any proper guidelines in place to safeguard information, I think cybersecurity is still a new phenomenon for us and if you look at how people are being hacked it tells you that this is still a new environment and I think we need to get a little bit more research on the subject from more developed countries	There is no proper guidelines because cybersecurity is a new phenomenon	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members

Sub-theme 2.2: The uncertainty of cybersecurity best practices and protocols in the organisation					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Main theme**
on cybersecurity, because when people talk cybersecurity they think it falls from the sky which is not the case you see, cybersecurity is linked to network security, which is more of your Internet type of security which protects the information. You see cyber is just a collective name where a lot of other securities are falling under it (10)					
"Like I said people don't know how crucial information security is because of the relaxed rules and regulations. So until such time where seriousness will be instilled and urgency to abide by regulations, the significance of cybersecurity won't be fully acknowledged. To be honest we don't really secure information at the unit because the seriousness of securing information is taken lightly" (7)	There is a lack of enforcement from the DoD side	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
I don't think the culture is there and that protocol is not being followed for example if you don't have a secret clearance then you are not entitled to that information (12)	The culture is present but it is not being adhered to	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
I personally think that the policy is restrictive. However, it is the application of commanders that is the problem. I do feel that Non-commissioned officers should be going on course to inform them about the dangers of sharing information and how we should go about storing this information, but also what information we should not be sharing. So, yes I think it is within our domain to protect this information going out. So for example if the person transgressed what mechanisms did you put in place to control it, because if you don't make an example the	The policies are too restrictive and is not enforced, which requires stricter implementation	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members

Sub-theme 2.2: The uncertainty of cybersecurity best practices and protocols in the organisation					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Main theme**
rest will just continue to bluntly share information. So I do think it's up to the commanders, but I think the policy is very clear on what to do and what not to do and the use of it. I do believe that it's about the application of the policy and the leadership in the organisation and how well your base is informed about information security" (1)					
I believe the DoD should adopt a stricter policy in terms of how we share information and post things online, because remember now the DoD is the last line of defence. If you're military is crippled then your whole nation will be crippled too (10)	Stricter policies should be adopted by the organisation in terms sharing information	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members
"In the DoD in terms of the cybersecurity, when I refer to the Y2K event we planned for it, but in terms of cybersecurity I have not seen a policy on it. And we have are not prepared to deal with it because we don't take the threats seriously. I have not even seen a draft policy on it, yet in every presentation it comes up like something important, it's almost like terrorism I have not seen any policy that deals with terrorism, yet the words are being thrown around like buzz words or trends (3).	I have not seen a policy on cybersecurity	Trust in policies	Practices and guidelines of cyber in the organisation	The uncertainty of cybersecurity best practices and protocols in the organisation	Challenges of trust with technology and members

Main theme 3: The construction of a digital culture among members					
Sub-theme 3.1 Culture of digital security among officers					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Main theme**
There are many formal presentations that have taken place regarding the awareness of cyberthreats and that are why when we speak about cybersecurity it's hyperlinked to something and it's not a stand- alone topic. And as the department of defence we should be more advanced than everybody else in the society, because if we cannot do that all nonsense ends up in the DoD" (3)	There's a lack of intent to focus on cybersecurity	Online security culture	Relaxed take on cybersecurity	Culture of digital security among officers	The construction of a digital culture among members
"Uhm eh a very interesting question. Uhm I would say passive. Passive in the sense that because it's not considered a real threat yet. Most likely because we have not have cyberattacks to an extent where I can say There's a threat so I can say guys seeing that there was a threat here is the protocol line it up with instruction and policy lets now do that, it's like closing the doors against anything and everything. I don't think we have closed the doors, we are still open and basically being passive until a real threat has presented itself and maybe it's a good thing or a bad thing. For now I would consider it passive (1).	I would say cybersecurity is considered to be relaxed	Online security culture	Relaxed take on cybersecurity	Culture of digital security among officers	The construction of a digital culture among members
It can be used to do research especially at this unit because of our students and for all the colonels to go and study. And it can be used to communicate with my lecturer or anyone else. The Internet is not a bad thing for the DoD, but there are bad people on the outside and it depends on how you will approach it and defend yourself and you're basically handle it. If people stick to the policy and remember that they aren't allowed	The Internet is not a bad thing	Online security culture	Relaxed take on cybersecurity	Culture of digital security among officers	The construction of a digital culture among members

Main theme 3: The construction of a digital culture among members

Sub-theme 3.1 Culture of digital security among officers

Meaning unit	Condensed meaning unit	Code	Category	Sub-theme	Main theme
to go on certain sites then it will be okay, if not, those who are not adhering to the policy must be charged (16)					
"I think the information security in the organisation is bad and I don't believe that there is a culture around it. I think if you don't make an example it will continue to go the same way" (5)	Information security is bad as there is no culture	Online security culture	Behaviour of not caring	Culture of digital security among officers	The construction of a digital culture among members
"We are completely 'slapgat' when it comes to information. We don't worry anymore; I think we are oblivious so they just share information yeah like there is no threat" (2)	There is a relaxed culture	Online security culture	Relaxed take on cybersecurity	Culture of digital security among officers	The construction of a digital culture among members
"It's a nonchalant type of attitude towards cybersecurity as we expect others to know everything about everyone and anything and here are people working at my unit that pretend to not be techno savvy, meanwhile have access to certain information and is aware about the technicalities of using the computer, and only when something happens in the unit in terms of a cyberthreat then everyone will try and be more secure or we hear about someone that has had his or her computer stolen then the rest will panic and change their passwords on their computers or laptops. I don't think being cyber secure or being safe is considered something that needs to be done very diligently by everyone" (11)	There is a culture of not caring about things	Online security culture	Behaviour of not caring	Culture of digital security among officers	The construction of a digital culture among members
Yes, definitely the computers and members' personal cellphone as they are open to being hacked as well. The relaxed culture in the DoD contributes to the likelihood that these devices can be hacked, that's	Relaxed culture in the organisation	Online security culture	Relaxed take on security	Culture of digital security among officers	The construction of a digital culture among members

Main theme 3: The construction of a digital culture among members					
Sub-theme 3.1 Culture of digital security among officers					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Main theme**
why I raised the issue of consistently monitoring the network and devices being used in units by enforcing the monitoring and evaluation capacity" (7)					
"You see the measures can be there, but the problem Is that the constant monitoring of people will be like I don't trust you DoD members. The guidelines can be there and the boundaries can be employed so that people can develop. But if the organisation creates guidelines and boundaries and still dictate to its members how it should be used then the organisation will not grow, because you have no faith in its members and there will be no innovation in the organisation. If the organisation is allowing its members to go to this end and that end as long as objectives are met. And that is where you allow the space for people to grow. If it's too restrictive then officers will think they cannot be trusted but if you employ the laws and guidelines and allow people to adapt to it than the organisation and people will grow" (3).	Members are not being trusted enough; hence they do not care what upper management introduces	Mutual trust	Absence of mutual trust	Culture of digital security among officers	The construction of a digital culture among members
"Yes, I think so, there should definitely be more education regarding this. Uhm remember you are sitting with two cultures the old school and the new school, the youngsters are having fun playing around with the new stuff and the old school guys are trying to play catch-up and there is a gap between them" (8)	There are two opposing cultures in the organisation	Organisational culture	Organisational response to cyber	Culture of digital security among officers	The construction of a digital culture among members
Well on the network you will see my folder and there are only files that I have shared with people. There are no photos or revealing information of mine on the T	Trust in DoD systems	Different generation	Cyber culture	Culture of digital security among officers	The construction of a digital culture among members

Main theme 3: The construction of a digital culture among members					
Sub-theme 3.1 Culture of digital security among officers					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Main theme**
drive not even on my desktop. This personal information belong to my computer at home" (12)					
"There is no awareness culture in the DoD about cybersecurity I would rate it as a 4 out of 10 which is at its worst, because the majority of officers save DoD information on their personal USB sticks or email it to their personal accounts and don't worry about whether their emails are hacked" (6)	There is no cybersecurity culture in the DoD	Online security	Cyber culture	Culture of digital security among officers	The construction of a digital culture among members

Sub-theme 3.2: Personal devices are considered more efficient to store organisational information					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
Just my memory stick, but what I have done in the past is and I think it was a habit, I started doing and saving my work on the H drive which is backed up, but now if you don't have a copy of your work on your C drive and the H drive is down then you can't work so. In the past I have been able to work because I primarily work on my C drive because what do you do now and I think this is illegal , but it saved my bum a few time, but I make copies of my work and save it on my hard drive and then I leave a copy of that at home and that also enable me when a general contacts me to provide him with the documents at odd hours because of access to the military servers or drives, or when the systems are down I have a copy. It has its positive side, but has a risk can you imagine they break into my house and they steal that information. There are a lot of copies of ID and number for applications,	Members are using their own storage devices to store sensitive information	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members

Sub-theme 3.2: Personal devices are considered more efficient to store organisational information					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
sensitive information and CV's. Okay, but luckily I don't have it anymore, because I'm not in charge of it anymore" (9).					
Yeah you see that's another one, it's not a safe environment this cyberspace, the space where we are operating in, you make access to the unit very difficult to access information especially on weekends., now it's difficult to say that you cannot take the laptop home because the work must be completed. But later you need to get permission to take the laptop home to do the work, but it should not be above your security classification or that you will store any confidential information on that laptop" (3)	It's a very dangerous space to work in and it's very difficult to not take your laptop home because one day you are able to and the next you are not	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members
"But to make sure that there is a computer standing alone somewhere in the building to access emails and have access to the Internet remains important, yet the computers in the DoD are so full of viruses there in the Internet there at uhm LIW that the MSD's used and if you unplug your memory stick there you should first run it through your laptop's virus protection software. The virus protection programme on the work computer is not regularly updated namely MacAfee. I use a different virus protection programme which I purchased out of my *own pocket. During December it costs me about R1000 to save my butt" (1)*	Members are utilising their own devices and Internet connection to browse the Internet due to having trust issues with DoD computers	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members
"The enforcement of the policies are just not right and I was never allowed as a junior officer to just take a file home and work at home, yet it happens now so there's no information security regulating the content	Members are taking home sensitive information and	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to	The construction of a digital culture among members

Sub-theme 3.2: Personal devices are considered more efficient to store organisational information					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
being taken out of the unit and being worked on. Protocol has changed over time" (12)	doing work on their personal devices			store organisational information	
Right now there is no best way as we communicate sensitive information through WhatsApp for the purpose of our day-to-day military activities. We have been cautioned uhm we want this type of information to be in the public domain. But there is no other way as the old methods of doing things , the old methods of using the filing system and using the fax machine we are all in a new era now and it doesn't work as we need to get information to others much quicker (Participant 2)	Ambiguous procedures are causing confusion for members	Unclear awareness procedures	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members
You know at this stage I believe that they are critical because that is the easiest way of sharing information eh. For example if you look at the resources that we have in the DoD, we are unable to secure a laptop for each and every individual. But now we can't say no more USB's to everyone has got a laptop to store information. With the economic conditions we find ourselves in, it's going to be hard for us to reach that goal. Now as a compromise a guy can come and say I've got a laptop at home I can take this information and work at home, and you want to deliver on a specific timeline and in that situation you are compelled to allow this individual to take the information home and complete the task" (3)	Members feel that the organisation cannot afford to buy laptops that are secure for everyone	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members
Well for example tablets that people use in the DoD can be a problem because you can't control them, you can't control the Internet if they don't write in the	Cannot control people who are	Personal devices	Reliance on technology for	Personal devices are considered more efficient to	The construction of a digital culture among members

Sub-theme 3.2: Personal devices are considered more efficient to store organisational information					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
registry and here we don't write in the registry because the learners are complaining about it. I mean it can be controlled because people are using an Internet dongle in the DoD. Here at the unit the only thing we are allowed to have connected is our laptops, but I think that's just protect the learners so that they can have something to do in their free time, but that's not really an effort that can be controlled (16)	using their own devices		operational activities	store organisational information	
Okay, let's put it in more practical and simpler terms let's say when you get to a meeting and you have to store or download information onto your personal USB or hard drive and its normal documentation that I need to panel beat at home and it's a letter to be drafted/ But Nevertheless, the problem is its still military information and I think that's where some of us tend to struggle. If it's not sensitive information I will put on a normal personal USB. And if that's the only one available you will have to drive all the way home pick up your hard drive and come back. So economically it can be hard" (1).	DoD information stored on personal storage devices.	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members
"Yes I use a Mac-Book and I store all my work information on my personal device. And then I save all work-related information on a flash disk which I received from Air Force HQ. Tomorrow I will bring it back to work and then work in such a way again" (2)	I store all my work-related on a flash disk and use my personal computer	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members
Yes, definitely the computers and members' personal cellphone as they are open to being hacked as well. The relaxed culture in the DoD contributes to the likelihood that these devices can be hacked, that's why I raised the issue of consistently monitoring the	Members' personal devices are vulnerable to threats that is why	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members

Sub-theme 3.2: Personal devices are considered more efficient to store organisational information					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
network and devices being used in units by enforcing the monitoring and evaluation capacity" (7)	awareness of the matter is raised				
"In terms of your access control anybody that leaves the unit with a computer should be checked by counter-intelligence and opened up to see what information is leaving. Even though you are deleting that information from the laptop, the problem you sit with is that your hard drive still stores that information on the internal memory, so even if you delete and empty your recycle bin the information can still be retrieved so you just need a person to steal your hard drive. In order to access that internal memory you need to have a tool to check what information is on your motherboard every time a person takes a device home out of unit lines and we don't have the technology to do that at the moment so it's better that people do the right thing but the issue is people are staying all over the place and they are in a rush to catch that bus so they sort of just store that information on a USB" (10)	When a computer leaves the unit, it needs to be monitored and deleted	Personal devices	Reliance on technology for operational activities	Personal devices are considered more efficient to store organisational information	The construction of a digital culture among members

Sub-theme 3.3: Cyber increases the skills gap between more senior and junior military officers					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
I would show them examples because that is the eye opener for people, and I would use scare tactics, yeah I would use bulletins as well, but then again not all troops have access to this resource and our junior officers are more into technology than the older officers, a demonstration and pictures about possible effect of cyberthreats (16)	The older generation needs to understand the dangers associated with cyberthreats	Lack of understanding	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members

Sub-theme 3.3: Cyber increases the skills gap between more senior and junior military officers

Meaning unit	Condensed Meaning unit	Code	Category	Sub-theme	Theme
“There is a culture, but whether we follow the rules and guidelines is another story. Often commanders do not exercise or implement these guidelines and it should be from the bottom down so that NCO’s are also aware of the dangers and threats” (1)	The management is failing to manage the implementation of best practices	Implementation	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members
The top structure of the DoD are not aware of the dangers that the officers are experiencing, I believe that they are confused. But we are also not excused from this as our officers are also responsible for finding out about cyberattacks and security” (7)	There is a limiting understanding on the cyberattacks and security by upper management	Lack of understanding	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members
Like I said sir it’s more of the older generation that promotes this lack of awareness and its more the younger generation is more up to date with cybersecurity and cybercrime. The older generation don’t actually know how to talk about it, they are used to the old way of doing things” (14).	The older generation uses social networking without understanding the dangers associated with it	Lack of understanding	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members
“Yeah you know the measures that we have are traditional measures and not in line with technological advancements and policies are outdated. When I worked in a different environment that is when I first realised that an IT qualification is something serious. You know we had this young guys working there with this qualification and what I noticed was that we cannot cope with this current scope of digital awareness and cannot cope with these guys” (3)	The older generation is used to the traditional modes of communication such as using a fax machine, and sending letters	Older means of communication	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members

Sub-theme 3.3: Cyber increases the skills gap between more senior and junior military officers					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
Yes, I think so, there should definitely be more education regarding this. Uhm remember you are sitting with two cultures the old school and the new school, the youngsters are having fun playing around with the new stuff and the old school guys are trying to play catch-up and there is a gap between them" (11).	The younger generation is fast-paced and that's where the struggle comes in, even securing information	More fast-paced	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members
There's technology that will worsen the situation and I'm afraid that we won't be able to handle the pressure associated with new advancements because we can barely manage our current state of affairs in the DoD" (4)	New technology will worsen the situation as they are not able to handle the current state of affairs	Expanding gap	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members
I think it all comes down to education, uhm let's take the lower-ranking guys and they are on social media and skipping and all these things are 'Lekker', and they don't always think twice before putting information online. Yeah and I just think they need education" (8)	The lower-ranking members are not aware of the dangers through the information they post	Lack of understanding	Divide in the understanding of cyber	Cyber increases the skills gap between more senior and junior military officers	The construction of a digital culture among members

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
It's not just low priority in my unit but across the DoD, I see the stuff that is mailed to me and communicated to me, I see how people say things on WhatsApp, even some exercises. I've heard people say that the exercise would not have been possible without the use of WhatsApp. All	WhatsApp is considered the common tool of communication	Open-source applications	Method of communication	The demand for faster and more efficient communication is becoming	The construction of a digital culture among members

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
command and control happens through WhatsApp, meetings happens through it and it's like the critical success factor.				normalised practice	
I am against this WhatsApp and it's like a losing battle as people adopted this mode of communication in sharing sensitive information, the experts will come and tell you that it's like an email being sent and it doesn't matter what type of information you send because it's like the same thing. I have yet to adopt this method of communication. Even the email I don't prefer to send it over that platform, sensitive information is meant to be on a physical basis from hand to hand. I still believe in the old way of ceiling the envelop and at least you have a point to start" (3)	I am against WhatsApp because sensitive information is being shared	Open-source applications	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
That is why I say rather not post because if you do then it's a breach in disclosing information. The same applies to WhatsApp or Facebook messenger it's not a dedicated tool or line of communication, but most of our officers are using WhatsApp to communicate with their members and for me that's also a security risk and a breach of information because they sometimes give an instruction and then you can access their WhatsApp or Facebook and as soon as you are hacked you have access to everything" (14)	Members are relying on WhatsApp and Facebook messenger to send information	Open-source applications	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
"No, definitely not. Although WhatsApp is a quicker way to receive information, especially when I'm out of town and where I cannot send emails, I mean it's a quicker way to send and receive information. My	It is faster and more efficient	Open-source applications	Method of communication	The demand for faster and more efficient communication is	The construction of a digital culture

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
issue is that it's not regulated or internalised. Remember when the cellphone came in, there was a policy on how to manage information on how to use it" (3)				becoming normalised practice	among members
Yes there are people in units that use these software and applications, but they do so because it's a cheap and easy way of communication, my view on that is and I say we having a meeting tomorrow and they don't consider that sensitive or whatever then it's okay, but if your borders have been breached and we are under attack then information cannot take place over WhatsApp. So you cannot share sensitive information over social media like WhatsApp, rather small things like to communicate a meeting or starting time of work for the next day (10)	People use these applications because it's cheap and effective	Open-source applications	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
Right now there is no best way as we communicate sensitive information through WhatsApp for the purpose of our day-to-day military activities. We have been cautioned uhm we want this type of information to be in the public domain. But there is no other way as the old methods of doing things , the old methods of using the filing system and using the fax machine we are all in a new era now and it doesn't work as we need to get information to others much quicker, we needs to give feedback much quicker and faster on ad hoc type of discussions and doing it the way we used to" (4)	Sensitive information gets shared on WhatsApp	Information security	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
“No, definitely not. Although WhatsApp is a quicker way to receive information, especially when I’m out of town and where I cannot send emails, I mean it’s a quicker way to send and receive information. My issue is that it’s not regulated or internalised. Remember when the cellphone came in, there was a policy on how to manage information on how to use it” (3)	The old way of using signals, letter, and using fax machines are not useful any longer	Emphasis on technology	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
“In the past we had the red telephones in your operational unit so you could communicate easily over that line and share sensitive information. I think we should liaise with the department of communication and external service provides and request that they develop a secure network on which sensitive military information can be communicated over a cellphone. This can also give you a longer ranger than a radio, so that you can easily communicate with someone in the DRC for example. But I believe it’s possible” (10).	A secure network needs to be developed for the defence	Emphasis on technology	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
“Well at this point WhatsApp has become the most commonly used communication tool in the defence force. No more signals and letters because it’s just a faster and quicker method, if you just look at the times we are living in all the red-tape and bureaucracy is delaying the process because operations are moving so fast that you need to make things happen. So yeah I’m not keen on WhatsApp because it costs the individual himself money to do military work” (8)	Information needs to get out quicker	Outdated technology	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
“Once a year there is a transfer signal coming out to say where the colonels are being transferred and that thing ends up in WhatsApp groups. I don’t think the drafter of the signal had time to still send it to 1 military hospital then that document is already in Cape Town and various other units. When I am looking for specific information, for instance it has happened when you are drafting a letter within a short- time space and that letter mist go to somebody but you not sure where the signature block should be and how it should look like and then you phone somebody in that environment and to ask that person to take a photo of a letter and send it to me as an example. It just makes things so much easier. I don’t ever send sensitive information to my colleagues” (9)	Photos of signals and letters are shared on social media as a way to reach others	Security awareness	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
I think sharing information on the WhatsApp group is dangerous. It also depends on the type of information that you are sharing. As you know the applications you have and download on your phone is always linked to a foreign country like China for example. But I do know that it all depends on the make of your phone so they have direct access and they can zoom in your information and so forth. Uhm and I must admit we have been doing as there is a clear absence of communication in the DoD, uhm we have systems in place, but has not been adjust through the times you understand. This is quick news, quick information, quick sharing whereas in the old days you had to write a signal	WhatsApp replacing current means of DoD communication because its faster and formal communication means such as telephones are not as efficient	Unclear awareness information	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
where you first have to prepare the content and go through the editing process and go onto the system by sending out the signal. Uhm, and yes we have official phones, but we don't have official network like SETA that will protect us from sharing information. Uhm, to a certain extent we do have a system in place, but we are not serious about the sharing of crucial information. The type of systems that we are using should be aligned with the modern technology. We are still using the SAT-Phones you know and things like that. I believe that the defence force has not moved on the use of new technology" (1).					
"Yeah it's not good at all; it has become a culture not to think about those things in the organisation. Uhm yeah, I was involved in a few years ago in accident, but the way those photos were transferred on flash disks was horrific, personally I am very secure about information as I deleted in immediately and clean it, but there is people that keep this information, and then they still say they are security conscious" (2)	Sensitive information such as video clips and pictures are shared online	Information security	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
Officers checking in, posting pictures of their uniform online, writing statuses and posting their location are not safe, because at the end of the day you are a public servant and your responsibility is to look after the public and South Africa. Let's say some of our enemies abroad are looking into our military systems and they happen to bump onto whatever it is you are posting how you are keeping	Pictures of members in their uniform are shared online or posted online is a way of compromising their own safety	Unclear awareness information	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
us safe as a country if you are revealing information, so I'm just totally against it (15)					
"It's bad. WhatsApp is not correct way of communication but it's the communication current way of communication, its quicker to WhatsApp someone than to phone them and I do feel it's a risk because sensitive information is shared over WhatsApp and it's not the safest communication source" (14)	The old way of communicating is tedious	Emphasis on technology	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
When I am looking for specific information, for instance it has happened when you are drafting a letter within a short-time space and that letter must go to somebody but you not sure where the signature block should be and how it should look like and then you phone somebody in that environment and to ask that person to take a photo of a letter and send it to me as an example (9)	Using social platforms to receive and send information	Emphasis on technology	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
I am of the opinion that it shouldn't take place, but I'm also of the opinion that communication overall in the DoD takes place when we react quicker to WhatsApp and those types of groups than by waiting for instructions and orders to be given and materialised. So currently it's not right, but it seems that it works, because we wait for paper orders and nothing happens" (5)	Communication is faster on WhatsApp	Emphasis on technology	Method of communication	The demand for faster and more efficient communication is becoming normalised practice	The construction of a digital culture among members
"I feel the SANDF cannot keep up with the rapid technology that is being introduced. For instances the use of drones can so easily be deployed, instead of sending 4 men with a vehicle to patrol the	The SANDF cannot keep up with the demand for faster technology	Emphasis on technology	Technological demand	The demand for faster and more efficient communication is	The construction of a digital culture

Sub-theme 3.4: The demand for faster and more efficient communication is becoming normalised practice					
Meaning unit	**Condensed Meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
perimeter, the amount of fuel, time and impact on the environment and patrol the area for the fraction of the cost. In terms of cybersecurity I feel the DoD should draw in the youngsters from the techno world and to go look for them" (1)				becoming normalised practice	among members

Main theme 4: The view on cyberthreats is constructed based on experiences in the physical domain					
Sub-theme 4.1: Information security as a practice					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
I am a bit of a private individual. My behaviour is adjusted towards the circumstances of the information being sent to me. People should be more aware in the DoD. Officers share things on the T drive and NCO's see this and will replicate the same behaviour. Access to certain information should be restricted in the DoD (11)	Knowledge practices cybersecurity in the personal capacity assists with securing information in the workplace	Prior knowledge	Prior knowledge assists with information security	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
You know from a personal point of view the nature of my information might be very personal for me so for me uhm I am aware of the dangers and consequences in going onto an open WI-FI network and Uhm I tend to ignore the security risk to myself, but within the security domain I find myself in I tend to be cautious when around those networks with my work hardware (1)	I find myself to be very cautious in the security domain	Physical security vs digital security	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"Because they are not interested, I think they still want to fight with big tanks and technology is just considered to be there, but what if they get attacked and they don't get paid, then they will realise that there is a problem because it will hit them in their hearts. Either they are	Physical security is considered more a threat than digital security	Physical security vs digital security	The balance between viewing threats in a physical	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain

Main theme 4: The view on cyberthreats is constructed based on experiences in the physical domain					
Sub-theme 4.1: Information security as a practice					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
not interested or it's the whole idea of we will rather fight with tanks and what not. So technology is not that important to them" (16)			and digital space		
Well we don't always follow protocol because we do renew our passwords on the military devices but not on all the stand-alone PCs at work. We are taking computers out of the unit with confidential information and it is not sometimes classified or that the information is sometimes encrypted or converted (4)	Computers are removed with sensitive information	Access to information	Official hardware used for securing information	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"The LAN system that we work on forces us to change our passwords regularly and apart from that more than one person is able to have access to the folder I created on the network. So it's just wise that one be aware of the information you put on the T drive and the sensitivity of documents. If you don't want your information on the T drive you can always save information on another device where few have access to it. So your information in the DoD is never 100% secure" (11).	The T and H drives are considered the digital way of securing information	Access to information	Official hardware used for securing information	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"I wouldn't say cyberattacks but we had serious communication failures one moment you may have access to the T drive and H drive depending where you are situated then you may be cut-off from the network because of some malfunction I don't necessarily see it as a threat, but it could be possible threats" (1)	Unstable access to online DoD storage systems	Access to information	Official hardware used for securing information	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain

Main theme 4: The view on cyberthreats is constructed based on experiences in the physical domain					
Sub-theme 4.1: Information security as a practice					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
I am a bit of a private individual. My behaviour is adjusted towards the circumstances of the information being sent to me. People should be more aware in the DoD Officers share things on the T drive and NCO's see this and will replicate the same behaviour. Access to certain information should be restricted in the DoD" (11)	Information on the DoD storage drives are easily accessible and can be used to store sensitive information	Access to information	Behaviour of information security practices	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"No, especially because I'm not very technologically competent. So nowadays people are calling you with scams and stuff, the other day I picked up a virus that was linking me to a Wi-Fi. So no, ideally it's not good" (5)	I am not technically competent and people are trying to exploit me	Access to information	Behaviour of information security practices	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"Like I said I put everything on the T drive. So that my subordinates are able to learn from me, so now while I'm on course the Lt Colonel that is acting and taking over from me, can get the documents on the T drive" (5).	I place everything on the T drive so that juniors are able to learn	Access to information	Behaviour of information security practices	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"Well we have servers such as the T drive and H drive and also other drives on the server if it's effective I don't know. But one thing I have noticed from the United Nations is that they make use of Outlook Express in order to transfer information in the mission area and if you open an email that was sent to you and if it's of a sensitive nature then the message and attached document will self- destruct that they send via outlook express and the South African Defence Force should maybe look into those areas" (10)	We have servers in the DoD that is maybe effective	Access to information	Behaviour of information security practices	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain

Main theme 4: The view on cyberthreats is constructed based on experiences in the physical domain					
Sub-theme 4.1: Information security as a practice					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
Uhm I am not aware of any technology that can be used for hacking or that can be hacked in the organisation, but I am of the opinion that were high technical equipment that was stolen, but uhm, I think operational plans and stuff was stolen once, but I cannot think of anything specific. I know the Persol system I assume will be secured so there's not actually something I can think about. Hacking is possible, which is like stealing. You protect your vehicle against theft, but they tell you what measures you have in place, but it still gets stolen within in seconds. Personally think where there is a will there's a way" (5)	There is technology in the organisation that can be used for stealing information	Accessing information	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
Uhm if you lock it in a safe uhm then it depends who has access to that safe you see. I think that there needs to be a central point it can either be locked in a unit level or counter-intelligence office or officer commanding or your staff head if it's in an admin or staff environment at your higher headquarters. But it should not be that everybody has got access to that mobile device or memory stick or some sort to store sensitive information. There should be one access point to that document and it should be locked in a safe totally sealed in an envelope for safe keeping" (10)	Using a central point in signing out documents are considered the safest way to secure information	Accessing information	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"Uhm it should be in one office, but on different computers. And in all the other offices it should only be a shorted version of the main one" (7).	Information should be on different computers and in the office	Physical security vs digital security	The balance between viewing threats in a physical	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain

Main theme 4: The view on cyberthreats is constructed based on experiences in the physical domain

Sub-theme 4.1: Information security as a practice

Meaning unit	Condensed meaning unit	Code	Category	Sub-theme	Theme
			and digital space		
“The old school way of filing documents in a locked file cabinet” (11)	Using a filing cabinet is considered a way of securing documentation in the workplace instead of relying on the DoD system	Physical security vs digital security	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
“The traditional way is the best way such as locking information in the safe. The challenge that we have is that digital migration has had a big impact on how we look at things. Eh. We are in a world that is evolving we can be seen sitting in corners and the development pass us, as a result of that we send information through emails so that we can catch up which makes the security of that information very difficult as there is someone that controls this information on this space. The best way to control this information is to lock it in a place where you can physically keep it safe” (3)	The traditional way of securing information is the more appropriate as digital security comes with challenges	Physical security vs digital security	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
“I would change my passwords once a month, but I would use the same one for all my accounts and devices. It’s been like this for years because if you check my Facebook, WhatsApp, twitter or banking details are all the same. ..In my personal capacity I am weak hey because most of my passwords are the same throughout the bank and social media. There	I would change my passwords regularly, but they are all the same one social media platforms	Physical security vs digital security	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain

Main theme 4: The view on cyberthreats is constructed based on experiences in the physical domain					
Sub-theme 4.1: Information security as a practice					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
are loads of sites so I prefer to have one password for all my things" (6)					
In the DoD we are using MacAfee on the network and on the stand-alone computers we have Kaspersky. But I wouldn't say that is enough security because that's just the antivirus, they do have firewalls and all that, but the human element is the problem because they can still find out what the passwords are (16)	The DoD provides MacAfee Internet security as a way to secure information on their computers and systems	DoD software	Members assessing the trustworthiness of DoD-sanctioned software	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
Uhm communication would never ever stop in the DoD, there is an email system in the defence force called Lotus notes where very few people have access to as I for one do not. It's an old system that is being used. In the unit I currently work at we are very fortunate where all of us have emails and computers so we email and fax communication. However, in the unit we also do the memos to inform people about certain things that are common and giving reports to your supervisor in writing and we send confirmatory notes of meetings" (11)	Some officers have access to Lotus notes, but this is not accessible to everyone in the DoD	DoD software	Members assessing the trustworthiness of DoD-sanctioned software	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
"There should also be an emphasis on what can happen and education on how you should secure yourself. I know we get uhm secure lotus notes as well, but uhm you don't always read it. But I do think the presentation should be more formal" (2)	There is information on Lotus notes but I don't always read it	Accessing information	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
There is software available for that. I feel that this software is not provided to all officers and If it is	Accessing the DoD software can be attained by members	DoD software	Members assessing the trustworthiness of DoD-	Information security as a practice	The view on cyberthreats is constructed based

Main theme 4: The view on cyberthreats is constructed based on experiences in the physical domain					
Sub-theme 4.1: Information security as a practice					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
provided we are not using it because we must log into a specific folder with a password (14).			sanctioned software		on experiences in the physical domain
But the main problem is the securing of information when it's off the network. That is more of a problem because now it's a physical problem because if you can gain access you can take the information and then you can put it on your memory stick. If you lose your memory stick it's easy for someone to get that information and log into your computer. So the measures are in place to secure information in the DoD. But it's the person behind the computer that must enforce the rules and adhere to the prescripts of the DoD-E and ISS policies	Information security is dependent on the individual behind the device	Physical security vs digital security	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain
I'm not much of an online person, but if I go online, I do what I need to do. I'm not an inquisitive person who would go outside my barriers for example if I go and research something I just go and do that. In terms of cellphone banking, it was useful because I could go and buy airtime and make a call. The basic stuff I can do, but beyond that I'm not curious (3)	I do what I need to online and perform the necessary functions	Accessing information	The balance between viewing threats in a physical and digital space	Information security as a practice	The view on cyberthreats is constructed based on experiences in the physical domain

Sub-theme 4.2 Perception is an important aspect for members					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
According tome our environment is a closed environment. And that is where I find problems where people past sensitive stuff on WhatsApp for other to view, everything we deal with here is sensitive, and if the public wants to know we should inform the public. Some information is transmitted to gadget and very difficult to control. There are two people that I don't like and that is Erica Gibson and bietjie Greef who are well connected and every time they have the correct information. The more you have measures in place, the more others want to break it" (4).	There is a fear for some journalists reporting about military issues	Vigilance	Perception of insecurity	Perception is an important aspect for members	The view on cyberthreats is constructed based on experiences in the physical domain
All information in the DoD is considered sensitive in my view thus being crucial. My personal information is also important, but DoD information is most important. The problem is people on the outside know more about what is happening inside the DoD than those who work there (3)	All information in the DoD is sensitive and the issue is that external people know more about the organisation	Vigilance	Perception of insecurity	Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain
Look somehow these sensitive documents containing information ends up with Erica Gibson because she has definitely been informed about our information and you see with cameras it's easy because you can easily take a photo or record a discussion. And in this environment if you want the information you will be able to get it and hurt somebody (9)				Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain
We share too many things in the organisation and a lot of information is founded on rumoured information, but usually where there's smoke there's fire. So we disclose information more easily. A lot of military information is shared with civilians and the next	Crucial military information is shared with the public	Vigilance	Perception of insecurity	Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain

Sub-theme 4.2 Perception is an important aspect for members					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
moment this information is in the newspapers and blown out of context" (4).					
Uhm I don't think people are aware of what they should be doing and how they should treat information for instance the in- thing as of late is when you get a signal you take a photo and send it to your colleague via WhatsApp, though WhatsApp is encrypted. But the thing is once the information is out in the public domain its public knowledge and with right software you are able to access that information. I often think that one should rather leave your cellphone at home or in your car so that you are not tempted. And I think that we are checking our messages and communicate with other through WhatsApp every single day" (9)	There is frustration that crucial information is known by members of the public whilst the officers In the force are not even aware of this information	Vigilance	Perception of insecurity	Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain
Yeah that's a difficult one hey, well I don't know if a stricter policy will be effective because we know how the policy of the country is working. Maybe when the policy is enforced there will be results so when I send a letter to the Chief Director it will be going straight to him and not a copy via WhatsApp being sent all over the world. for example when the Chief communicated that the course will take place two weeks later that information was communicated with everyone, but the institution did not know about it on an official document, yet this information was published by Erika Gibson, so now where the hell did she get it from, and if you receive a letter and its addressed to you, then it's for your eyes, if not then it has nothing to do	The public knows more what is happening in the DoD than its members	Vigilance	Perception of insecurity	Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain

Sub-theme 4.2 Perception is an important aspect for members					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
with you. Currently it does not work like that because in this era all information is shared" (12)					
"In actual fact it should be a lifestyle, they should not only be informed they should live it. For example if I take a picture of one of my colleagues and put it on social media, what perception are you creating to the general public about the South African soldier. But if I innocently put something online where we as soldiers are singing then the perception will be on the outside look at these soldiers they are dancing and singing should they not be drilling for example so it creates a total different perception, we saw during the armed forces day where the sergeant major brought the guys to attention and some of them were just standing around that says to me there's no discipline you see and that's the perception that is created. People create their own perceptions on social media but also internationally how other armed forces are viewing the South African soldier" (10)	Public perception is important especially for the South African soldier	Vigilance	Perception of insecurity	Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain
I would rather say that we need to be aware of the impact of social media and how they use social media. For example people should not pose where they stand with weapons in the field because that depicts our training regime. People should be discouraged of them in uniform on social media, to post photos when they are in training and I know people want to show how they look to their friends, but I think they should rather put those pictures on a CD and show it to their family instead of posting it online. However, we also need to be matured in	Being aware of social media and how the military is depicted	Vigilance	Perception of insecurity	Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain

Sub-theme 4.2 Perception is an important aspect for members					
Meaning unit	**Condensed meaning unit**	**Code**	**Category**	**Sub-theme**	**Theme**
terms of social media because whereby we should post positive things and not things that break down the organisation. If you are going to put something on social media it should be of the benefit to market the organisation and not to break down, because I see in the US they make a lot of use of social media, but the negative stuff you won't see (10)					
Currently yeah uhm, I don't think there is good control over it. I just think there are people posting on the DoD web and there's undisciplined comments being made and stuff so, I think it can be a big threat in general and I do believe that most people are not very secured. We know about the dangers, but I don't think we are doing enough. I have the ability to access my phone and laptop with my thumb scanner, but now I am thinking I should have actually applied it and I haven't (5)	There is a need to control cyberspace in the organisation due to members posting information	Vigilance	Perception of insecurity	Perception as an important aspect to military members	The view on cyberthreats is constructed based on experiences in the physical domain

APPENDIX M: DISPLAY OF CODES FOR QUALITATIVE INTERVIEWS (EXAMPLE INTERVIEW 1)

Meaning unit	Code extraction
Respondent: Any information that can be classified under confidentiality doctrine or any security classification that may entail secrecy	Classification of information
Respondent: Well we do have systems in place and uhm also the registry in order to work your way to top secret, restricted, classified documentation, so there is a clear guideline on how to deal with information. The problem comes in you know, ever since the computer generation in terms of putting documentation on the hard drive, it becomes uhm eh a risk because you are sometimes requested to work at home. And because the systems are not allowed to give you military hardware, it can be become a bit confusing as your personal information can be mixed up with your work information that is often-times considered to be top secret or sensitive. So now the attempt I made was to purchase my own defence hard drive so I store all the defence related documents there and my private documentation separately. Although sometimes it's easier said than done and this is where uhm… you sometimes blur the line when saving official information on your personal hard drive. And sometime visa-versa as sometimes you are not in possession of your defence hard drive, and sometimes you transfer that information to a personal hard drive which could be problematic.	Physical domain digital information Clear guidelines Work pressures Personal devices BYOD Personal storage device Access to information Lack of implementation Secure information Organisational devices Storage of organisational information Personal information on organisational devices Online security culture Emphasis on technology
Respondent: I think we all know it's not supposed to be done. But sometimes you don't have a choice and now I'm being completely honest and well contravene these now and then. Although as an officer you should know what is right or wrong. And to be ethical to save your official information on your personal hard drive is not right. But, uhm sometimes you are forced to do things that is not supposed to be done in that manner. However, this also depends on the classification, uhm I personally feel that if its uhm…an unrestricted document then I don't see a problem, but when it comes to sensitive information the lines should not be blurred	Clear guidelines Breaching guidelines Personal devices Personal storage device Sensitive information Organisational information on personal devices Personal information on organisational devices
Respondent: Okay, let's put it in more practical and simpler terms let's say when you get to a meeting and you have to store or download information onto your personal USB or hard drive and its normal documentation that I need to panel beat at home and it's a letter to be drafted/ But Nevertheless, the problem is its still military information	Personal storage device Organisational information on personal devices

Meaning unit	Code extraction
and I think that's where some of us tend to struggle. If it's not sensitive information I will put on a normal personal USB. And if that is the only one available you will have to drive all the way home pick up your hard drive and come back. So economically it can be hard. The factors around it sometime forces you to make a decision is the information crucial, can it affect national security, is it going to affect the organisation. And Uhm to some extent no it doesn't	BYOD Personal devices Work pressure Breaching guidelines Sensitive information
Respondent: I think they do realise that fact. In my base we do information security and the cyber awareness in the organisation. We also have this security programme which we send out to all that are on courses. So I think it's very clear what to do and what not to do. But as a human being you do something that in actual fact is not supposed to be done. And obviously you have to make a decision on the concept, but also the confidentiality of the matter. I do think that all officers are of it uhm I don't remember the course name but uhm we have the basic and advance course in our unit that deals with the security of information.	Awareness through education Regular training Breaching practices Online security culture Security culture Trust in policies Awareness of threats
Respondent: Besides your normal USB, we have a normal network or the CPU that is connected to the LAN system. Uhm we save our normal and important documentation on the T drive and on the H drive. The H drive is more for sensitive information and the T drive is for everyone to have access to your documentation with certain restrictions	Organisational storage devices Online security culture Security culture Clear guidelines
Well it's through registry, whether it top secret or secret, it has to go through registry. Well the other way uhm is to keep a back-up which is to go about it on your official laptop. Uhm however, the laptop if it is being taken out of the Unit Lines it must have the necessary counter-intelligence clearance. At AFB Makhado they do random checks with SETA and they will come around and scan the Hub to see if some computers are using	Physical security Digital security Personal devices Security checks BYOD Organisational device Clear security processes
I don't use these networks on a work laptop. Personal laptop I do just that most often uhm and then obviously you'll need to have a firewall. You also need to consider the networks and area you are in, for example when you go to a wimpy, that's not a very secure network. But my emails I will open at wimpy, or I will go Telkom or in a network where I feel safe to enter a network. I normally don't use any network; I have my personal Wi-Fi router so often more than usual use that. Every time I normally do or use open-source networks with this bugger called the cellphone, I usually use the hotspot option to just receive my WhatsApp or email. But normally I don't use the open-source networks mainly because of the sensitivity of the information	Personal devices BYOD Personal devices Unsecure network WhatsApp Open-source tools Security awareness Organisational devices WI-FI

Meaning unit	Code extraction
	Security culture Online security practices
Respondent: You know from a personal point of view the nature of my information might be very personal for me so for me uhm I am aware of the dangers and consequences in going onto an open WI-FI network and Uhm I tend to ignore the security risk to myself, but within the security domain I find myself in I tend to be cautious when around those networks with my work hardware.	Awareness of threats Violations in cyberspace Online security culture Online security practices BYOD Personal devices Vigilance
Respondent: First and foremost information about my personal identity remains crucial to me and secondly my bank account, I think that is the most critical one, because if that goes my whole lively hood goes with it. Uhm and then obviously personal matters with institutions that has to do with debt or an application for loans that I would classify as critical not so critical I would classify a message such as hi Mum or sending a pic or two that's not so sensitive for me, but it obviously depends on the content.	Personal information is important Trust in policies Vigilance WI-FI Awareness of threats Online security practices
Respondent: I would say sharing information neither on social media that's a no go nor on a Facebook profile. I think sharing information on the WhatsApp group is dangerous. It also depends on the type of information that you are sharing. As you know the applications you have and download on your phone is always linked to a foreign country like China for example. But I do know that it all depends on the make of your phone so they have direct access and they can zoom in your information and so forth. Uhm and I must admit we have been doing as there is a clear absence of communication in the DoD, uhm we have systems in place, but has not been adjust through the times you understand. This is quick news, quick information, quick sharing whereas in the old days you had to write a signal where you first have to prepare the content and go through the editing process and go onto the system by sending out the signal. Uhm, and yes we have official phones, but we don't have official network like SETA that will protect us from sharing information. Uhm, to a certain extent we do have a system in place, but we are not serious about the sharing of crucial information. The type of systems that we are using should be aligned with the modern technology. We are still using the SAT-Phones you know and things like that. I believe that the defence force has not moved on the use of new technology.	Online security culture Open-source applications Unclear information sharing DoD software Access to information Efficient information sharing Open-source applications Perception of sharing information Restricted information being shared on social media platforms Digital domain Unclear information Mode of communication Open-source applications
Respondent: I personally think that the policy is restrictive. However, it is the application of commanders that is the problem. I do feel that Non-commissioned officers should be going on course to inform them about the dangers of sharing information and how we should go about storing this information, but also what information we should	Restrictive policy Knowledge creation Training of members

Meaning unit	Code extraction
not be sharing. So, yes I think it is within our domain to protect this information going out. So for example if the person transgressed what mechanisms did you put in place to control it, because if you don't make an example the rest will just continue to bluntly share information. So I do think it's up to the commanders, but I think the policy is very clear on what to do and what not to do and the use of it. I do believe that it's about the application of the policy and the leadership in the organisation and how well your base is informed about information security	Trust in policies Organisational guidelines Trust in military members Unclear guidelines Access to information Unclear information-sharing practices Trust in policies Physical security Digital security Online security culture
Respondent: I think it has been classified, I just think it has not been enforced to such an extent where it is punishable by law or that you can lose your job. No the consequences should be well known to everybody. I think we choose not see this as a real threat that's why we are not taking it seriously, but in the meantime this is a real threat and to the National Security because you don't know what type of information another person is sharing. Uhm let's say personal information about the commander that may put him in disrepute with another faction or another individual. And people have been sharing with the medial all types of information about the military, now the question is that Cyberwarfare or information warfare so there is a territory between the two. Information has been used put onto a system where it was shared with other users and should be punishable by law, except if it's to one military person to another. But we should have uhm defence networks that you only operate within this network for communication or email, WhatsApp or so forth. We need to get the same type of network to protect this information that is shared, because what happens now is that you know that the email service is unprotected and the information attached to that email is confidential or restricted, yet you send it anyway because there is a need for it, so what do you do in such a case because you need to get that information across. There is no system that caters for this, and we all talk about the DoD network and emailing this information, but we have not received any confirmation that you will now register as an active DoD user, to use this domain, you see we have not received that information and it is sometimes problematic you understand	Lack of implementation Lack of consequences Vulnerable information Sharing information online Consequences of sharing information. DoD software Access to information Efficient information sharing Open-source applications Perception of sharing information Restricted information being shared on social media platforms Digital domain Unclear information Mode of communication Awareness of threats Open-source applications
Respondent: I will say yes I am, uhm however certain information I don't classify as important I will share. For example I will send a message over WhatsApp stating please plan for 1, 2, and 3. If I feel that I need to share information a little bit more closely I will send an email, because at least an email is a lit bit trickier as you need a password to get in. There are ways you need to go about retrieving that information. But WhatsApp is like social media, if you give it to one the one can share it with others without your permission, with an email you can at least determine who it was send to and actually track it.	Mode of communication Open-source applications Mode of communication Security awareness Communication over social platforms Information sharing

Meaning unit	Code extraction
	Emphasis on technology
Respondent: Yes, my wife is more paranoid than I am. But nonetheless, what I feel as a security risk and what my wife feels is security risks are two different things. For example she will tell me not to share my ID no with others, however, if I verify who's on the line and I pose a range of questions before I give my data out such as please tell me a little bit about yourself, why are you calling me and what is the purpose of this call. And seeing that they know who I am, you should have my details such as my email address I will ask them to confirm it for me. If they ask for the ID number I inform them that I cannot divulge such personal information, so I will ask them to please confirm the first 6 digits of my ID and then I will complete the rest, But yes I am paranoid.	Previous experience Security threats Online security practices Awareness of threats
Respondent: Well information is sensitive when it comes to the military domain uhm because everything you do is either made on decisions or a plan of action or information that you need to share with others to inform others on what your intent is or to deal with the risks and implications. So information is quite sensitive and needs to be controlled. You know when I got to air force base Makhado the whole issue was that everyone writes letters but nothing goes through registry, so when you look for a document, you can hardly find a document at registry anymore . You have to ask people do you remember this letter that has been written 3 years ago before my time. Then apparently this information would not be at registry, instead the information would be located on their laptops or at home or little flash drives. It took me more than a year to find the base standing orders as it was not on the T or H- drive nor in the registry, I got the document from an individual who had to re-write the new base standing orders. It is always difficult for incoming commanders to get certain tasks done or tracing the necessary information because there is no trace, unless it is registered at the registry. And that is why the registry will always play a pivotal role in safeguarding and securing information	Physical security digital security Sensitive information Old way of doing things Personal storage devices BYOD Unsecure information security practices Personal devices
Respondent: Yes it is, look there is systems that will do mustering at least every quarter and check-up, and however they don't know what information has gone through and things like that. For example if you get an email and print it, people don't put it through registry to be booked out. So that processes will have to be reformulated and restructured because we are still sitting with the old way of doing things and like I said we have not gone up with the times. Believe it or not in the past we received faxes and this went through registry and had to be booked out by registry. Now will get a fax most likely in the officer commanding's office, second in charge office, squadron commander's office, but this information does not get through registry. You will see in my minutes in the base command council this is one of the issues that we have picked up and we are trying to address it as well. I'm not saying its 100%, but whatever I get I push through the registry and book it out. And I try to make copies and say it's coming from registry but here are your copies and it's called the minutes by objects, it's called the MBO, an excel spread sheet that lays out the who's responsible for documents, the timeline, is it completed and why it is	Old way of doing things Generational divide Physical security Digital security The old way of securing information Security procedures BYOD Unclear procedures Emphasis on technology Trust in technology

Meaning unit	Code extraction
not completed and the remarks and then we colour code it. So once the document is in there and the file reference is also there you can trace it in the MBO and at registry to make the link. Yes commanders do follow certain procedures when it comes to information security. Information security is vital to the base but also organisation.	
Respondent: Well we on this security and defence programme so there are many descriptions in terms of security, but of you look at you know and now we not talking about uhm local national security, we talking more about personal security, well I would say it's mostly to safeguard your personal information and yourself as a person and to be free of fear and want. Well, that's basically what the constitution also says. But I think security means like whatever you do you don't have any threat to that information that will be utilised against you or secondly that the organisation is put in distrust that the information will be leaked and so forth. I think in essence security means more safeguarding of all aspects from information to personal information	Leaked information Distrust in one another Securing information Emphasis on technology
Respondent: I feel like being a human is sometimes being ignorant, ignorant in the fact that information can be used against you and that information is available on that domain. You may think that you have a firewall, Norton, MacAfee and passwords that you are secure, and yes to some extent you are, but personally I believe we are ignorant and we don't consider that this information can be used against yourselves. And I believe, yes additional guidelines should be given and more attention should be driven towards implementing, but also the execution part you know. I think if I was not exposed to cyber-related issues during the chief of the air force forums ours I would probably be as empty-headed as any normal to say agh it's just information, but when you are brought into perspective in terms of what that domain actually entails your paranoia becomes 100% more than what it was. I think that's how I currently am with information. I am carrying information with me the whole time as I don't want it to be laying in my room or whatever the case may be as the information is so sensitive and can be used against you. Yes, I think we can use more guidelines and the penalties for those types of things should be executed ion such a way where you won't lose your job but sensitised to you might lose your job if you do not conform to 1, 2 and 3 especially when it comes to social media because people think social media is there for people to know what's happening at work and it's not true. You work for an organisation that is very sensitive towards information and therefore, you must be careful in terms of the information you do share. We do have a form to complete which is a DD112 which is disclosure of information and a lot of people know about this form and have signed it, but you will not know how many people in this organisation divulges personal information by standing naked in front of a camera and you are an officer and then to put it on social media, whether it is just the top par or so. Uhm I personally think there's nothing wrong to have a picture of yourself to identify who you are, but it could also be used to profile you so to what extent do you do it and to what extend don't you. And if you don't do it your family does it. So they don't work for the DoD but how do you restrict from using Twitter, Facebook or Instagram.	Policies and guidelines Emphasis on technology Trust in technology Emphasis on technology Vigilance Emphasis on technology Trust among military member Open-source applications Unclear awareness information Previous experience Clear guidelines Social media practices More clear guidelines Awareness of guidelines Staff awareness of guidelines Social media information sharing No exposure to cyberthreats Secure password Physical security Emphasis on technology

Meaning unit	Code extraction
Respondent: Look the Internet is probably the only way now to steal information, in the old days you will have spies coming in to get into your office and then the human part of it was gathering information through sources. But from the work perspective besides human sharing state information is to hack into your network which is the DoD network, how secure this network is I am not too sure. I don't personally think it's that secure. The DENEL issue a couple of years ago could maybe give some more insight in terms of how light we take security and putting information and the availability of information on our systems. Uhm I believe that if my laptop that I carry around does not have sensitive information, it should not pose a risk, but it is accessible and can be remotely accessed through cyberattacks.	Violations in cyberspace DoD online systems DoD Software Access to information BYOD Physical domain Information sharing Cyberthreats Awareness of threats Digital space
Respondent: Like I said being a human and pushing the military away from the normal human being, uhm which is from a personal capacity uhm I don't think that I take it that seriously, but in my work environment I take it very seriously and I know the consequence and implications. But from a personal view people or hackers can build a personal profile of you and putting it out there and that's why I don't belong to Facebook or have a Facebook Profile, but I am on WhatsApp as it is more commonly used. So you can see my profile, but it doesn't say anything more on me. One thing that I do use is LinkedIn which is what I use for jobs and linking with other professionals in my field and sharing information and creating a network. I also see a lot of my other colleagues on LinkedIn that is of national security value in the sense that this information can be used either against or for. And you can use cyberattacks to get this information which is another form of warfare in my opinion and if you are not aware of it you may see your downfall.	Prior knowledge Open-source applications Access to information Emphasis on technology
Respondent: Well I would say according to SETA that MacAfee is the best antivirus software; however I don't feel that it is the best as it doesn't pick up all the viruses after updating it once a week or even once a month. I have cleared many viruses by using Kaspersky. But I think they cannot trace all viruses because the network is so big. I think it's bigger than any other network beside Vodacom, Cell C and MTN. No I don't think that the SETA Network is that secure.	DoD software Vigilance Own software Antivirus Regular software update Unsecure network Emphasis on technology
Respondent: Well I must say from the bases perspective. You can't just download an application; you need the administrator's password. And the Administrator is ICT-M. if they see there that this app must not be loaded onto your system they will not give permission. So what I have requested is because it goes onto the LAN system so what I have requested in order to have those apps is I requested for a stand-alone computer, so in other words I don't connect to the LAN system. But if I do want the app they will grant me a password and to come and do the	DoD software Vigilance Secure password Physical domain BYOD

Meaning unit	Code extraction
necessary and load the application. At the war college we had a choice between a work laptop or your own. If you use the work lap you will request access to the Internet and they will give you the administrator password, but only they know the password. And you can only use it in this domain. So I think from a security perspective the DoD is trying their best to deal with these issues.	Emphasis on technology
Respondent: Well first and foremost, training is considered the tool that we are currently using. The awareness campaigns that are used by the counter-intelligence officers, we do use them. Uhm and we do use them when we pick up certain trends and threats where we see there are security risks which they do present. And we have a threat analysis that we go through every year which we submit. Cybersecurity or information security is one the aspects we look at. Yet, like I said the biggest issue is that we do not have the personnel to do that continuously but uhm we do awareness campaigns during the officer commanding periods that we have, counter- intelligence presents then uhm with collaboration with SITA we schedule information security courses. There is a basic course and then there is an advance course and that is once a year for both courses, which means that we run two courses per year on the base so SITA comes down and presents it to us.	Lack of seriousness Training of members Awareness of threats Security risks Risk Security awareness courses Regular training
Respondent: Very easy and this is most probably where the policy does not make uhm…like when I speak on my base, I think I am able to speak on all other air force bases. At our base we don't have a SETA person sitting at the base dealing with information security. However, we have an ICT-M section but there primary reason for being there is not to look at firewalls and see if its secure, but rather to check if the systems are up and running and the reporting mechanisms, sending signals or if there is a password that needs to be replaced they will go through the password system to replace they will replace your password. The big issue is that we should have a cyber-technical expert on each base to make sure that the day-to-day activities are good and if he picks up something it should be immediately addressed and not wait for an inspection or wait until SETA comes and does a laptop site and checks that you not supposed to be on this site or there's too many pictures on this one and so forth. We should have SITA personnel at each base. Currently we have one person in Polokwane dealing with a range of Bases, he does not come out immediately and because they don't take cybersecurity seriously, that's why we have these little challenges on base levels.	Vigilance Awareness though training Access to information Personal devices Trust in policies
Respondent: I feel the SANDF cannot keep up with the rapid technology that is being introduced. For instances the use of drones can so easily be deployed, instead of sending 4 men with a vehicle to patrol the perimeter, the amount of fuel, time and impact on the environment and patrol the area for the fraction of the cost. In terms of cybersecurity I feel the DoD should draw in the youngsters from the techno world and to go look for them.	Generational divide Faster and more efficient mode of communication

APPENDIX N: CODE LIST FOR SHORT QUESTIONS IN THE CYBERSECURITY ORIENTATION QUESTIONNAIRE

Dominant Number of Codes From SANWC and SAMA Sample Groups			
Theme 1: Information Sharing on Best Practices Requires Implementation			
Code Count in Data for SAMA	**Code Count in Data for SANWC**	**Condensed and Combined Codes for SAMA and SANWC**	**Percentage of Respondents (SAMA and SANWC)**
Limited cybersecurity culture (12)	Low priority for cybersecurity (39)	Lack of policy implementation and cybersecurity awareness practices (34)	19%
Low priority given to cybersecurity (23)	Almost non-existent information security culture (3)	Low priority allocated to information security and promoting best practices (69)	38%
Not fully implemented (10)	Lack of awareness of cybersecurity (3)	There is an information security culture in the organisation (29)	16%
Important for organisation (3)	Lack of policy implementation and awareness (12)		
Basic form of policy and cybersecurity awareness (4)	There is security cybersecurity awareness in the organisation (17)	Limited information security awareness of best practices (26)	14%
There is awareness (5)	Limited cybersecurity culture (4)		
Limited information security culture (6)			
Relaxed and carefree cybersecurity culture (7)			
Lack of policy implementation (10)			

Theme 2: Cautionary Behaviour Is Linked To The Navigation Of Cyberspace			
Sub-theme 1: Cautiousness When Navigating The Internet			
Code Count In Data for SAMA	**Code Count In Data for SANWC**	**Condensed and Combined Codes for SAMA and SANWC**	**Percentage Of Respondents (SAMA and SANWC)**
Cautiousness (39)	Cautiousness (43)	Cautiousness when using the Internet (82)	45%
Carefree usage of cyberspace (22)	Practising cybersecurity behaviour (5)	Applying cybersecurity practices when navigating the Internet (20)	11%
Aware of threats (4)	Distrusting of cyberspace and others (18)	Vigilant about information on cyberspace and sharing information with others (22)	12%
Good cybersecurity practice (15)	Using the Internet only when needed (7)	Using social media to update myself about matters (5)	3%
Social media usage (3)	Using the Internet for social media (2)	Using the Internet only when required (19)	10%
Use only when needed (12)	Limited awareness (2)	Relaxed security behaviour when using the Internet (24)	13%
Theme 3: Cybersecurity Training and Education as a Way to Enhance Security Measures			
Sub-theme 1: Cybersecurity Awareness Training for the Entire Organisation			
Code Count in Data for SAMA	**Code Count in Data for SANWC**	**Condensed and Combined Codes for SAMA and SANWC**	**Percentage of Respondents (SAMA and SANWC)**
Cybersecurity awareness training and education (52)	Cybersecurity awareness training (47)	Cybersecurity awareness training and education for military members (99)	54%
Stricter security measures (16)	Stricter security measures (7)	Employment of stricter security measures through monitoring the Internet and employees (48)	26%
Monitor the Internet and military officers (16)	Monitoring (9)	Implementation of cybersecurity policies (10)	5%
Using own software and developing policies (2)	Implementation of policies (4)		
Policy implementation of cybersecurity (4)			

APPENDIX O: QUALITATIVE AUDIT TRAIL (REFLECTION ON RESEARCH PROCESS)

Identification of the research problem	During my PhD journey, it was rather challenging to confirm what the actual research question will be due to the field still emerging. As I reviewed literature regarding cybersecurity my understanding of the topic developed and became more evident.
The research proposal	I needed to construct a research proposal which was reviewed several times before submission was made to the Ethics Committee. In addition, the researcher also presented the proposal in- front of a faculty Committee who provided input. Moreover, all the methodological considerations were noted and suggestions were made so that the researcher is able to engage in PhD study that shows methodological rigour.
The search for a theoretical framework	The securitisation framework appeared to be most challenging yet. I was not prepared to deal with the complexities of the framework as it is challenging to integrate the human element into a theoretical stance that is driven by power and the state. Understanding the context of the theoretical framework was challenging. However, as the research progressed, the variables within the theory became easier to understand. This allowed for the researcher to map out the all the actors in the security process.
Reviewing the literature	The literature review was also one of the most challenging chapters in the research process. One of the main reflective processes that I underwent was to focus my research question. This facilitated my understanding of what I want to achieve in the research process. There was a lack of literature focusing on cybersecurity in the SANDF context. This made the entire literature search process challenging as I needed to relate international literature focusing on the armed forces to the SA context. Furthermore, literature focusing on cybersecurity is also lacking in a SA context.
Designing a research framework	The next step in the research process was to select a sound methodological approach to guide the research process. The data-collection strategy involved two phases which each a defining approach. Phase 1 was qualitative and Phase 2 was quantitative. The mixed-methods research design was the best possible option considering the research question and the emerging topic of interest.
The interview schedule	I made use of semi-structured interviews in order gauge the perceptions of cybersecurity among military officers. The questions were constructed based on the literature review that has been carried out. Due to the timeframe of the study, the interview questions could not be piloted or tested. Furthermore, I made use of peer reviewed literature on cybersecurity in organisation and adapted it according to the military context. The interview schedule also assisted the me in construction questionnaire items for the COQ.
Accessing the sample population groups	The next step was to access the sample population groups. The first sample population was the SANDC. This sample consisted of senior military officers and was the easiest to access. This was also the site where 10 semi-structured interviews were conducted. The second sample group was located in the Western Cape and the researcher needed to use research assistants located at the SAMA to administer the questionnaire to students. Note the SAMA population groups

	consisted of junior to senior officers. The researcher created an administration guide in order for the research assistants to be aware of the data-collection processes and the potential questions participants may ask them. This needed to be implemented as the researcher was not present to collect data. The last sample population group located in Phase 2 of the study focused on administering the COQ at the SANWC. Accessing this sample proved to be challenging as the researcher should be have been done with data collection in his second year. Instead this sample population group could only be access in the third year of the researcher's PhD. I maintained all ethics throughout the data-collection process.
The transcription and data-cleaning process	The findings of the interview needed to be transcribed from audio recordings so that the I was able to engage in the analysis process. The researcher started the transcription process after the first interview. During the process of transcription, the researcher needed to reflect on the content and process. The researcher made notes about his reflection so that he could be aware of his ideas and prejudices. In addition, transcribing the first interview also allowed the researcher to take note of the interview process and questioning style used. This enabled the researcher to be aware of his position when entering the second interview. The same process was followed throughout the transcription process where the researcher needed to be actively involved in the data transcription process and being in touch with the narratives. This also allowed the researcher to be fully immersed in the analysis of the qualitative narratives. In terms of the data collected from the SANWC and SAMA, I needed to actively engage with the cleaning process as avoid any discrepancies in how items are being coded.
The analysis of interview data and COQ findings	I used content analysis for the interview data. Several steps needed to be completed for the researcher to extract the themes for Phase 1. Narratives linking to each theme needed to be presented as well. The COQ scale items were constructed based on the findings of the interview data. Once administered, I needed to engage with the analysis process of the scale items, by focusing on the frequency distributions and overall percentages. It should be noted that the short questions listed in the COQ also needed to be analysed. I used thematic analysis as he wanted to provide a general view of the thematic points that respondents presented.
The writing up of the results	With the writing up of the findings I needed to show his academic voice so that the interpretations made came from a point where literature informed the argument. In addition, I needed to be aware that his own preconceived ideas will not taint the findings retrieved in Phase 1 or Phase 2. Emphasis needed to be placed on reflection throughout this process as it could have been easy to get lost in the data for the two phases. The researcher needed to engage in a structure whereby it was able to logically apply the findings and literature in a discussion format. Furthermore, the research supervisors also checked and re- checked the presentation of results and the discussion.

APPENDIX P: PROCESS OF DATA ANALYSIS

Preparation phase for the data-collection technique used	
Questions	**Answers**
Data collection	
How do I collect the most suitable data for my content analysis?	I utilised the semi-structured interviews to explore the narrative related to cybersecurity. Interviews were used to explore the narrative regarding cybersecurity.
Is this method the best available to answer the target research question?	Yes, therefore semi-structured interviews were used as an inductive approach to the study. Engaging with the narratives about cybersecurity would and did answer the research question.
Should I use either descriptive or semi-structured questions?	Semi-structured interviews were used as they linked up with the inductive approach.
Sampling strategy	
What is the best sampling method for my study?	Purposive sampling was used to recruit the sampling population.
Who are the best informants for my study?	Senior South African military officers from the SANDC were targeted as the primary information site.
What criteria should be used to select the participants?	Criteria included: senior-ranking officers and a knowledge base of cybersecurity.
Is my sample appropriate?	The sampling technique used was appropriate for answering the research question and in alignment with qualitative content analysis.
Is my data well saturated?	Saturation in the information was met in the 8th interview, after which no new data emerged.
Sampling strategy	
What is the unit of analysis used in the study	The units of analysis were military officers in training at three identified military training institutions.
Is the unit of analysis too narrow or too broad?	The units of analysis were broad as senior and junior military officers were selected at the SANDC, SAMA and the SANWC.

Organisation phase of the study	
Is there any overlap between categories?	Yes. Some of the categories in the coding and meaning making units can seem interlinked. For example, the process of integrating technological devices can take on a meaning of having both procedural and behavioural facets.
Interpretation of the findings	
What is the degree of interpretation in the analysis?	The degree of interpretation of findings are extensive. I engaged with the participant excerpts by specifically highlighting specific aspects that link to cybersecurity in the SANDF.
How do I ensure that the data accurately represents the information that the participants provided?	An audit trail, along with this checklist, ensured that there was quality assurance in validity and reliability.
Reporting results	
Can the reader evaluate the transferability of the results (are the data, sampling method and participants described in detail)?	Yes, the data, sampling method and participants were detailed in chapters 4 of the study. This detail in can be found in chapter 4 where the participants are discussed in detail.
Are quotations used systematically?	Yes, quotations are used based on their relevance and importance in the analysis phase.
Are the results reported systematically and logically?	Yes, the process and actual findings are separated and comprehensively detailed in chapters 5 and 6
How are connections between the data and results reported?	Findings can be linked to literature and the theoretical framework. This was performed in chapters 5 and 6
Are there similarities within and differences between categories?	Yes, there are, specifically concerning awareness and best practice and they are presented.
Is scientific language used to convey the results?	APA standards are complied with in reporting findings.
Reporting analysis process	
Is there a full description of the analysis process?	Yes, the process of analysing the data can be found in section 4.7.1.1 which emphasises the application of the technique.
Is the trustworthiness of the content analysis discussed based on some criteria?	This is discussed in relation to the validity and reliability of the data.

APPENDIX Q: ADMINISTRATION GUIDELINES FOR THE CYBERSECURITY ORIENTATION QUESTIONNAIRE

UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvennoot • your knowledge partner

The questionnaire should be administered by the designated data collector in the below-mentioned manner.

- Make sure that the members are all neatly seated and are provided with a pencil or pen with which they are to complete the consent form and questionnaire.
- Introduce yourself and make them feel at ease. Also explain to them that you will be providing them with both a consent form and questionnaire that needs to be completed, but you will explain exactly how to do so. Make sure they are relaxed and emphasise that the questionnaire is not a test.
- Please familiarise yourself with the content of the information sheet and consent form, so that you may summarise the information sheet when asking them to complete a consent form. The most important aspects to indicate on the consent form are the following: they are completing a consent form for ethical purposes, this is voluntary but their participation will be greatly appreciated, there is no harm or benefit from participating, except that the information may improve their outlook on cybersecurity in the organisation. The consent and questionnaire will not be linked (please make sure that you collect the consent form and put it in an envelope before letting them complete the questionnaire. This will ensure confidentiality of information), the results will be analysed as a group and the information on the consent form is only for ethical purposes.
- Once the consent forms are completed by members, please collect them and store in an envelope indicating the following details: Date, amount of members, place in which administration is taking place and 'consent forms'.
- Hand out the questionnaire to the members and read the information provided on the cover of the questionnaire (instructions), where necessary explain in your own words, as to ensure that they all understand both the purpose and need for the questionnaire. Answer any questions they may have concerning

this information. It should be fairly straight forward. Please ensure that you emphasise that they complete all the sections.

- Section A is biographical information and members are encouraged to complete in full.
- Section 1: ***Information-Sharing Culture*** has options for the different items such as "Strongly Disagree, Disagree, Agree, and Strongly Agree". Please ask them to make sure they indicate the relevant action, either "Strongly Disagree, Disagree, Agree or Strongly Agree" if they do so. If not marked, it will be interpreted as they do not agree or strongly agree to those items. Also they need to indicate whether they strongly disagree or disagree with some of the items.
- Please also indicate that each section has a short question section which they are encouraged to complete.
- Section 2***: Security Orientation*** has options for the different items such as "Strongly Disagree, Disagree, Agree, and Strongly Agree". Please ask them to make sure they indicate the relevant action, either "Strongly Disagree, Disagree, Agree, and Strongly Agree" if they do so. If not marked, it will be interpreted as they do not agree or strongly agree to those items. Also they need to indicate whether they strongly disagree or disagree with some of the items.
- Section 3***: Views on Cybersecurity*** has options for the different items such as "Strongly Disagree, Disagree, Agree, and Strongly Agree". Please ask them to make sure they indicate the relevant action, either "Strongly Disagree, Disagree, Agree, and Strongly Agree" if they do so. If not marked, it will be interpreted as they do not agree' or strongly agree to those items. Also they need to indicate whether they strongly disagree or disagree with some of the items.
- Section 4***: Cybersecurity posture in the organisation*** is the last section of the questionnaire and has a short question section that follows. Section 4 has options for the different items such as "Strongly Disagree, Disagree, Agree, and Strongly Agree". Please ask them to make sure they indicate the relevant action, either "Strongly Disagree, Disagree, Agree, and Strongly Agree" if they do so. If not marked, it will be interpreted as they do not agree or strongly agree to those items. Also they need to indicate whether they strongly disagree or disagree with some of the items.

APPENDIX R: TERMINOLOGY LIST FOR SEMI-STRUCTURED INTERVIEW

UNIVERSITEIT•STELLENBOSCH•UNIVERSITY
jou kennisvennoot • your knowledge partner

Cybersecurity: "*Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights*" (Craigen et al., 2014, p. 13).

Cyberthreat: "*A cyberthreat refers to anything that has the potential to cause serious harm to a computer system. A cyberthreat is something that may or may not happen, but has the potential to cause serious damage*" (Techopedia, 2022, para. 2).

Cyberattack: "*A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft*" (Techopedia, 2019, para. 2).

WI-FI: "*Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet. It allows these devices--and many more--to exchange information with one another, creating a network"* (Cisco, 2022).

Open-Source Software Tools: "*Open-source tools are software tools that are freely available without a commercial license. Many different kinds of open-source tools allow developers and others to do certain things in programming, maintaining technologies or other types of technology tasks*" (Techopedia, 2017, para. 2).

APPENDIX S: PHASE 1 CODES THAT INFORMED PHASE 2 OF THE STUDY

Codes	Qualitative themes	COQ dimensions
Violations in cyberspace	Knowledge production and training focusing on cybersecurity awareness	Cybersecurity posture in the organisation: Dimension 4
Violating organisational trust		
Awareness initiatives		
Awareness through education		
Lack of seriousness		
Proactive measures		
Trust in technology	Challenges of trust with technology and members	The officers' view of cybersecurity: Dimension 3
Trust in each other		
Trust in the organisation		
Uncertain of policies and directives		
Mutual trust	The construction of a digital culture among members	Information-sharing culture in the organisation: Dimension 1
Refusal to adapt		
Different generations		
Online security		
Personal devices		
Unclear awareness procedures		
Limited understanding		
Implementation		
Limited understanding		
Older means of communication		
More fast-paced		
Expanding gap		
Open-source applications		
Information security		
Outdated technology		
Vigilance	The view on cyberthreats is constructed based on experiences in the physical domain	Security orientation among military officers: Dimension 2
Prior knowledge		
Physical security vs digital security		
Removal of devices		
DoD online systems		
Access to information		

APPENDIX T: HOW ELEMENTS OF SECURITISATION THEORY INFORMED PHASE 1 AND PHASE 2

Elements of ST	Phase 1
Securitising actor	Cybersecurity posture: Questions focused on how military officers verbalised the threat and the significance placed on cyber threats in the organisation. Questions ranged from the military officer's perspective to what they think the organisation does. Furthermore, this element of ST focuses on the role of the actor that initiates the speech act. Therefore, the essence was on the role of security and its importance for military officers: The questions are directed as follows: • What is your view on cybersecurity? • What is cyberspace/Internet in your opinion? • What does this mean for you? • What are your views on cyberthreats? • What cyberattacks are you aware of? • What is your understanding of cyberthreats cyberthreats/attacks? • What are your thoughts on equipping all military officers with the technical skills to combat cyberthreats? • Given the importance of cyberthreats pose, why do you think there is a lack of awareness of cyber-related issues in the organisation? • How would you describe the nature of communication on cybersecurity that is taking place in the organisation? • In your opinion, should there be collaboration between cyber commands and units? • Do you feel that the guidelines concerning cybersecurity currently under review are limiting your work? • Do you consider this a space that needs to be controlled by the armed forces or other state-affiliated actors? • How would you approach this domain of warfare? • Do you feel that cyber space should be monitored at work?
Referent Object	Security orientation: Questions focused on how military officers perceived the threat and what needs to be protected In terms of their information: • Are you a security conscious individual? Explain • What are your views on information security within the organisation? • How do you secure information at your organisation? • What does the term "security" mean for you? • In your opinion is there a culture of cybersecurity within the organisation? • How would you describe this culture of cybersecurity within the

Elements of ST	Phase 1
	organisation? ● How often do you share organizational information with colleagues? ● What is your opinion on sensitive information that is being shared with colleagues'? ● Are you aware of technology that may be prone to hacking in your workplace? ● What is your perception on browsing websites that are unprotected on your work devices? ● What are your thoughts on downloading documents from the Internet on your work device? ● How do you feel about state documents that contain sensitive information being taken home on personal devices? ● How do you assess your cybersafety?
Elements of ST	**Phase 2: Cybersecurity Orientation Questionnaire**
Securitising actor	**Dimension 3**
Referent Object	**Dimensions 1 and 2**