

**Wielding the Double Edged Sword in The Cyber Domain – The Utility of
Internet Securitisation in Countering Islamic State Cyberjihad**

By

Nikita Hiralal

Thesis presented in partial fulfillment of the requirements for the degree of Master
of Arts (International Studies) in the Faculty of Arts and Social Sciences at
Stellenbosch University



Promotor: Prof. Pieter Fourie

March 2017

Declaration

By submitting this thesis 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 obtaining any qualification.

Date: March 2017

Abstract

The astronomical success and ubiquity of the Internet has resulted in the manifestation of new interdependencies and vulnerabilities in the international system. Widespread access and the decentralised structure of its architectural framework has reduced barriers to participation, meaning the cyber-domain exhibits an even landscape that has served to empower non-state actors. Security threats online have created new challenges to the international community, as the multiplicity of actors and dispersed technical infrastructure of the Internet mandates transnational responses and cooperation amongst states, as well as public-private collaboration. Pronounced integration of the Internet into all facets of life has led it to being deemed a critical infrastructure, and the assertion that ensuring its safety is essential so as to preserve the security and economic interests of the nation state. Following its unprecedented success in 2014, the jihadist organisation Islamic State (IS) has supplanted al Qaeda as the greatest contemporary terrorist threat. IS has been unparalleled in its accomplishments, securing substantial territories in Iraq and Syria and rallying thousands to join its cause. Much of IS's notoriety and appeal has been attributed to its capacity to unleash an online propaganda campaign and amass phenomenal support from the global populace, that has yet to be realised by any other terrorist groups. Recent developments in the fight against IS demonstrate that the group's prospects for maintaining its Caliphate are tenuous at best, as global efforts have resulted in military setbacks and significant loss of territory. However, this study argues that military efforts will not suffice, as greater integration of the Internet into IS operational strategies has meant the group has been able to adopt a horizontal organisational structure that will allow it to continue the global jihad and ensure its ideology survives. This study applies the Copenhagen School's Securitisation Theory to the single case study of IS and cyberjihad in an effort to explore how securitisation can serve to allow for more effective countermeasures to be adopted in efforts to prevent terrorist exploitation of the Internet. The main research question informing this study seeks to determine the utility of Internet securitisation in efforts that seek to mitigate the threat of IS and cyberjihad. The primary research question is supplemented by the three sub-questions that aim to determine; (1) how cyberjihadists have sought to exploit the Internet; (2) what measures have been taken to counter cyberjihad and to what degree have these measures proven successful; and (3) what the disadvantages and benefits of securitisation of the Internet are, in terms of the international security context. Findings suggest that the uptake of extraordinary measures, validated through a successful securitisation, will provide the facilitating conditions necessary for greater transnational and public-private cooperation and the additional resources required to develop more salient strategic communication measures in the battle of ideas.

Opsomming

Die astronomiese sukses en alomteenwoordigheid van die Internet het gelei tot die manifestasie van nuwe interafhanklikhede en kwesbaarhede in die internasionale stelsel. Wydverspreide toegang en die gedentraliseerde struktuur van die Internet se argitektoniese raamwerk verminder struikelblokke tot deelname. Dit beteken dat die kuber-domein 'n gelyke speelveld geword het om nie-regerings akteurs te bemagtig. Aanlynse veiligheidsbedreigings het nuwe uitdagings vir die internasionale gemeenskap geskep, siende dat die veelvoudigheid van akteurs en verspreide tegniese infrastruktuur van die Internet transnasionale reaksies en samewerking tussen state sowel as openbare-private samewerking bevel. Prominente integrasie van die Internet in alle fasette van die lewe het daartoe gelei dat dit geag word as 'n kritieke infrastruktuur, en die bewering dat die versekering van veiligheid noodsaaklik is ten einde die veiligheidsbelange sowel as ekonomiese belange van die nasie-staat te bewaar. Na aanleiding van hul ongekende sukses in 2014, het die jihadistiese organisasie, Islamitiese Staat (IS), Al-Qaeda vervang as die grootste hedendaagse terroriste bedreiging. IS is ongekend in hul prestasies - die beveiliging van aansienlike gebiede in Irak en Sirië en die mobilisering van duisende om by hul stryd aan te sluit. Baie van IS se populariteit en appèl word toegeskryf aan hul vermoë om 'n aanlynse propaganda veldtog te loots wat fenomenale ondersteuning van die globale bevolking verkry het, 'n prestasie wat nog oortref moet word deur ander terroriste groepe. Onlangse verwikkelinge in die stryd teen IS toon dat die groep se vooruitsigte om hul Kalifaat te handhaaf broos is op sy beste, aangesien globale pogings gelei het tot militêre terugslae en aansienlike verlies van grondgebiede. Nietemin, hierdie studie argumenteer dat militêre pogings nie voldoende is nie, aangesien groter integrasie van die Internet in IS se operasionele strategieë die groep instaat gestel het om 'n horisontale organisatoriese struktuur aan te neem om sodoende voort te gaan met hul globale jihad en te verseker dat hul ideologie oorleef. Hierdie studie pas die Kopenhagen-skoolse beveiligingsteorie toe op die enkele gevallestudie van IS en kuberjihad in 'n poging om te ondersoek hoe beveiliging kan dien om voorsiening te maak sodat meer doeltreffende teenmaatreëls aangeneem kan word in pogings om terroriste uitbuiting van die Internet te voorkom. Die primêre navorsingsvraag van hierdie studie poog om die nut van Internet-beveiliging in pogings wat daarop gemik is om die bedreiging van IS kuberjihad te versag te bepaal. Die primêre navorsingsvraag word aangevul deur drie sub-vrae wat daarop gemik is om te bepaal; (1) hoe kuberjihadiste probeer om die Internet uit te buit; (2) watter maatreëls getref is om kuberjihad teen te werk en tot watter mate is hierdie maatreëls suksesvol bewys; en (3) wat die nadele en voordele van beveiliging van die Internet is, in terme van die internasionale veiligheidskonteks. Bevindinge dui daarop dat die opname van buitengewone maatreëls, bekragtig deur 'n suksesvolle beveiliging, sal die fasilitering van toestande wat nodig is vir aansienlike transnasionale en openbare-private vennootskappe en die bykomende hulpbronne wat nodig is om meer belangrike strategiese kommunikasie maatreëls in die stryd van idees te ontwikkel voorsien.

Acknowledgements

First I would like to thank Professor Pieter Fourie for his patience and for agreeing to be my supervisor despite his unfamiliarity with the subject matter of this study. Above all else, I would like to thank my amazing parents, Melanie and Mukesh, for their love and support during this process. You have provided me with everything and more throughout my life and I am privileged and grateful for this, the greatest gift you could ever give me, my education.

List of Tables & Figures

Table 1: Cyber-threats – Typology	5
Table 2: Dynamics of Securitisation in accordance to Sector.....	58
Table 3: Selected international, government and civil society CVE initiatives.....	85
Figure 1: Motivations Behind Registered Cyber-Attacks for March 2016.....	9
Figure 2: Motivations Behind Registered Cyber-Attacks for April 2016.....	9
Figure 3: Freedom on the Internet – Country Comparison	27
Figure 4: Timeline of IS attacks outside of Iraq and Syria	71
Figure 5: IS territorial losses between January 2015 and July 2016.....	81

Abbreviations

AITNS	Advanced Information and Telecommunications Network Society
APEC	Asia-Pacific Economic Cooperation
AQI	al Qaeda in Iraq
Centcom	US Central Military Command
CERT	Computer Emergency Response Team
CoE	Council of Europe
COPRI	Copenhagen Peace Research Institute
CSCC	Centre for Strategic Counter-Terrorism Communications
CTIRU	Counter-Terrorism Internet Referral Unit
CTITF	Counter-Terrorism Implementation Task Force
CVE	Countering Violent Extremism
DNS	Domain Name System
DOD	Department of Defense
GGE	Group of Governmental Experts
HTTP	Hyper Text Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IHS	Information Handling Services
IR	International Relations
IS	Islamic State
ISOC	Internet Society
ISP	Internet Service Provider
ITR	International Telecommunications Regulations
ITU	International Telecommunication Union
P2P	Peer-to-Peer
PCCIP	President's Commission on Critical Infrastructure Protection
SCO	Shanghai Cooperation Organisation
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development

UNDP	United Nations Development Programme
UNESCO	United Nations Education, Scientific and Cultural Organisation
UNHROHC	United Nations Human Rights Office of the High Commissioner
UNODA	United Nations Office of Disarmament affairs
UNODC	United Nations Office on Drugs and Crime
WCIT	World Conference on International Telecommunications
WEF	World Economic Forum
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organisation
WSIS	World Summit on the Information Society
WTO	World Trade Organisation
WWII	The Second World War
WWW	World Wide Web

Table of Contents

DECLARATION	I
ABSTRACT	II
OPSOMMING	III
ACKNOWLEDGEMENTS	IV
LIST OF TABLES & FIGURES.....	V
ABBREVIATIONS.....	VI
CHAPTER 1: INTRODUCTION	1
BACKGROUND & RATIONALE:	1
<i>The Internet & International Relations:</i>	2
<i>Security in the Information Age:</i>	4
<i>Islamic State & Cyberjihad:</i>	10
PROBLEM STATEMENT:	14
RESEARCH QUESTIONS:.....	14
THEORETICAL & CONCEPTUAL FRAMEWORK – SECURITISATION THEORY:	15
RESEARCH DESIGN & METHODOLOGY:	16
SUMMARY OF CHAPTERS:	17
CHAPTER 2: THE INTERNET – GOVERNANCE MODALITIES & ITS PLACE IN THE INTERNATIONAL SECURITY CONTEXT	19
INTRODUCTION:.....	19
INTERNET GOVERNANCE:.....	19
<i>Delineation of Internet Governance:</i>	19
<i>Standardization and Protocol Governance:</i>	20
<i>Structural Management Governance:</i>	21
<i>Intellectual Property Governance:</i>	23
<i>Internet Security Governance:</i>	23
<i>Internet Filtering Governance:</i>	24
<i>Discourse Pertaining to the Future of Internet Governance:</i>	28
THE INTERNET IN THE INTERNATIONAL SECURITY CONTEXT:	33
<i>UN Resolutions Related to Cybersecurity:</i>	35
<i>UN Resolutions Related to Information Security:</i>	37
CONCLUSION:	39

CHAPTER 3: THEORETICAL GROUNDING – THE COPENHAGEN SCHOOL’S SECURITISATION THEORY	42
INTRODUCTION:	42
SECURITY STUDIES – DEVELOPMENT, DEBATES & THEORETICAL APPROACHES:	42
<i>The Development of Security Studies:</i>	42
<i>Epistemological Debates in Security Studies:</i>	47
<i>Mainstream Theoretical Approaches in Security Studies:</i>	49
SECURITISATION THEORY:	53
CONTEMPORARY SECURITY CONTEXT:	61
CONCLUSION:	66
CHAPTER 4: TERRORIST EXPLOITATION OF THE INTERNET – THE CASE OF ISLAMIC STATE AND CYBERJIHADIST STRATEGIES	68
INTRODUCTION:	68
BACKGROUND OF ISLAMIC STATE:	69
CONTEXTUALIZATION OF CYBERJIHADIST STRATEGIES:	72
<i>Propaganda Creation and Dissemination:</i>	72
<i>Recruitment and Radicalization:</i>	75
<i>Strategic Operations – Communication, Organization & Planning:</i>	77
<i>Operational Training:</i>	79
<i>Fundraising:</i>	79
COUNTER-TERRORISM EFFORTS PERTAINING TO EXPLOITATION OF THE INTERNET AND CHALLENGES TO THEIR SUCCESS:	80
<i>Countermeasures to Prevent Terrorist Exploitation of the Internet:</i>	82
<i>UN Countermeasures to prevent Terrorist Exploitation of the Internet:</i>	85
<i>Factors Undermining Effective Internet Related Counter-Terrorism Efforts:</i>	87
APPLICATION OF THEORY – SECURITISING THE INTERNET:	92
<i>Identifying Security Discourses and Threat Construction:</i>	92
<i>Acceptance of the Securitising Move by a Relevant Audience:</i>	96
<i>Extraordinary Measures:</i>	98
SHORTCOMINGS AND BENEFITS OF SECURITISATION IN COUNTERING CYBERJIHAD:	99
CONCLUSION:	104
CHAPTER 5: CONCLUSION	106
SUMMARY OF THE STUDY:	106
SOLVING THE RESEARCH QUESTIONS:	108
AREAS FOR FUTURE RESEARCH:	110
BIBLIOGRAPHY:	112

CHAPTER 1: Introduction

Background & Rationale:

The proliferation of the Internet has demonstrated the most outstanding growth and development experienced by modern information and communication technologies (ICTs), such as mobile phones and email. In recent decades the contemporary international system has undergone drastic reform as a direct implication of globalisation. The driving force behind the advent of this new order has been the growth of the Internet. The development of the Internet can loosely be explained as having developed out of the obscurity of an internal military experimental network, to the point where it has served to "...transfor[m] commerce, created social and cultural networks with global reach, and become a surprisingly powerful vehicle for political organization and protest alike..." (Negroponte *et al.*, 2013:ix). The astronomical scope of the Internet as a global system and network for communication is demonstrated in that recent statistics published by the International Telecommunication Union (ITU),¹ have estimated that "...3.2 billion people are now using the Internet..." (ICT Data and Statistics Division, 2015:1).

As the culmination of technological progress and infrastructure deployment allow the Internet to diffuse at a spectacular and yet still increasing speed, growing interconnectedness in the 21st century has meant the world is moving ever faster towards becoming a digital society. Persisting inequalities in the international system have given rise to a 'digital divide', typified by access to the Internet and usage. However costs of ICTs have continued to shrink, rendering them "...widespread and decentralized, reaching far beyond the political and economic elites of western societies..." (Eriksson & Giacomello, 2007:1). As such, for the first time in humanity's history, advances in ICTs are within the potential reach of much of the global populace.

The Internet is defined as a global computer network, which boasts electronic communication tools and provides electronic information and media facilities. Interconnected communication between computers and networks on the Internet is made possible by the standardised protocol for file transfers, the Hypertext Transfer Protocol (HTTP). The World Wide Web (WWW), also referred to as the Web, denotes the global network of "...interlinked files

¹ The United Nations (UN) specialised agency for information and communication technologies.

which can be located using the HTTP protocol...” or simply put, read by any computer connected to the Internet with a Web browser (Gauntlett, 2000:227). Throughout this study, the prefix ‘cyber’ is used to indicate a characteristic pertaining to information technology and the Internet in its capacity as an electronic communications network. The phenomenology of cyberspace is described as the amorphous conceptual terrain that has emerged isochronously with the advance of the Internet. It is the domain of virtual interaction where information hardware and software, users, communication networks and application programmes converge. Cyberspace is a “...venue that allows users to engage in activities conducted over electronic fields whose spatial domains transcend traditional territorial, governmental, social, and economic constraints...” (Choucri, 2012:6). Although the concepts are concatenated, it is important to recognise the distinction between cyberspace and the Internet, with the latter denoting the circuitry and connectivity needs requisite to both access and navigate the cyberspace arena of interaction. Without the Internet there would be no cyberspace.

The rapid spread of the Internet has wrought irreversible changes in the global environment and all aspects of life. Because of its permeability and the perceived benefits of increased connectivity, public and private actors alike have progressively sought to shift their operational systems online. “Governments, academic institutions, private corporations, armed forces and individuals now share a common, global infrastructure...” which owing to “...the pervasiveness of the Internet has created significant personal, organizational, and infrastructural dependencies that are not confined by national borders...” (de Borchgrave *et al.*, 2000:1). Global dependency on the Internet is evident in the manner that it has been so seamlessly integrated into daily operations ranging from providing critical security structures, databases for medical records, facilitating financial transactions, social interaction and even something as mundane as allowing for net-enabled household appliances. The assimilation of technology and the Internet has led to the creation of a “...globally immersive environment of cyberspace that encompasses the entire connected world...” (Kingsmith, 2013:1). Increased dependence on ICTs and our transition towards an information society has led humanity into a new epoch of global existence, widely regarded as the Information Age.

The Internet & International Relations:

Amidst this Information Revolution, the domain of International Relations (IR) has not remained untouched. The ubiquity and non-transparency of the Internet has had a tumultuous effect on IR notions of power, security, borders and influence. As these understandings must

change in an effort to reflect contemporary realities, so too will theory, policy and practices of IR be reshaped (Choucri, 2012:3). The most discernible impact resultant of the spread of the Internet, points to the manner in which cyberspace has empowered non-state actors and the individual. The higher capacity for organising and communicating afforded by the Internet has led to a paroxysm in global civil society, as the Information Age has made it "...easy to form virtual communities, mobilise support, and effect political change..." (Deibert & Rohozinski, 2008:123). The manifestation of global civil society has both revolutionised mass protest and invigorated opposition movements as the combination of technology and the Internet has allowed for local politics to be catapulted into the international forum. What's more, states remain a latecomer to cyberspace and they are not the primary actor in the virtual domain, as its construction, development and the operation of the Internet are ascribed to the private sector. These new and distributed changes have served to challenge traditional notions of sovereignty and political authority.

Due to the positivist, state-centric focus adopted by the major academic schools of IR, much of the theory in the discipline sits uncomfortably with the changes introduced by the rise of the Internet and cyberspace.² For the past two decades, the theme of the Internet has featured prominently in intellectual inquiries and on research agendas (Dahlgren, 2005:147), whilst the topic of its perceived impact has been hotly contested by the various tenets of IR. Much of the academic debate on the impact of the Internet has focused on issues of sovereignty. Early authors on the subject were of the optimistic view that as the Internet continued to reduce barriers to participation it would increasingly undermine the sovereignty of the state, which would not be able to assert its authority in the virtual domain (Barlow, 1996). However, this argument has come under increasing challenge as states have demonstrated a capacity to actively assert their authority in cyberspace by regulating and censoring online content (Goldsmith & Wu, 2006).

An evaluation of the impact of ICTs, the Internet in particular, on state sovereignty is beyond the scope of this research. Instead, this investigation posits that the Internet has played an insurmountable role in the evolving and broadening of the public sphere "...by bringing in a diversity of actors and their perspectives..." and by fostering interactions "...that change the identity of the actors and their interests in global politics..." (Singh, 2013:6). Although the

² Non-state actors cannot be excluded from analysis. Not only has the Internet reduced barriers to participation but also its operations and regulation lie with the private sector.

effects of the Internet should not be exaggerated, it would be ludicrous to dismiss the transformational impact it has had on conventional understandings of power in terms of the capabilities of actors. Within the field of IR, the significance and impact of these changes are most evident in the intersection of the Internet with security issues.

Security in the Information Age:

During the early 1990s, shifting geopolitical conditions and new developments in technology led to the introduction of a new notion in computer sciences. The term ‘cybersecurity’ was first used as a technical conception to describe the insecurities that arose from the use of networked computers (Hansen & Nissenbaum, 2009:1155). Increased penetration and growing connectivity of the Internet have since drastically altered understandings of cybersecurity as proponents of international affairs have systematically warned of the potentially disastrous effects posed by ICTs and digital technologies. Whilst the benefits of interconnectedness afforded by the Internet are incalculable, its pervasiveness has “...created significant personal, organizational, and infrastructure dependencies that are not confined by national borders...” (de Borgrave *et al.*, 2000:i). What’s more, the greater inclusion and capabilities granted to individuals and non-state actors by the Internet have revealed new threats to state security interests, which this study refers to as cyber-threats. The term ‘cyber-threat’ denotes the potential for the unauthorised access to a computer device, system or network through the use of ICTs, with the intention to either damage or disrupt the target. The act of gaining unauthorised access to a computer or system is referred to as ‘hacking’.

The Internet maintains a number of qualities that are of great salience to state security interests,

particularly the fact that it allows unauthorised users to invade critical computer facilities around the world; its capacity to empower individuals and small groups by allowing them to transmit information across the globe on a secure basis by means of encryption and the fact that it gives everybody access to powerful weapons

such as tools for hacking that are readily available online and that are becoming increasingly user-friendly and sophisticated (Cavelty, 2007:131). Furthermore, due to the transcendent nature of the Internet, it is viewed as an intrinsically insecure technology. The framing of cyber-threats has developed significantly over the years, escalating from the singular issue of

cyber-crime,³ to national security concerns of espionage, critical infrastructure protection,⁴ terrorism, and foreign exploitation. An exponential number of means and methods with which to mount a cyber-attack exist, thus an operational understanding of these threats is mandatory so as to avoid confusion of terminology that could lead to fallacious claims. The extensive range of malicious activity and actors, inclusive of cyber-threats are summated in the following table.

Table 1: Cyber-threats – Typology

	Motivation	Target	Method
Cyber Terror	Political or social change	Innocent victims	Computer-based violence or destruction
Hactivism	Political or social change	Decisionmakers or innocent victims	Protest via web page defacements or distributed denial of service (DDOS)
Black Hat Hacking	Ego, personal enmity	Individuals, companies, governments	Malware, viruses, worms, and hacking scripts
Cyber Crime	Economic gain	Individuals, companies	Malware for fraud, identity theft; DDOS for blackmail
Cyber Espionage	Economic and political gain	Individuals, companies, governments	Range of techniques to obtain information
Information War	Political or military gain	Infrastructures, information technology systems and data (private or public)	Range of techniques for attack or influence operations

Source: (Lachow, 2009:439).

Lachow defines cyber-espionage as the “...use of information technology systems and networks to gather information about an organization or society that is considered secret or confidential without the permission of the holder of the information...” (2009:440). Cyber-espionage is consistent with existing state perceptions pertaining to information gathering but it is specific to concerns regarding national security interests. Cyber-war or information war pertains to overt and offensive attacks between nation-state actors, in a deliberate effort to either disrupt or damage Internet based systems or networks. For further reading, Clarke and Knake (2010) provide an extensive mapping of the realities and threats of cyber-espionage and cyber-warfare. These two cyber-threats are often identified as the primary concern of states in considerations of information security, which pertains to the prevention of unauthorised access, disclosure, recording, manipulation or destruction of information. The

³ Cyber-crime is the term used to denote conventional criminal offences that are committed by means of computer technology or the Internet.

⁴ A term that denotes the systems or structures, either physical or virtual, deemed vital to the state. Should such a system or asset be incapacitated or destroyed, it is believed that it would have a debilitating effect on any sector or combination of sectors critical to the nation; such as national security, the economy, public health or safety (Westby, 2004:xxxiii).

increased tendency to store sensitive information electronically has resulted in a connection between cybersecurity and information security considerations. Hacktivism refers to the act of hacking for socially or political motivated purposes or to promote a political ideology, whereas black hat hacking is conducted merely for personal gain or malicious intent. Much like hacktivism, cyber-terrorism is politically motivated; yet they differ in that hacktivism does not aim to create a sense of fear or horror (Lachow, 2009:439).

The United States (US) Department of Defense (DOD) defines terrorism as the “...unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs to instil fear and coerce governments or societies in pursuit of goals that are usually political...” (Department of Defense, 2010:241).⁵ Inclusion of the prefix ‘cyber’ points to the convergence of understandings pertaining to cyberspace and terrorism, such that this study defines cyber-terrorism as “...the unlawful attacks and threats of attacks against computers, networks and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives...” (Weimann, 2004a:4). This study does not consider physical attacks on ICT systems and infrastructure to denote an act of cyber-terrorism; rather this constitutes a conventional terrorist attack wherein such systems just so happen to be the target.

Dorothy Denning, one of the world’s leading authorities on cyber-terrorism and information warfare, goes on to make the distinction that in order to qualify as cyber-terrorism, violence against persons or property must be an outcome of a politically motivated attack, or at the very least it must cause sufficient harm to instil fear (Denning, 2001:281). Ample credence is afforded to this distinction in that the media, academics and state actors alike have sought to apply the term to a vast array of activities resulting in an almost systematic acceptance of misclassified cyber-threats. Failure to operationalize definitions has meant there has been much confusion and misinterpretation of cyber-attacks, as concepts pertaining to the cybersecurity lexicon have continued to be employed in a transposable manner (Jarvis *et al.*, 2015).

⁵ The DOD definition is taken as a pragmatic starting point for conceptualizing terrorism in that, although seemingly state-centric, it’s understanding of the term is quintessential and shared by other literature included in this research. Conflation of the definition with insights drawn from additional resources leads to this study’s demarcation of the term ‘cyber-terrorism’.

Following the September 11 attacks substantial political attention has been afforded to a host of new threats and challenges, with the rise of cyber-terrorism featuring prominently in state security concerns. Government officials have continuously warned of potential *cyber-doom* scenarios wherein vulnerabilities introduced by networked systems and ICTs wreak widespread havoc. To illustrate such a scenario Caveltly constructs a narrative wherein a 12-year old boy hacks into the control system of a dam, opens the floodgates and releases trillions of gallons of water, ultimately flooding nearby cities and resulting in thousands of deaths (Caveltly, 2007:3). This story she develops from an article reported in the Washington Post wherein a hacker broke into a water facility in Arizona. However, whilst the individual accessed critical areas in the system, it was merely a server that monitored water levels, and it would not have been possible to control the dams. Furthermore, the individual was 27, not 12. The point here has been to demonstrate a tendency of both the media and political officials to greatly exaggerate and misconstrue disruptive occurrences in the cyber-domain.

The result of these misclassifications and fixation on potential threats and vulnerabilities has meant that much of the global cyber-populace (policy-makers in particular) have been gripped by cyber-terrorism angst. This has manifested in a climate of disquietude wherein "...instances of hacking into government websites, online thefts of proprietary data from companies, and outbreaks of new computer viruses are likely to be labelled by the media as suspected cases of "cyber-terrorism"..." (Weimann, 2004a:4). Ultimately, frequent and improper use of the term have clouded understandings of cyber-terrorism and more so the current realities of security in the information age.

Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.
(National Academy of Sciences, 1991:7).

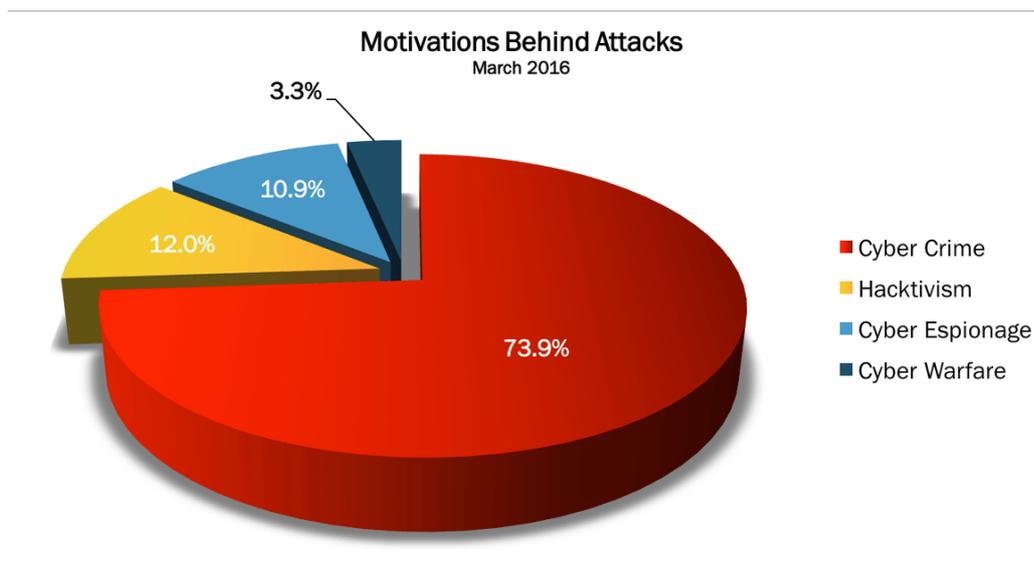
Fears of a digital Pearl Harbour abound as nation states continue to reassert the idea that cyber-terrorism poses one the greatest threats to modern society. The belief is that cyber attacks could destroy or compromise information infrastructure that could go on to jeopardise economies, physical infrastructure or even civilian life. These claims remain speculation and are lurid, as to date; no cyber-attack has come close to constituting a disaster of this level (Kenney, 2015:122). Moreover, both states and the private sector have invested so heavily in bolstering cybersecurity that computer systems have become increasingly resilient. In 2015 alone, global cybersecurity investments reached an excess of \$2.3 billion (Somerville, 2015).

Further doubt is cast on the potential for cyber-terrorism by the protection afforded by ‘air-gapping’, that is to say the process of isolating critical systems from the public Internet or other networks so that they cannot be accessed externally (Byres, 2013:29). For example, government sectors such as the US DOD employ this precaution to protect its nuclear weapon systems and the Pentagon’s internal network (Weimann, 2004a:9). This does not mean to suggest that it is not possible for a cyber-terrorist attack to be mounted.⁶ However, the technological capacity requisite for an individual or group to overcome state measures is highly unlikely and the effects of such events have been sensationalised.

Thousands of attacks are carried out against public and private computers and networks on a daily basis with recent years demonstrating an exponential increase in cyber-crime and hacktivism. The statistical data regarding the frequency of cyber-attacks is staggering and extremely difficult to quantify owing to variance in the nature of attacks and ambiguity in that many cyber-breaches are undetected. An indication of the monumental scale at which they occur can be demonstrated in that the cost of cyber-crime on businesses was estimated to be \$400 billion in 2015 and is projected to reach a global cost of \$2.1 trillion by the year 2019 (Morgan, 2016). Although cyber-attacks are becoming more complex and ever prevalent, the nature of the attacks has stayed fairly consistent. Cyber-crime remains the most prominent cyber-threat, yet as civil society and the idea of a global citizenship online continues to reach a growing consensus, groups such as Anonymous and whistle-blowers like Edward Snowden have been on the rise and have heralded an upsurge of hacktivism. In addition, the entrance of state actors and security interests has led to “...the creation of a militarized Internet used as a contested space for intelligence, economic espionage, information operations, and to destabilize adversarial states...” (Kallberg & Thuraisingham, 2013:230). This has served to drastically alter the dynamics of the cyber domain and has led to an increase in cases of cyber-espionage and cyber-warfare. The following graph provides an indication of cyber-threat schematics by summing the motivations behind cyber-attacks for the months March 2016 and April 2016.

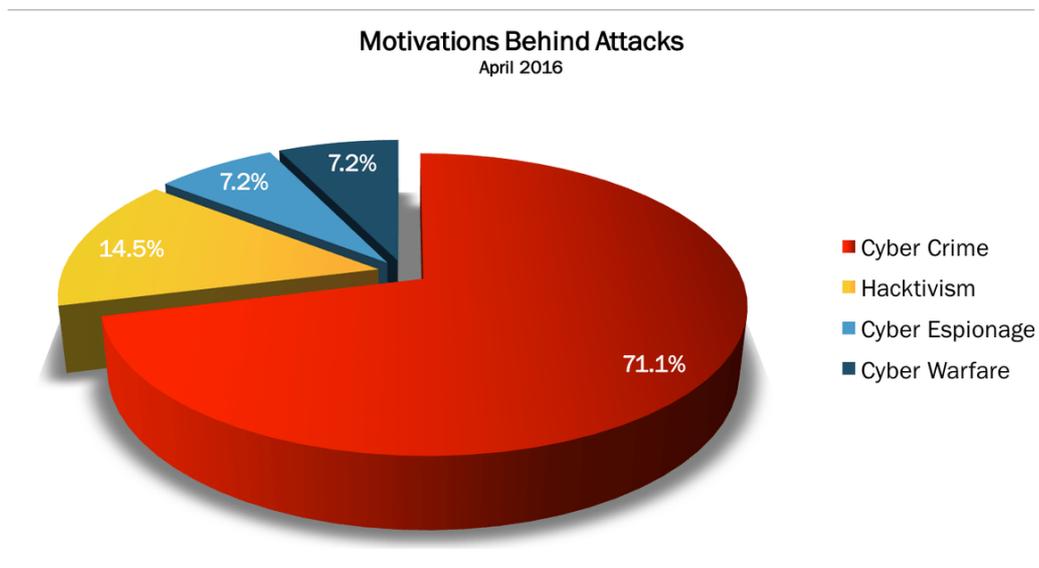
⁶ The efficacy of air-gapping had been hotly debated (Byres, 2013).

Figure 1: Motivations Behind Registered Cyber-Attacks for March 2016



Source: (Passeri, 2016a).

Figure 2: Motivations Behind Registered Cyber-Attacks for April 2016



Source: (Passeri, 2016b)

To reiterate, there has yet to be an account of cyber-terrorism. As previously elucidated, the response to this blatant lack of cyber-terrorist activity has been the conflation of the term's understanding with other species within the cyber-threat genus, allowing policy-makers and the media to label other forms of attacks that are more commonplace, as incidences of cyber-terrorism. What's more, there has been an increasing trend to classify online activity of

traditional terrorists as cyber-terrorism. It would be imprudent if not reckless to completely rule out the possibility of a cyber-terrorist attack from known terrorist groups and their affiliates. However, fixation on this idea of cyber-terrorism has served to undermine the efficacy of online counter-terrorist operations in that the most immediate online threat posed by contemporary terrorist organisations such as al Qaeda and Islamic State (IS) resides in their capacity to exploit the Internet as a tool to instrumentalize and “...facilitate their own real world activities, rather than bring the Internet crashing down...” (Kenney, 2015:128).

Islamic State & Cyberjihad:

Within the current global context, IS has managed to assert itself as one of the most accomplished terrorist organisations of the 21st century. In the past decade, IS has gained territories in both Syria and Iraq, managed to build a self-sustaining financial model, boasts substantial military capacities and has an estimated 30 000 fighters at its disposal. Such unprecedented success has not been realised by any other terrorist organisation. Some authors have even come to regard IS as a pseudo-state, stating that in its capacity, IS exceeds the definition of a terrorist organisation (Cronin, 2015:88). Of the known and active terrorist organisations it is logical to suggest that owing to IS’s substantial resources and reach it is amongst the most likely non-state actors to boast the capability and resources to carry out a cyber-attack. However, technical analysis reveals that not only has IS yet to show an interest in mounting a cyber-attack of significant scale, they have also yet to demonstrate the requisite training, knowledge or expertise to do so (Fidler, 2015:2).

These limited capacities are illustrated by the attack mounted against the YouTube and Twitter accounts of the US Central Military Command (Centcom). A group that has called itself the “Cyber-Caliphate” had written the message “I love you ISIS” on the webpage and had tweeted messages that included pictures of US personnel and military documents. This attack would seem to suggest that IS affiliates had compromised military servers and installations, however although extremely embarrassing and highly publicised the attack boils down to a simple act of vandalism as the information shared “...was widely available and non-official...” (Harrison, 2015). Nevertheless, this attack serves to reflect upon IS’s wider online strategy. IS has indeed weaponised the Internet, but not in the manner that cyber-terrorist discourse has dramatized. IS has instead demonstrated its ability to exploit the Internet to ultimately serve in the purposes it was intended. That is to say, the Internet has afforded IS an advanced networking capacity in that “...it enables terrorist organisations to

operate as transnational, virtual organizations....” by facilitating a means through which they can “...do fundraising, recruiting, training, execut[e] command and control, intelligence-gathering, and information-sharing...” (Lachow, 2009:459). This deterritorialisation of jihadi warfare represents a shift in modern Islamic extremist modes of interaction and operation.

The term ‘jihad’ refers to dialogue about Islamic identities and the religious duty and spiritual struggle of Muslims to maintain their faith. Following the September 11 attacks the word has been used widely by the western media and state officials to describe the violent struggle that is perceived as obligatory by jihadists, “...to eradicate obstacles to restoring God’s rule on Earth and defending the Muslim community...” (BBC News, 2014). Islamist extremist groups such as al-Qaeda and IS have applied the word to legitimise violent attacks mostly directed against western governments in what they have deemed to be a ‘Holy War’ to affirm their religious beliefs. Most Muslims do not accept the application of the term in this way in that they feel that it is falsely associated with a noble religious concept denoting personal struggle and merely serves as a means to validate violence. Modern jihad has demonstrated the melding of terrorism and globalization as the Internet has manifested as “...a virtual sanctuary, where every dimension of the global jihad is taking place online...” (Ranstorp, 2007:32).

Within the information age the methods and intentions of terrorist organisations have evolved. The Internet has enabled the creation of a complex networking system which provides a cheap and anonymous communication platform as well as a functional tool that has astronomically increased the global reach of terrorists groups, allowing for more fluid and efficient multi-dimensional propaganda dissemination and the introduction of a wider audience. The term used to express this transformation and shift to digital applications is ‘cyberjihad’. The concept of cyberjihad in this study connotes the militaristic application of understandings of jihad (Bunt, 2003:11-12). In the context of Islamic extremism, the shift to the digital frontier has been attributed to al-Qaeda as its application of the Internet as an intrinsic structure for ensuring its viability and mandate has been heralded by some as “...the first guerrilla movement in history to migrate from physical space to cyber-space...” (Coll & Glasser, 2005). IS originally formed as an affiliate of al-Qaeda to fight against the 2004 US invasion in Iraq. Although it has since broken away from al-Qaeda’s leadership, as its progeny, IS has profited “...from the roots of al-Qaeda’s already highly developed communications strategy...” (Liang, 2015:1).

By building on a decade of experience from al-Qaeda, IS has unleashed a cyberjihad campaign that has occupied social media platforms such as YouTube, Facebook and Twitter, and which has ultimately succeeded in attracting a worldwide network of followers. Support from this network combined with a universal cyber-presence has allowed IS to articulate and amplify its extremist messages and violent ideology on a global scale whilst also allowing them to disseminate complex information. The Internet has served as an indispensable channel to communicate anything from tutorials on how to assemble a suicide vest at home, to information on suitable targets to attack (Heickerö, 2014:557). As an operational tool, publicly available web applications like Google Maps have been used by IS to plan physical attacks whilst videos of beheadings are uploaded to conduct psychological warfare and garner global attention. Arguably the most important role of the Internet for IS has been that of recruitment, in that online extremist content and interaction with like minded individuals has accelerated the process of radicalization. Not only has there been an influx of foreigner fighters to Iraq and Syria who seek to join IS, but dozens of people have been inspired by cyberjihad content to conduct lone-wolf acts of terror in their own countries (Liang, 2015:2).⁷ An example of such an attack is demonstrated in the events of 12 June 2016, when Omar Mateen, an American born who pledged his allegiance to IS, opened fire at a night club in Florida, killing 49 people and wounding 53 (Ellis *et al.*, 2016).

The upsurge of jihadi websites and social media accounts operating online is indicative of the inexhaustible tactical and strategic operational advantages provided by cyberspace. A census of Twitter conducted by the Brookings Center for Middle East Policy from September through December 2014 estimated that there was anywhere between 46000 to 70000 Twitter accounts used by IS supporters (Berger & Morgan, 2015:2). Islamic State has proven that it is “...more strategic online, demonstrates greater social media sophistication, and operates in cyberspace on a larger scale and intensity than previous terrorist groups...” (Fidler, 2015:2). In shifting to cyberjihad, a distinction must be noted in that the capabilities afforded by the Internet have not supplanted conventional forms of political expression as terrorist activities still greatly center around mounting physical attacks; rather cyber-space has delivered a means by which IS can transcend conventional barriers and boundaries (Bunt, 2003:11). Although IS has engaged in hacking, the cyber-attacks have been relatively menial and have

⁷ ‘Lone-wolf’ is the term used to denote individuals who sympathize or are affiliated with a terrorist organization, who are radicalized and encouraged to carry out insurgent attacks.

resulted in nugatory damage. IS's capacity to mount an attack that qualifies as cyber-terrorism depends on its ability to attract elite hackers and computer literate foreigners to its cause. Managing the threat of cyberjihad should precede concerns of cyber-terrorism in that it is only through online recruitment that terrorist groups such as IS will gain the requisite expertise to plan and carry out a cyber-attack of significant scale.

In line with an analysis by the New York Times, as of 1 July 2016, "...more than 1200 people outside of Syria and Iraq have been killed in attacks inspired or coordinated by the Islamic State..." (Yourish *et al.*, 2016). Taking precautions to limit the potential of a cyber-terrorist attack occurring is indeed important but in the current global context, policy-makers and the media alike should be wary of confusing and prioritising a hypothetical threat over cyberjihad. When considering the number of people who have died from physical attacks carried out through online planning and co-ordinating, it is irrefutably in the interest of state actors to either subvert or disrupt cyberjihad activities (Lachow, 2009:459).

Islamic State territorial gains, the influx of foreign fighters, the volume of its online propaganda, and extremist attacks in Paris converged to catalyze more policy action in 2015. In February, the U.S. government convened a summit on countering violent extremism, which discussed extremist use of social media (Fidler, 2015:2).

The rise of Islamic State and the increasing potential for radicalization pose a monumental challenge to global security interests. Having recognized the threat of cyberjihad, state actors have pursued countermeasures that are either content-based; focusing on censoring jihadist material online, or aim to develop a counter-narrative that seeks to reduce the likelihood of radicalization. These efforts have thus far proven ineffective (Liang, 2015:1). Challenges to the success of these countermeasures stem from numerous outlets, particularly issues of censorship, which bring into question concerns of transparency and the impact on freedom of speech and state endorsed surveillance and its impact on privacy rights. Owing to the decentralized operations of the Internet, censorship also mandates co-operation amongst states and with private companies. Efforts based on counter-narrative measures have similarly confronted issues in that it remains difficult to determine the success of preventative work and so far, government sponsored online efforts "...aimed at blunting the Islamic State's appeal have been criticized as ill conceived and counterproductive..." (Fidler, 2015:3).

Problem Statement:

In recent years IS has proven extremely adept and proficient in its cyberjihadist activities. The group has succeeded in exploiting the Internet as a platform for disseminating its propaganda and as means through which to radicalize vulnerable and isolated individuals (Berger & Morgan, 2015:2). Popular social media platforms such as Twitter, Facebook & YouTube have come under increasing pressure to adopt more aggressive policies towards tackling terrorist content. Augmented efforts have resulted in greater censorship, filtering and account suspension of jihadist material on the Internet. However the topic of censorship proves contentious in that it is at odds with values pertaining to freedom of speech and expression. Debate over such values has meant that responses and policies have not been expeditious; furthermore it remains unclear as to whether the policing of online jihadist content has been successful. In addition, much of the Internet's infrastructure is owned and operated by the private sector, locating issues of its management and control firmly in line of concerns with public policy (Lachow, 2009:458). Review of existing policies points to the need for greater international cooperation in an effort to promote more efficacious content-based measures and dissemination of government sponsored counter-narratives aimed at suppressing and undermining extremist ideology both on and offline (Liang, 2015:1). Securitisation Theory points to the politicisation of issues by framing them as an existential threat to security. In doing so, certain emergency conditions can be adopted that allow for extraordinary measures to be taken should they serve to undermine or counter the perceived threat. It is unclear whether a Securitisation framework can be applied to the issue of cyberjihad and whether such a frame would have utility in terms of overcoming those challenges that have thus far hampered countermeasures to prevent terrorist exploitation of the Internet.

Research Questions:

Refining the problem statement allows for this study to be guided by an exploratory research question, namely:

What utility can Internet securitisation boast in an effort to mitigate the threat of Islamic State (IS) cyberjihadism?

In order to facilitate a greater understanding of the primary research question, the following sub-questions are posed:

1. How have cyberjihadists sought to exploit the Internet?
2. What measures have been taken to counter cyberjihad and to what degree have these measures proven successful?
3. What are the disadvantages and benefits of securitisation of the Internet in terms of the international security context?

Theoretical & Conceptual Framework – Securitisation Theory:

The Copenhagen School of Security Studies has widened the security agenda by “...offering a Constructivist counterpoint to the materialist threat analysis...” of traditional⁸ studies by demarcating securitisation as a social process through which certain actors construct an issue as a threat (Buzan & Hansen, 2009:36). Securitisation Theory states that within the realm of international relations, for an issue to be constituted as a security concern, it must pose an existential threat to a particular referent object.⁹ By fulfilling this quality, “...the special nature of security threats justifies the use of extraordinary measures to handle them...” (Buzan *et al.*, 1998:21). Whereas traditional approaches to Security Studies have focused on material interests such as military capacity and distribution of power, Securitisation Theory has instead sought to demonstrate that security in itself is not an objective condition. Rather an issue becomes securitised through discursive and political forces that frame it as a security concern (Balzacq, 2011:1). Illocutionary devices are employed as securitising moves, yet an issue cannot be successfully securitised until it is accepted as a threat by a distinct audience. Conceptualising the research question allows for the components of the securitising act to be delineated; this study regards international governmental organisations (the UN in particular) as the *securitising actors*, cyberjihad as the *existential threat*, and the global population as the *referent object*.

⁸ ‘Traditional’ denotes a “...shorthand, most commonly used by writers in or sympathetic to critical Security Studies, which refers to Realist, Liberal, Peace Studies and Strategic Studies perspectives in the study of security that prioritise the state as the referent object of security, and focus primarily on military threats to the security of the state (sometimes also known as a ‘state-centric’ approach)...” (Peoples & Vaughn-Williams, 2010:4).

⁹ The referent object is an entity that is taken as the focus for analysis in Security Studies such as the state or the ecosystem. Essentially the referent object is ‘that which is to be secured’ (Peoples & Vaughn-Williams, 2010:4).

Whereas the profound spread of the Internet and the development of cyberspace was once firmly located in the realm of low politics¹⁰ and benign public policy, “...today states of all stripes have been pressed to find new ways to limit and control them as a way to check their unintended and perceived negative public policy and national security consequences...” (Deibert & Rohozinski, 2008:123). The assertion of power in cyber-space is in no way a recent development as states have increasingly targeted the Internet through content filtering and access regulation, in an effort to overcome the new challenges presented in the information age. Thus despite outcry from global civil society, securitisation of the Internet is already underway. The logic for applying Securitisation Theory in this study is grounded in its exploratory capacity and its readiness to be applied to concepts that exceed positivist limitations of state centrism and military concerns. “Cyberspace has created new conditions for which there are no clear precedents...” as contemporary global realities have served to insidiously compromise traditional understandings of sovereignty (Choucri, 2012:13). As a global phenomenon that transcends boundaries, the Internet has challenged major IR theories that are not readily imported to the cyber-domain. Because traditional theories continue to focus on the state, it is posited that they hold limited explanatory power in this study owing to the intrinsic dynamics of the research subject.

Research Design & Methodology:

Determining the utility of Internet securitisation in mitigating cyberjihad proves complex. A case study design is believed to best suit this research in that it calls for an evaluation of numerous variables and a coherent understanding of both cyberjihad activities and the efforts that seek to undermine it. In order for the research to have a “...wider impact than that of merely being a detailed account of a unique case, a strong theoretical dimension is often incorporated into a case study design... (Burnham *et al.*, 2008:64). As mentioned above, the research will be guided by the assumptions and assertions posited by Securitisation Theory. Although the selection of multiple cases generally allows for a more robust test of theory, writing constraints place such research beyond the capacity of this study. Furthermore, preference is afforded to the single case study design in that specification will facilitate more in-depth analysis and bring focus to the research. In terms of case selection, IS has proven itself uniquely adept and proficient in its capacity to weaponize the Internet as a tool for

¹⁰ ‘Low politics’ is a term used to denote “...background conditions and routine decisions and processes...”, whereas ‘high politics’ usually pertains to matters of “...national security, core institutions, and decision systems critical to the state, its interests, and its underlying values...” (Choucri, 2012:3).

cyberjihadist activity. Although other extremist groups have also sought to exploit the Internet, often it has been in mimicry of IS and more pressingly, they have not been as successful. In the context of the current security climate, the threat of cyberjihad has been afforded state attention as a consequence of IS activity on the Internet. For this reason, IS has been selected as the single case study. The approach to this study is most certainly grounded in the qualitative process due to the inductive nature of the research.

As the design approach of this study is qualitative, the majority of the research data will be derived from documentary and archival analysis. Tertiary resources such as books and peer reviewed academic journal articles will provide the theoretical basis for research (Burnham *et al.*, 2008:190). Findings and assertions will be complemented by primary sources such as state endorsed policy statements and reports, which will also be incorporated in order to conduct content analysis on existing policies. Owing to the very contemporary and highly news worthy subject matter of the case study, substantial use of secondary sources such as newspaper articles and reports on IS cyberjihad updates will also be incorporated. Whilst some books will be taken from the Stellenbosch University library, the majority of tertiary and secondary sources will be gathered online. Electronic journal archives such as JSTOR and Google Scholar will be used in tandem with online news websites such as BBCnews.com. This study includes overviews and analyses of policies and legal instruments adopted by states and international organisations, which will also be collected online. Although it is imperative to incorporate books to form the foundation of the research in terms of theory and research methodology, the cyberspace environment is dynamic and IS is still highly active, thus the use of electronic sources is essential to this study as they are more regularly updated and published. Quantitative data such as graphs and statistics derived from sources will be incorporated into the research so as to substantiate posited statements.

Summary of Chapters:

Chapter 2, 'The Internet – Governance Modalities & its Place in the International Security Context', aims to develop a base of understanding for the study. The Internet is a multifarious subject to research in that it serves as a point of convergence for many fields ranging from computer studies to policy design. This study takes Internet governance modalities as a starting point. Thereafter the study is shifted towards a security frame by focusing on security discourses and instruments in the international context that are linked to cybersecurity and information security; as these areas serve to implicate the Internet. The research focuses on

Resolutions passed by the UN on issues of cybersecurity and information security. Chapter 3, ‘Theoretical Grounding – The Copenhagen School’s Securitisation Theory’, presents the theoretical framework that has been selected to guide the subsequent research. This thesis approaches the issue from a Security Studies perspective understood as a sub-field of IR. After mapping the development of Security Studies and the most dominant perspectives within it, seminal works pertaining to Securitisation Theory are recapitulated so as to both contextualize descriptive inferences and identify limits of the theory and how it addresses issues related to the Internet in the contemporary security context. Concepts, challenges, and applications of Securitisation Theory are presented in this chapter. Chapter 4, ‘Terrorist Integration of Cyberjihadist Strategies – The Case of Islamic State’, develops the case of IS and its integration of cyberjihadist strategies. Thereafter application of theory allows the study to demonstrate how Internet securitisation can be realised. The research then converges to determine the benefits and disadvantages of Internet securitisation as a strategy in countering cyberjihad. In Chapter 5, ‘Conclusion’; all findings are summarised; the research problem and questions are addressed; and areas for future research are identified.

CHAPTER 2: The Internet – Governance Modalities & its Place in the International Security Context

Introduction:

The field of IR displays a general ignorance to all matters concerning the Internet. This is particularly evident in IR's unfamiliarity with the terminology, operational details, and security challenges pertaining to the Internet (Mueller *et al.*, 2014:87). In this chapter, the study aims to develop a base of understanding for the subsequent research by providing an overview of the various Internet governance modalities and by locating the Internet in the international security context; dividing this chapter into two sections. The section on Internet Governance begins by defining the concept itself. Thereafter, the chief modes of Internet Governance are demarcated and their primary tenets are elucidated upon. The major modalities of Internet Governance are identified as; Standardisation and Protocol Governance; Structural Management Governance; Intellectual Property Governance; Internet Security Governance; and Internet Filtering Governance. Governing the Internet proves to be a highly contentious issue owing to the need for multi-sectoral and transnational cooperation. Ongoing debates and lack of consensus on the issue reveal that the future architecture of the Internet is not assured. As such, the section then proceeds to highlight the major discourses surrounding the future of Internet governance and the role of states in determining its outcome. This segues into the second section of this chapter. The second section links discourse surrounding Internet regulation; to concerns in the international security context. Issues pertaining to international security are intrinsically linked to states. State policies and narratives reveal that their primary focuses (on issues pertaining to the Internet) are cybersecurity and information security. As state security policies and strategies are highly variegated; major developments in the fields of information security and cybersecurity conducted under the UN are used to indicate the overall international security context. Finally the concluding section summarises the chapter and links it back with the research problem and questions.

Internet Governance:

Delineation of Internet Governance:

Contextualizing the concept of Internet Governance proves prudent in an effort to facilitate a concise summation of its ontology. This in itself is difficult, in that review of the academic literature demonstrates that defining the term has been a subject of great contestation and

debate for the past two decades. Hoffman provides an extensive account of the development of the term's understanding (2005). For the purpose of this study, the definition developed by the United Nations (UN) Working Group on Internet Governance (WGIG) will be employed. Namely, Internet governance can be defined as

the development and application by Governments, the private sector and civil society, in their respective roles of shared principles, norms rules, decision-making procedures, and programmes that shape the evolution and use of the Internet (WGIG, 2005:4).

This definition remains the most widely accepted and most encompassing understanding of the term. Malcolm provides a succinct case for its efficacy by demonstrating the manner in which it serves to include notions of networks, hierarchy and market governance (2008). Furthermore, numerous authors have sought to develop and build upon it, for example Bygrave and Bing (2009), as well as Mathiason (2008). What is considered most useful about the definition developed in the report is that, not only is it explicit about the inclusiveness of both state and non-state actors, it extends the scope of Internet governance beyond system protocol to include issues regarding security, public policy, developmental aspects and critical Internet resources (WGIG, 2005:4). The inclusion of these facets allows for the delineation of the different subsets of Internet governance. Augmentation of the definition lends to the development of a framework for organising the most apparent facets associated with Internet governance.

Standardization and Protocol Governance:

During the early stages of its expansion the proliferation of the Internet mandated the development of technical standards, known as protocols, to facilitate the networking and flow of information between devices. Internet standards, codes and guidelines were drafted in a bottom-up process by key actors in the global community who served to develop a new form of legislation and broaden understandings of regulation and governance by introducing a paradigm that was not state-centric (DeNardis, 2009:7). Government involvement was limited to funding and private and public-private institutions developed the majority of standards. The Internet Engineering Task Force (IETF) is recognised as the pioneering organisation in the development and promotion of voluntary Internet standards and remains instrumental to the process. Emphasis on private-sector leadership, served to endorse a governing framework that was self-regulating (Bradner, 1999:48).

Governance in this regard is limited to the standardisation of Internet protocols and functional commands. Early writers on Internet freedom argued that due to the open source development of these protocols, the Internet is inherently decentralised and favours principles of democracy (Zittrain, 2008). Lawrence Lessig was one of the first in a line of many authors, who sought to dispute this view. Lessig argued that the code that governs the Internet is influenced by the values and beliefs of the people who write it. As those people are controlled by laws and can be coerced, so too can the Internet be controlled and regulated in effect (Lessig, 1999). He maintains that code is not neutral in that it can be shaped to enshrine values of liberty or control.

Structural Management Governance:

Following its unprecedented spread, technical issues regarding the scarcity of domain names¹¹ which are essential to the Internet's address system led to the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998. In this regard, when the term Internet governance was originally introduced in the 1990s it was used "...mainly to describe the specific form of the technical management of the global core resources of the Internet: domain names, IP addresses, Internet protocols and the root server system..." (Kleinwachter, 2008:10). In light of ICANN's role in co-ordinating Internet domain names and addresses, it has been recognised as a critical Internet resource. Although ICANN is regarded as a private entity, it has been the source of considerable controversy due to its contractual relationship with the US (Gross, 2013). To elaborate, certain actors in the international system maintain that US influence over ICANN has served to compromise the institution's neutrality and politicised its functions demonstrated in that the US asserts sole political authority over the root zone file, which is an essential construct of the domain name system (DNS) (Mueller, 1999:42).

Criticism regarding this relationship essentially instigated larger governance concerns pertaining to the Internet and culminated in the development of the World Summit on the Information Society (WSIS). Endorsed by the UN General Assembly Resolution 56/18, the WSIS took place in two phases the first of which was held in Geneva in 2003 (2003,

¹¹ A domain name is an identification string used in web addresses that serve to designate a realm of administrative authority or control within the Internet. Examples include generic top-level domains like *.com* or *.org*; and country code top-level domains like the South African, *.co.za*. The domain name system (DNS) is responsible for assigning domains to different entities.

Declaration of Principles Building the Information Society: a global challenge in the new Millennium). The primary objective of the first phase was to develop a coherent statement of political will and initiate the push to establish the foundations of an inclusive Information Society that reflects all divergent interests at stake. The summits failure to reach a consensus, led to the commissioning of the aforementioned WGIG as a task force to identify public policy issues and develop proposals for action regarding Internet governance leading up to the second phase. The primary outcome of the first phase of the WSIS exists in that it served to challenge the unilateral authority of the US over ICANN, which Klein describes as a “...violation of sovereignty through its control of Internet’s globally-shared core resources...” (2004:9).

The political and economic implications associated with the control of core Internet resources, has served to place emphasis on the role of states and institutions in Internet governance. As the Internet is based on global and non-proprietary standards that are freely available and accessible, it essentially constitutes a global commons (Mueller *et al.*, 2007:246). Conceptualising the Internet as a global resource in much of the literature pertaining to policy creation has thus led to the extension of national sovereignty into its governance modalities and has facilitated the application of the multi-stakeholder model.

The multi-stakeholder approach to Internet governance was first recognised at the second phase of the WSIS, held in Tunis in 2005. Participants once again failed to reach a consensus regarding changes to ICANN’s control structures. The only significant outcome of the summit was the creation of the multi-stakeholder Internet Governance Forum (IGF), which would serve as a platform for further policy discourse regarding the development of a more inclusive Internet governance framework.¹² The IGF boasts no decision making authority, thus it has been described as a compromise between countries that oppose the involvement of national mechanisms in Internet governance and those who petition for a more formal structure (Mathiason, 2008:5). The Internet Society (ISOC), which is considered to be a leading organization in the Internet’s standardisation and development processes, affirms that

¹² Following the Summits, the WSIS in collaboration with the ITU, UNESCO, UNDP and UNCTAD have held an annual Forum that that gathers the worlds ‘ICT for development’ community and WSIS stakeholders. The Forum has been used as a “...mechanism for coordination of multi-stakeholder implementation activities, information exchange, creation of knowledge, sharing of best practices and continues to provide assistance in developing multi-stakeholder and public/private partnerships to advance development goals...” and provides “...structured opportunities to network, learn and participate in multi-stakeholder discussions and consultations on WSIS implementation...” (ITU, 2016a).

the multi-stakeholder model has emerged as a dominant paradigm for Internet governance modalities (ISOC, 2013). Following years of negotiation, both ICANN and the US government have confirmed the Internet management body will be reformed into a new kind of international organisation, managed by a body that is largely independent of state authority. The US government has agreed to relinquish its oversight of the DNS from 1 October 2016, placing control of key technical Internet function under a global stewardship (The Economist, 2016).

Intellectual Property Governance:

The increase in information flows and free and open access to knowledge is central to the Internet's development and functionality. As such, increased network capabilities have led to issues regarding the protection of intellectual property. Intellectual property governance is thus best understood as the issues pertaining to copyright laws, patents and trademarks. Whilst ICANN remains the primary authority on trademark protection, intellectual property governance occurs at the international level through institutions and policies like the World Intellectual Property Organisation (WIPO) and the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement of the World Trade Organisation (WTO) (Mueller & van Eeten, 2010:726). Academic literature in this field is focused on debates over transnational copyright infringement and concerns regarding the issues of peer-to-peer sharing¹³ (De Beer & Clemmer, 2009; Litman, 2001).

Internet Security Governance:

Increased networking capabilities and connectivity in the information age reveals that the Internet has developed in manner that has made it an integral facet of modern communication modalities. Governments, commerce and the public have become increasingly reliant on the Internet as it continues to be integrated into the critical information structures of the public and private sectors (Sofaer & Goodman, 2001:1). Due to the inherent openness and universality of the Internet, this increased dependence, has exposed both state and non-state actors to new forms of security risks. Criminal activity propagated through the Internet, has arguably been deemed the most critical branch of Internet governance and denotes a vast scope of security threats. Academic review reveals that the issue of Internet security governance is extremely multifaceted due to the complexity of concerns and numerous actors

¹³ The sharing and distribution of digital media using peer-to-peer (P2P) technology; users are able to connect to other computers on the P2P network and by using software, which also allows them to locate and access desired content such as music (Carmack, 2005).

involved. For the purposes of this section, further elaboration will be limited to the mainstream international relations understanding of the term 'security' with regards to state security concerns (Deibert & Rohozinski, 2010).

Due to the omnipresent connectivity capabilities of the Internet states are now vulnerable to transnational attacks on critical structural resources like ICANN, as well threats to cybersecurity namely; cyberterrorism, cyberespionage, and cyberwar. Within the context of international relations, the decentralised architecture of the Internet poses challenges to state control. Existing Internet security governance structures and policies lack the capacity to deal with these transnational vulnerabilities (Arquilla & Ronfelt, 2001). Thus intergovernmental co-ordination has been deemed mandatory to the development of Internet security governance, yet no mention of it was made during the WSIS. Much of the literature pertaining to Internet security governance discusses mediations between states and institutions towards the development and standardisation of Internet security (Kuerbis, 2011).

Internet Filtering Governance:

The final predominant subset of academic literature regarding Internet governance is centred on the role of the state in Internet filtering. Internet filtering is essentially the assertion of national controls on the content of information accessed online by civilians. As has been the norm in Internet governance considerations, the range of topics filtered globally is markedly broad (Faris & Villeneuve, 2008). In an effort to provide a competent elucidation of the extent to which filtering occurs, these topics can be organised thematically. Categorisation reveals that the primary motives or rationales for state filtering pertain to issues of political assertion, moral and societal norms, and security concerns.

Political assertion filtering refers to the censorship of political opposition by ruling governments. Blocked content is usually information pertaining to opposition parties or critics of the existing order. This form of filtering is most evident and characteristic of authoritative and repressive regimes. Whilst numerous countries employ political assertion filtering, most of the literature in the field discusses its extensive application in China. For further reading, Kalathil and Boas (2003) discuss the implications of the Internet for authoritarian regimes, whilst Lu and Liang (2012) map the development and extent of China's regulatory policies. Security concerns filtering, relates to the state rationale of national security. This form of filtering ties in with Internet security governance, in that it

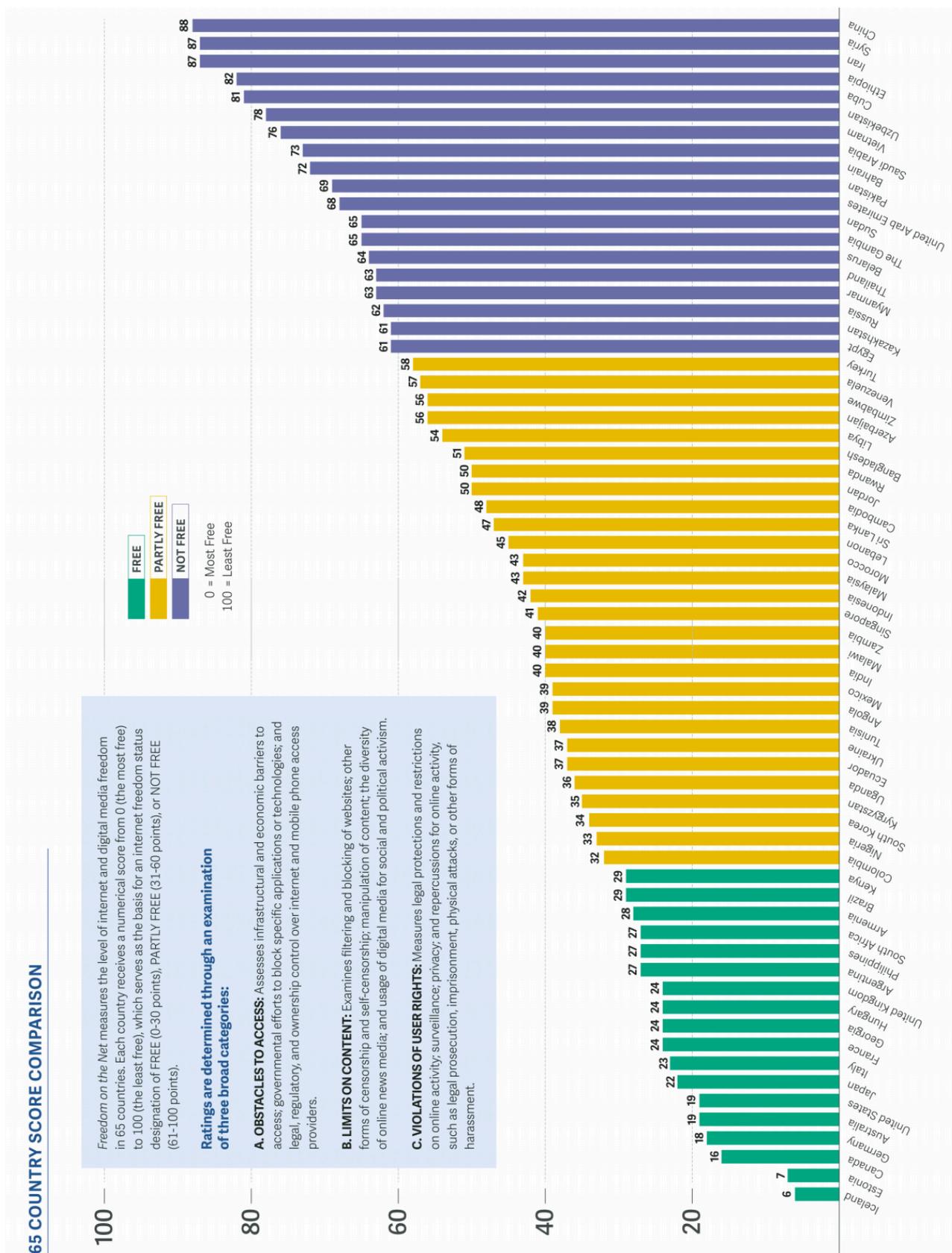
involves blocking websites that boast content relevant to terrorist or insurgency threats. Moral and societal norms filtering, pertains to censorship on an ethical basis. Varying values and societal norms, renders this form of filtering subject to localities. Prominent concepts in social filtering literature are issues of pornography, homosexuality and online gambling. A comprehensive yet succinct understanding of Internet filtering is afforded by the OpenNet Initiative, which has conducted an expansive study documenting the collective works of prominent researchers in the field. Their findings regarding the trends and patterns shaping information controls around the world have been published in the *Access* series (Deibert *et al.*, 2008; 2010; 2011).

A prominent issue conveyed in articles on Internet filtering governance is the concern of civil liberties and freedom of speech. In light of the fact that the Internet plays an increasingly important role in terms of how individuals in the global society communicate and express themselves, the extent of state regulation has been an issue of substantial contention. The possible ramifications of filtering policies on civil liberties and justice, has resulted in outcry from the global civil society (Villeneuve, 2007). The Freedom House organisation has been central to the research discourse regarding Internet freedom. Internet freedom is best understood as the promotion of free speech and access to information online. Literature in this regard is concerned with regimes that use legal mechanisms, intimidation, imprisonment or mute political speech and organizing in order to control information flows (Kelly *et al.*, 2012).

On the international platform, policies regarding Internet freedom and rights have been ratified by the UN Human Rights Council by affirming that the same fundamental freedoms enshrined in the Universal Declaration of Human Rights must apply to Internet governance (UN Human Rights Council Resolution on: The promotion, protection and enjoyment of human rights on the Internet, 2012). However, principals of sovereignty and territoriality remain and state policies on Internet filtering and freedoms are extremely divergent. Freedom House has quantified these differences in their studies and classified states accordingly. Findings reflect obstacles to online Internet access, limits on content and violations of user rights. Issues regarding the use of the Internet for surveillance and privacy concerns are included in the study. The infograph that follows indicates levels of Internet and digital media freedoms in 65 countries as determined by the Freedom House study. Each country is allocated a numerical score ranging from 0 (the most free) to 100 (the least free). Ratings are

determined through an examination of 3 categories; obstacles to access; limits on content; and violations of user rights (Kelly *et al.*, 2015:20). The activities encompassed by these categories directly correlate to Internet Filtering Governance practices, hence the infograph is employed as a numerical indicator of the levels of Internet Filtering Governance in different states.

Figure 3: Freedom on the Internet – Country Comparison



Source: (Kelly *et al.*, 2015:20-21).

Discourse Pertaining to the Future of Internet Governance:

Discourse regarding the future of Internet governance has been a subject of heated debate and conflict. In *Networks and States* Milton Mueller argues that as a distinctive global rhetoric continues to develop around the Internet, issues pertaining to its governance will increasingly emerge as a basis for "...contentious politics and institutional change at the global level..." (2010:1). The academic locus of this discourse has been centred around concerns of who should be governing the Internet, if it should be governed at all and whether its intrinsically decentralised information infrastructure mandates the production of new global institutions. Voicing these concerns has inexorably led to issues regarding determining the role of states in policy formulation. The following section seeks to demarcate the varying paradigms and architectural models that have gained prominence in Internet governance discourse.

In the debate regarding the role of states in the structuring of the Internet, much of the early writings point to the existence of a pronounced dichotomy. Two polarised views regarding the future of its governance are presented in the cyber-libertarian and political realist divides. The view posited by cyber-libertarians is that the Internet is intrinsically irrepressible and thus will not be controlled. Cyber-libertarians subscribe to a technologically deterministic ideology that advocates the use of the Internet as a mechanism for promoting decentralised initiatives that reduce the dependence on central governments and state actors. The doctrines most frequently cited author, John Perry Barlow, whom in his Declaration of the Independence of Cyberspace addresses the governments of the industrial world; can summate their values;

On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear (Barlow, 1996).

In stark contrast to cyber-libertarians is the realist view; which asserts that changes to information dissemination and communication elicited by the Internet will pose no implication for determining policy as the dominance of states will persist within the international system. Jack Goldsmith and Tim Wu have been referenced as the epitome of

this standpoint and in their book, *Who Controls the Internet*, they contest what they believe to be fallacious techno-utopian claims (2006). The authors maintain that the unequivocal authority of the state ensures that no substantial restructuring of the system will occur and the role of institutions will remain much the same. Goldsmith and Wu are critical of paradigms that underestimate the efficacy of governments to enforce their authority and territorial sovereignty through coercion, which they argue will be "...central to understanding the future of the Internet..." (Goldsmith & Wu, 2006:184). The realist standpoint is thus in favour of the notion of a bordered Internet.

The underlying tensions pervading from this dichotomy exist in that although states can exercise authority on physical devices located in their territories, like servers, Internet users can link their devices to any location within the global network. Thus highly complicating the assertion of sovereign rights on a national basis and mandating greater call for international cooperation that has yet to be established. Within this understanding is embedded the longstanding discussion of the implications of globalisation on state capacity. One such view perceives the nation state as now being too small to cope with the expansive scale of global concerns. This argument advocates neither state centralisation nor decentralisation, but rather seeks to assert a middle ground wherein some state functions are "...migrate[d] to a supragovernmental or transnational level,...[devolved] into local units,...[or transferred] to the private sector..." (Bell, 1976:47). The extent to which these state functions are relocated allows for the outlining of prominent models for Internet governance.

Demarcation of the literature reveals three prevalent models for Internet governance, namely the aforementioned multi-stakeholder and private-sector leadership models, as well as the increasingly employed balkanised model. The multi-stakeholder model has sought to foster a process towards enhanced cooperation and assert that international management of the Internet should be multilateral, transparent and democratic. It is worth noting that divergent views exist on what it is enhanced cooperation denotes and that exchanges between different actors vary considerably. Ambiguity in this regard has been perceived as a matter for contention, in that it allows for a bulwark under which interested parties can advance their own relative positions and the extent of state authority is not defined. Potential ramifications are demonstrated in that increased regulatory capacities will serve to empower authoritarian regimes and undermine civil society (ISOC, 2013).

The main justification for the need to reform Internet Governance structures in favour of the multi-stakeholder model is rooted in the perceived weakness of the system pertaining to issues of representativeness and inclusion, as well as imbalances of power. In addition, state actors are wary of the absence of agreed procedures and distributed governance arrangements in that they lead to opaque governance structures, which facilitates powerful actor dominance (Segal, 2014). Lastly, policy concerns such as security and consumers' rights are becoming increasingly transnational. As such, advocates of multi-stakeholderism argue that existing institutions have been rendered incompetent as they lack the capacity to address contemporary issues. State cooperation is thus regarded as mandatory. Issues of contention arise in that how then will proposed reform ensure inclusiveness and equality of actors, whilst maintaining efficiency of the system.

Numerous state backed conferences and partnerships have developed out of support for the multi-stakeholder model, the most prominent and recent of which was the 2014 NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance. NETmundial was effectively a meeting convened by the Brazilian government that sought to gather the various international actors and stakeholders involved with Internet governance in an effort to contribute "...to the evolution of the Internet governance ecosystem..." (NETmundial, 2014). The meeting sought to facilitate multi-stakeholder discourse surrounding Internet governance principles and develop recommendations for a roadmap for the future evolution of the Internet governance system. The mandate of the initiative has since run out, with both ICANN and the World Economic Forum (WEF) withdrawing from the project just prior to its deadline in July 2016.

Justification for maintaining the private-sector leadership model exists in that throughout the varying fields of literature, the massive success and spread of the Internet in its early years has been attributed to the absence of governmental legislation. In addition, there is a pronounced fear within the global community that facilitating the exercise of state control on the Internet will lead to the restriction of individual rights and freedoms, particularly with regards to the rights to privacy and freedom of expression. Further justification stems from the fear that increased regulation will lead to the introduction of time and cost consumption procedures, which will serve to hinder the speed of innovation in the development of new Internet services and applications (Kleinwachter, 2008:13).

A congruent ramification of the introduction of such procedures lies in that they are likely to be administered in manner that is uneven and potentially biased to specific actor interests. The repercussions thereof, exist in that they stand to exacerbate existing inequalities demarcated by what has been termed the digital divide. One of the essential criticisms of the private-sector leadership model exists in that the primary Internet governing authority, the Internet Corporation for Assigned Names and Numbers (ICANN), has been criticised for its contractual relationship with the U. S. government. (Gross, 2013). As previously stipulated the U. S, has not renewed its contract with ICANN as the condition that the institution or authority that follows advocates the multi-stakeholder model has been met (Segal, 2014; Farrel, 2016).

The final prominent model for the future of Internet governance outlined in academic literature pertains to the growing consensus for an increasingly fragmented cyberspace. Due to exacerbated interconnectivity and networking capabilities through the Internet, cyber based criminal activity in the international system is becoming increasingly prominent. Escalating numbers of attacks on states and the private sector have essentially resulted in a scramble to reduce vulnerabilities and prevent future cyber attacks (Negroponte *et al.*, 2013:3). As such, many countries have sought to erect technical barriers to information flows as a precaution and means to enforce cybersecurity.

The notion of a balkanised Internet has gained precedence as “...many countries seek increased security and control over the type of information and knowledge that flows across the Internet...” (Negroponte *et al.*, 2013:4). Adoption of the balkanised model has been an issue of vehement contestation amongst state actors. Criticism towards increased fragmentation stems from the argument that the Internet’s exponential growth and proliferation is attributed to the decentralised manner in which it initially developed. Furthermore, critics argue that certain state actors are pursuing the fragmentation model so as to divide the Internet in an effort to assert their sovereignty over it. They maintain that ramifications exist in that constricting information flows may foster disparities in accessing knowledge, result in the oppression of civil liberties and negatively affect the architecture and resilience of the Internet (Negroponte *et al.*, 2013:15). Whilst global flows of communication have made state censorship difficult, it is most certainly possible and regularly enforced. Pronounced regulations and penalties have effectively carved out “...national censorship islands within the global flow of information...” (Deibert, 2003:511).

Disparities amongst state opinions regarding the balkanised model were most evident at the 2012 World Conference on International Telecommunications in Dubai (WCIT). The WCIT, first of its kind, was held in an effort to renegotiate the International Telecommunications Regulations (ITR) treaty, which had remained unchanged since 1988. The site of contention pertained to the adoption of Resolution 3, which sought to “...foster an enabling environment for the greater growth of the Internet...” (Final Acts WCIT, 2012:20). States were divided between those who lobbied for a more state-centric system to manage the Internet, for example China and Iran, and those that opposed the International Telecommunications Union’s (ITUs) involvement in Internet regulation. Member states that were against the ITUs involvement, most notably the U. S., maintained that it would serve to threaten the multi-stakeholder model (ARIN, 2012). A notable development in WCIT proceedings is that a significant number of African states signed the treaty. The Council on Foreign Relations independent task force on Internet governance attributed this pattern to the argument that African states lack the technological expertise to deal with cybersecurity threats on their own. Thus in light of the long history they share with the ITU, it has been regarded as a credible partner.

Advocates of Internet freedom (in line with technological determinism) maintain that attempts to assert conventional understandings of governance pertaining to sovereignty will fail, as they cannot scale up to the cyberspace domain. Realist paradigms perceive fragmentation as inexorable. Many authors in the field have accepted the onset of fragmentation as inevitable. Thomas Schultz goes on to make a distinction between the different forms of which the balkanisation process can assume and their varying implications. He argues that fragmentation will occur in either a vertical or horizontal process. Whilst the horizontal process is driven by the pursuit of commercial efficiency and pertains to considerations of legal pluralism, the vertical process is concerned with issues of public policy “...and the protection of local values...” which if mishandled can effectively lead to “...an informational impoverishment of the Internet...” (Schultz, 2008:799). Regardless of whether authors support or are opposed to the balkanisation model, the general academic consensus within the literature is that the fragmentation of the Internet by modality of local territorialism or discrete legal spheres; will ultimately detract from its efficacy.

The Internet in the International Security Context:

Achieving cybersecurity and information is a global issue that mandates the involvement of all users of ICTs; it cannot be realised by a scattering of state actors. Traversing the international legal landscape reveals a plethora of national laws and initiatives by multilateral and international organisations that have tried to foster cooperation on issues of cybersecurity and information security. This section outlines major developments in the field of ICTs in the context of international security. National and regional efforts are briefly outlined, but only the account of UN activity is in depth. The UN is employed as a lens to focus the scope of the literature. The rationale behind focusing on the UN lies in that in the current global context it serves as the primary intergovernmental organisation informing state policies and boasts the greatest capacity to promote international cooperation. State actors tend to boast individual policies; meaning literature on the issue is extremely broad, divergent and exhibits different levels of complexity. Developments as they relate to the UN are seen as the most useful in terms of providing a general idea of the field. Furthermore issues of Human Rights tend to fall to the UN, so in this study it is perceived as the actor most suited to address concerns of Internet freedom (Bowcott, 2011).

Societies in the 21st century have demonstrated a growing dependency on ICTs. However, because ICTs are globally interconnected risks and interdependencies that must be addressed not only at the national, but at the regional and international level as well, have manifested. Augmenting cybersecurity and ensuring the protection of critical information infrastructures has been deemed essential to the security and economic prosperity of the nation state. At the national level, this has often been framed as “...a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and civil society...” (ITU, 2016 b). States have taken individual action and implemented policies to protect their own network/computer systems and critical infrastructures. Examples of *some* of the state policies and programs implemented by the US, Japan and Australia are included to give a scant indication of the nation state’s interaction with cybersecurity and the Internet.

The Japanese government formed the Advanced Information and Telecommunications Network Society (AITNS) (Act No. 144, 2000), implemented the e-Japan Strategy and its Special Action Plan on Countermeasures to Cyber-Terrorism of Critical Infrastructure (IT Strategy Headquarters, 2001; IT Strategy Headquarters, 2000). The Australian government

published a report on ‘Australia’s National Information Infrastructure: Threats and Vulnerabilities’ in 1997 (Westby, 2004:75), established the E-Security Coordination Group and introduced a Cybercrime Bill in 2001 (Waters *et al.*, 2008:122; Parliament of Australia, 2001). Under the Clinton administration the US established the ‘President’s Commission on Critical Infrastructure Protection’ (PCCIP) (Cavelty, 2007:10).¹⁴ Further policies include the US 2015 Cybersecurity Act (US Congress, 2015), DOD Cyber Strategy (US DoD, 2015), and the Cybersecurity National Action Plan (The White House, 2016). It is evident that state strategies for cybersecurity and ICT infrastructure protection are not uniform or consolidated in a single instrument. Rather states tend to incorporate multiple documents and different instruments, and adopt a fragmented approach to dealing with cyber-threats that culminate to form what is usually referred to as a National Cybersecurity Strategy (ITU, 2016 b).¹⁵

Interdependencies have also warranted greater regional co-operation. Examples of regional responses to cybersecurity and critical ICT infrastructure protection are illustrated by the development of the United Kingdom’s (UK) ‘UK Government Strategy for Information Assurance’ and the formation of the UK Government Computer Emergency Response Team (CERT), as well as the central role that the Asia-Pacific Economic Cooperation (APEC) takes in co-ordinating much of the cybersecurity activity in Asia (Westby, 2004:71-72). One of the most successful examples of regional co-operation stems from the Council of Europe’s (CoE) promulgation of its ‘Convention on Cybercrime’, which is recognised as the first international treaty that has sought to tackle issues concerning the computer crime and the Internet thorough legislating and co-ordinating laws in a multinational forum.¹⁶

With regards to efforts concerning security and the Internet at the international level, activities conducted under the guises of the United Nations serve as arguably the best indicator of progress on the issue. The UN “...has been extensively involved in the development of cyber security policy at the international level...”, evident in that as early as 1990 issues of international cooperation in cybercrime investigation were adopted by the

¹⁴ “In 1997, the PCCIP concluded that the security, the economy, the way of life, and perhaps even the survival of the industrialized world were dependent on the triad of electric power, communications, and computers. Furthermore, it stressed that advanced societies rely heavily upon critical infrastructures, which are susceptible to physical disruptions of the classical type as well as new virtual threats...” (Cavelty, 2010:10).

¹⁵ For a list of publicly available National Cybersecurity Strategies, refer to the ‘National Strategies Repository’ compiled by the ITU (ITU, 2016c).

¹⁶ Although the CoE is a regional grouping, it is primarily a multinational organisation. Several observer states located outside of Europe, such as Canada and South Africa played an active role in the drawing up of the Convention on Cybercrime. Most are signatories but not all have ratified the treaty (CoE, 2016).

Congress on the Prevention of Crime and the Treatment of Offenders and in 1995 the UN published its *Manual on the Prevention and Control of Computer Related Crime* (Westby, 2004:82).¹⁷ What follows is a demarcation of the UN's further ventures into the cyber-domain; accomplished by providing succinct elucidations of Resolutions passed by the UN General Assembly pertaining to cybersecurity and information security.

UN Resolutions Related to Cybersecurity:

AS the proliferation of ICTs continues to increase and opportunities for real-time borderless exchange grow, cybersecurity has developed into a complex global issue that demands transnational cooperation in order to ensure the safety of the Internet. The dramatic increase in threats to cyberspace (particularly cybercrime) has led different UN organs to develop numerous policies and instruments that seek to address the issues and challenges around cybersecurity. This section puts forth an enumeration of the various Resolutions adopted by the UN General Assembly on the issue of cybersecurity in an attempt to map the international legal landscape.

Resolution 55/63, adopted by the UN General Assembly in January 2001 placed on the agenda 'Combating the criminal misuse of information technologies'. In this Resolution the General Assembly members recognised the contributions and efforts of several different organisations and bodies that sought to develop strategies towards preventing the criminal misuse of information technologies. The Resolution goes on to invite member states to adopt various measures¹⁸ to combat such misuse and provides that states "...should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies..." and recommends educating both the public and law enforcement officials on issues of cybercrime (UN, 2001). In legislating, the Resolution emphasises the need for Member states to uphold privacy and individual freedoms, whilst concomitantly ensuring that national governments maintain the capacity to combat misuse.

Resolution 56/121, adopted by the UN General Assembly in January 2002 once again placed on the agenda 'Combating the criminal misuse of information technologies'. In this

¹⁷ "This extensive document examines a wide range of issues related to crime and technology, including procedural law, substantive criminal law, international cooperation, data protection, security and privacy..." (Westby, 2004:82).

¹⁸ Some of the measures addressed in comparable international cybercrime prevention initiatives include the criminalization of illicit online activities "...information exchanges..." and "...cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies..." (UN, 2001).

Resolution the General Assembly inspired by the work of the CoE Convention on Cybercrime and other international and regional organisations' efforts; and sought to encourage the development of a global legal framework for combating cybercrime. In this Resolution, that value of the measures set out in Resolution 55/63 were reiterated and member states were invited to "...take into account, as appropriate the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organisations..." in developing legislation to combat the criminal misuse of information technologies (UN, 2002).

Resolution 57/239, adopted by the UN General Assembly in January 2003 placed on the agenda the 'Creation of a global culture of cybersecurity'. In this Resolution, the General Assembly emphasised "...that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society..." and demarcated the 'Elements for creating and fostering a global culture of cybersecurity'; inviting member states and all relevant international organisations to take account of them in their preparations for the WSIS and encouraging members to work towards incorporating these elements in their own countries (UN, 2003). The resolution also stressed the need to provide technical assistance to developing countries, recognising that a divide in technological capacity amongst states can diminish the effectiveness of cooperation in combating the criminal misuse of information technologies and undermine the creation of a global culture of cybersecurity.

Resolution 58/199, adopted by the UN General Assembly in January 2004 placed on the agenda the 'Creation of a global culture of cybersecurity and the protection of critical information infrastructures'. In this Resolution, the General Assembly built upon its assertions from Resolution 57/239 and noted the "...increasing links among most countries' critical infrastructures...and the critical information infrastructures that increasingly interconnect and affect their operations..." (UN, 2004). In addition to considerations of the impact on the relationship between critical infrastructures and ICTs the Resolution outlined 'Elements for protecting critical information infrastructures'; again stressing the need to address "...the gaps in access to and the use of information technologies by states..." through technological transfers and capacity building so as to protect critical information infrastructures and encourage socio-economic development (UN, 2004).

Resolution 64/211, adopted by the UN General Assembly in March 2010 placed on the agenda the ‘Creation of a global culture of cybersecurity and tacking stock of national efforts to protect critical information infrastructures’. In this Resolution, the General Assembly invited member states to assess their efforts to date towards strengthening cybersecurity by providing a ‘Voluntary self-assessment tool for national efforts to protect critical information infrastructures’ which states could use to take stock of their cybersecurity needs and strategies. The Resolution also encouraged member states and relevant regional and international organisations to share their best practices and measures developed to deal with cybersecurity and for the protection of critical information infrastructures in an effort to assist other member states to develop their own strategies for doing so (UN, 2010).

UN Resolutions Related to Information Security:

Resolution 53/70, adopted by the UN General Assembly in January 1999 placed on the agenda ‘Developments in the field of information and telecommunication in the context of international security’. In this Resolution, the issue of information security was introduced to the UN agenda for the first time with the General Assembly acknowledging that the dissemination and use of information “...technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States...” (UN, 1999). The Resolution called upon member states to give consideration to existing or potential threats pertaining to information security at a multilateral level and share their views on issues of information security. Since its introduction to the General Assembly agenda, “...there have been annual [R]esolutions calling for the views of UN Member States on the issue of information security...” (UNODA, 2015).

Resolution 70/237, adopted by the UN General Assembly in December 2015 placed on the agenda ‘Developments in the field of information and telecommunication in the context of international security’. Information security has become a standing agenda issue for the UN General Assembly.¹⁹ In the Resolution, the General Assembly notes that substantial progress has been achieved globally due to the development and application of the most up to date

¹⁹ By recalling Resolutions; 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25, 65/41, 66/24, 67/27, 68/243, and 69/28, Resolution 70/237 takes into account previous assertions and developments on the issue of information security put forth by the UN (UN, 2015). Resolution 70/237 provides an up to date summary of all the preceding Resolutions, so they have been excluded both for the sake of pragmatism and due to the format constraints placed on this study.

information technologies and means of telecommunication, which have in turn facilitated; the increased potential for the development of civilization, the enhancement of creative potential and the expansion of opportunities for the benefit of all states. The General Assembly carries through the sentiment of previous Resolutions, expressing concern that these technologies could be exploited in a manner that is adverse to the objectives of international stability and security, as well as the integrity of state infrastructure security.

In Resolution 70/237, the agenda reiterates “...that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes, *Noting* the importance of respect for human rights and the fundamental freedoms in the use of information and communication technologies...” (UN, 2015). In Resolution 56/19, it was decided necessary to appoint a Group of Governmental Experts (GGE)²⁰ to conduct a study of the relevant international concepts of strengthening global ICT systems. (Westby, 2004:85). Resolution 70/237 welcomes the effective work of the GGEs and calls upon Member States to make use of the assessments and recommendations outlined in the report developed by the 2015 GGE, and to further promote multilateral co-operation on the issue of information security (UN, 2015).

Of the four GGEs, the first failed to produce a substantive report in that an accord could not be reached amongst the experts over two pivotal policy issues. The first pertained to disagreement over the amount of emphasis that should be placed on the impact of ICTs on national security and military concerns and whether the report should incorporate language that warned of the potential threats posed by state exploitation of ICTs. The second disagreement was on whether the report should address concerns of information content or whether the focus should be limited to concerns of information infrastructure (UNODA, 2015).²¹

The second GGE, was established in 2009 and successfully issued report A/65/201 in 2010 (UN-GGE, 2010). The report included recommendations about the; “...Dialogue on norms for State use of ICTs to reduce risk and protect critical infrastructure, Confidence-building and risk-reduction measures,...Information exchanges on national legislation and national

²⁰ There has since been four GGEs that have focused in researching both potential and existing threats in the cyber-domain and how best to address them in terms of international co-operative measures.

²¹ Procedural matters of the GGEs work was published in UN document A/60/202 (UN-GGE, 2005).

ICT security strategies, policies and technologies, Capacity-building in less developed countries...and Elaboration of common terms and definitions on information security...” (UNODA, 2015).

Following the success of the second GGE, the UN General assembly called for a follow-up in Resolution 66/24, with the third GGE being unanimously approved and established in 2011. The third GGE made grounds by succeeding in gaining consensus in a substantive report; A/68/98* which was issued in 2013 (UN-GGE, 2013). In the report the Group reached posited that “...International law, in particular the UN Charter, is applicable to the cybersphere,...State sovereignty applies to States’ conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory, States must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-State actors for unlawful use of ICTs, [t]he UN should play an important role in promoting dialogue among Member States...” (UNODA, 2015).

Following the success of the third GGE, the UN General assembly called for a follow-up in Resolution 68/243, with the fourth GGE being unanimously approved in 2013 and established in 2014. The fourth GGE agreed on a substantive consensus report; A/70/174 which was issued in 2015 (UN-GGE, 2015). In the report the Group focused on issues regarding; existing and emerging threats, norms, rules and principles of responsible behaviour of States in the cyber-domain, confidence-building measures, and recommendations for international co-operation and capacity building. The Group made progress in the area of determining how international law should be applied to the use of ICTs by states, highlighting the importance of the Charter of the United Nations in particular. In calling for increased exchange of information and assistance to prosecute terrorist and criminal use of ICTs, the Group again emphasised the need for states to “...guarantee full respect for human rights and fundamental freedoms...”, including privacy and freedom of expression (UN-GGE, 2015). Following a unanimous decision by the UN General Assembly, Resolution 70/237 has called for a fifth GGE to be established in 2016/2017.

Conclusion:

To conclude; the terminology, policies, infrastructure and institutions associated with the operation and governance of the Internet demonstrate a highly esoteric body of knowledge.

As this is an exploratory study, delineating governance modalities provides a framework under which possible future policies can be designed. As such, this chapter has taken Internet Governance as a starting point for the research and has aimed to develop a concise base of understanding for the subsequent study. The first section of this chapter elucidated upon the various facets of Internet governance. First the concept was defined; thereafter the various governance modalities were identified and their practices expounded. This study distinguishes between five types of Internet governance; Standardization and Protocol Governance; Structural Management Governance; Intellectual Property Governance; Internet Security governance; and Internet Filtering Governance. The field of Internet governance proves highly dynamic as competing interests and technological innovation render it ever changing. After demarcating the modality typologies, the study attempted to outline possible trajectories for the Internet's future so as to ensure trends in Internet Governance are accounted for, as changes in the architecture of the Internet will also affect future policies and the conditions under which they operate.

Thereafter the study attempts to shift the research towards a security frame by focusing on security discourses and instruments in the international context that are linked to cybersecurity and information security. On matters of the Internet and security, these areas are afforded the greatest attention by the international community. The sheer scope and variegation of policies and practices amongst states on issues relating to cybersecurity and information security, mandates the need to adopt a focal lens. Focusing on the UN's Resolutions pertaining to cybersecurity and information security served to narrow the scope of the literature. With regards to resituating the chapter in terms of the research problem and questions, the study has sought to discern the legal landscape under which states and international organisations must manoeuvre, on issues concerning the technical operation and security of the Internet. This is imperative in order to grasp the framework under which countermeasures to cyberjihad must be developed and also to comprehend the inherent complexities and challenges that arise from private sector involvement and lack of consensus amongst states on how the Internet should be governed. Considerations regarding the future of the Internet's architecture also points to a potential downside of securitisation, in that balkanization. In the subsequent chapter, this study attempts to segue from security considerations and policies, into theoretical arguments that address security; namely the field of Security Studies. Specifically, The Copenhagen School's Securitisation Theory is selected as the guiding theoretical supposition in this study. Chapter 3 will both summarise the

principles of the theory and justify why it is most appropriate for addressing the issue of cyberjihad.

CHAPTER 3: Theoretical Grounding – The Copenhagen School's Securitisation Theory

Introduction:

As this is an academic study, it is mandatory to ground the research in a theory of International Relations. Securitisation Theory has been selected as the guiding theoretical framework. The first section of this chapter locates the theoretical underpinnings of Securitisation Theory within the broader cognitive discipline of Security Studies. The development of Security Studies reveals that its scholastic agenda has been greatly influenced by external events. After demonstrating the development of the study into a sub-discipline of International Relations, the most prominent epistemological debates are highlighted before leading into a brief overview of mainstream theoretical approaches in the field. The second section proceeds to put forth a coherent account of the Copenhagen School's Securitisation Theory. Finally, the last section aims to prove the utility of Securitisation Theory in this study by applying the theory to the contemporary security context and demonstrating that; of the major IR theories, Securitisation Theory boasts substantial explanatory power with regards to issues of the Internet and cyberspace.

Security Studies – Development, Debates & Theoretical Approaches:

The Development of Security Studies:

Security is a unique manifestation of politics, in that although all security issues are politicized, political conflicts do not always escalate into security concerns. Should discordant actors seek a non-violent resolution to their disputes, the solution has been to reach a settlement based on shared rules, institutions or principles. If an accord is reached, the political issue persists, yet the security dimension of the issue is diminished. In the event that an actor opts to use or threaten the use of force to resolve a political dispute, the security dimension surfaces as a crucial aspect of the conflict (Kolodziej, 2005:22). Within the guise of International Relations, the chief purpose of Security Studies has been to understand and explain how and why actors use force, and in concurrence whether force works. What follows is an ontogeny of Security Studies, which is presented as a historical narrative in light of the fact that research in the field "...has been heavily shaped by changing international conditions..." (Walt, 1991:228).

The development of Security Studies can be traced back to a time that precedes the Second World War (WWII). Antecedent academic literature denotes content pertaining to War Studies, geopolitics, Military History and grand strategy. Subsequent to the conclusion of WWII, the debates that followed were borne out of concern over how to protect the nation state against internal and external threats alike (Buzan & Hansen, 2009:8). As research evolved in tandem with changes in the global context, ‘in the interest of national security’ became a maxim for international relations political discourse, ultimately distinguishing it from earlier thinking and the disciplines from which it developed. The term ‘security’ has come to denote an objective of policy (Wolfers, 1952:483), and has served as a conceptual link that has bridged together programmes in an increasingly diverse research agenda.

Though security had become a new cardinal concept in the post-WWII context, it was not until the later years of the Cold War that its capacity for extending the field beyond military-political understandings became apparent. Much of the Cold War is described by its predominantly military agenda of “...questions surrounding nuclear weapons and a widely embedded assumption that the Soviet Union posed a profound military and ideological threat to the West...” (Buzan & Hansen, 2009:2). The bipolarity of the Cold War system was structured, quite disconcertingly so, around the nuclear capacity of the Soviet and American superpowers, yielding a dubious yet ostensibly unchanging and uncontested global order. By this corollary, neither superpower had reason to attack in that doing so would more than certainly risk obliteration. Furthermore, both powers maintained an incentive to keep their allies in check and limit conflicts, so as to mitigate the threat of nuclear war. Hence, “...the Cold War nuclear bipolar balance of power appeared to offer an uneasy peace, orchestrated under the directing batons of two rational, prudent superpowers...” (Kolodziej, 2005:11-12). As the superpower relationship matured, complexities and dimensions intrinsic to the term security resurfaced in the 1970s resulting in a greater push to extend the global security agenda beyond the military-political focus.

Economic and environmental issues were begrudgingly added to the security agenda in the 1980s, soon followed by the inclusion of issues such as food security, societal security and human security in the 1990s. The dominant national security frame of the Cold War continued to inform much of this literature in that these facets were incorporated because of their bearing on the threat, use and control of force. Hence they were included because of their impact on military issues, rather than because they were security concerns in their own

stead. Conceptions of security were not problematised and were deemed important only insofar as they were grounded in military, strategic and Realist political and academic debates. This would not go uncontested, as some of the literature "...began to challenge the emphasis on material capabilities as well as state-centric assumptions, opening paths to studies of the importance of ideas and culture and to referent objects for security other than the state..." (Buzan & Hansen, 2009:2). Scholars such as Richard Ullman sought to encourage a conceptual shift in the mindset of policy-makers, stating that traditional understandings of security were defined "...in excessively narrow and excessively military terms..." (Ullman, 1983:129). For Ullman, such an underdeveloped concept of security resulted in a preoccupation with military issues, which served to undermine the potential threat of other concerns. Furthermore, this manner of thinking served to advance the inescapable militarization of international relations, ultimately resulting in the reduction of total global security.

Writings such as this began to appear at the closing stages of the Cold War in tandem with increasingly radical and critical challenges to the state-centric status quo "...with the result that instead of flowing as a single river within one set of quite narrowly defined banks, [Security Studies] has broadened out into several distinct but inter-related flows of literature..." (Buzan & Hansen, 2009:2). The unraveling of the Cold War and the Soviet Union's demise resulted in the collapse of the bipolar global system. So too did the precarious stability afforded by the superpower competition come to an end, leaving in its wake a far more complex global order that has defied understanding and a new world "...beset by unprecedented security threats, dramatized by global terrorism and the diffusion of weapons of mass destruction..." (Kolodziej, 2005:11). Since the Cold War Security Studies have since expanded beyond the more traditionalists, military-centric studies to include new research programmes such as Constructivist Security Studies, Feminist Security Studies and Post-structuralism.

Whilst the guiding theme of the research in these fields is 'security', lack of conceptually explicit discussions during the Cold War has meant that the term itself has yet to be universally defined and instead has dissolved into a site of conflict for disciplinary politics with diverging understandings and perspectives. In their Handbook of Security Studies, Cavelty and Mauer maintain that "...[m]ost researchers would agree that security is somehow related to a threat to a given object of protection, and that it is most often linked to

survival...”, hence linking the concept to existential concerns and high stake issues that legitimise emergency actions (Cavelty & Mauer, 2010:2). However, conflict persists in that even when policy-makers, theorists and observers settle on a common understanding of security they are still hampered by efforts to apply it as a conceptual tool in policy-making due to the terms ability to encompass a range of goals so exceedingly wide that “...highly divergent policies – say combating global poverty or terrorism – can be interpreted as policies of security...” (Kolodziej, 2005:21).

The lack of consensus and absence of a universal definition on the meaning of security has led to observations over the years that it is an essentially contested concept. What’s more, because security is a condition it is permeated by values and emotions, rendering security not only a contested concept, but also a site for contested values. “Strong subjectivity is an inevitable side effect of this – and therefore, security will always mean different things to different people...”, whilst remaining a normative enterprise in itself (Cavelty & Mauer, 2010:2). It is quite fitting then, that security has been referred to as a “...Tower of Babel...” in that the augmenting and multiplying of definitions has resulted in pronounced confusion regarding its conceptual underpinnings, made further incoherent by the myriad of academic literature that has failed to “...keep pace with rapidly changing events, notably those impacting security...” (Kolodziej, 2005:11). Not only has Security Studies been subjected to substantial changes over recent decades, currently it is arguably the most dynamic area in International Relations.

The intrinsic analytical difficulties security poses to disciplinary politics and their diverging perspectives are encapsulated in Stephen Walt’s *The Renaissance of Security Studies*, wherein in he simultaneously warns of the dangers of broadening the research agenda of security, as well as the need to ensure that theory remains relevant in terms of its political applicability. Walt locates his assertions in Realist sentiment by positing that Security Studies must pursue cumulative knowledge regarding the role of force and the military because should research in the field continue to fixate on immediate policy issues at the expense of enduring research questions, a decline in the rigor and quality of theory is inevitable (Walt, 1991:222). Yet he maintains that the alternative may jeopardize the development of Security Studies even more so, in that the field has benefited from its link to contemporary and real world issues. Should Security Studies yield to the inclination of academic disciplines to pursue “...the trivial, the formal, the methodological, the purely theoretical, the remotely

historical- in short the politically irrelevant...” (Morgenthau, 1966:73), Walt maintains that the theoretical progress and practical value of the field will certainly decline.

Where then should the line be drawn in terms of what is included and excluded in Security Studies. If the point of departure were taken to be an extensive understanding of security that is contiguous with the perspectives of a given observer, then a definition of security would be the equivalent of proclaiming every human interest and value (perceived by those implicated) to stand as a security issue. This conception is too capacious and serves to undermine the furthering of research in the field. Contrarily, if a more limited understanding of security is applied, recognised exclusively in terms of its relation to coercive threats and force, theorists risk the exclusion of actors and dynamics, which are of vital pertinence to security. “We will be unwittingly relying on conceptual filters that project widely contrasting and refracted images of what security is and how to address it...”(Kolodziej, 2005:2). An inclusive and holistic understanding of security thus mandates the incorporation of a broad array of threats and referent objects that go beyond the state, as well as those non-violent stratagems and mechanisms employed by actors so as to overcome the impetus to evoke force and threats to settle conflicts.

In this conspectus of Security Studies a commodious definition of security is applied so as to ensure that the scope of understanding encompasses the often oppugnant approaches and opinions of actors in security. In doing so, more discerning applications of theory within the discipline of International Relations is possible. In his classic work “*National security*” as an *ambiguous symbol*, Wolfers’ states that “...security, in an objective sense measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked...” (Wolfers, 1952:485). This definition is used as a starting point to developing an understanding of security, as it reminds scholars that whilst security is afforded a degree of primacy in IR, it remains intrinsically subjective. Credence is afforded to this definition in that it reminds theorists “...it is a ‘sweeping generalisation’ that all states tend to pursue a ‘uniform and imitable policy of security...”, furthermore Wolfers draws attention to the flexibility of the term ‘security’ and how it is crucial to remain mindful of the manner in which it is manipulated by policy-makers (Hughes & Lai, 2011:1). By highlighting the tendency of policy pertaining to security to be privileged over other national interests, Wolfers emphasises the rhetorical and political force imbued in the term ‘security’ despite its lack of inherent meaning (Buzan & Hansen 2009:1).

Epistemological Debates in Security Studies:

Having already outlined points of contention in the preceding subsection it should be clear that far from progressing towards a cohesive stream of research, Security Studies has demonstrated astonishing diversity methodologically, substantively and even politically (Walt, 1991:231). As mentioned at the beginning of this chapter, the development of Security Studies into the body of work it is today has been heavily influenced by the debates that took place in the later stages of the Cold War, regarding what should be included and excluded in the field. These clashes have come to be regarded as the ‘traditionalists vs. wideners-deepeners’ debates. To elucidate, traditionalists remain opposed to broadening the scope of Security Studies beyond the boundaries of studying the threat, use and control of military force. State-centric assumptions persist in the interest of intellectual and conceptual cohesion. Conversely, wideners have sought to include facets such as the economy, the environment, society and political concerns to the research agenda, whilst the deepeners – who are usually the same researchers pushing for the widening of Security Studies – have sought to include supplementary units of analysis that exceeds the emphasis on the state maintained by the traditionalists. Most notably, the deepeners have posited the notion that “...there are five levels of depth to security: international systems, international subsystems, units, subunits and individuals...” (Cavelty & Mauer, 2010:2).

Broadly speaking, Security Studies has been regarded and subsequently researched as a sub-field of IR. Consequently, much of the conflicts that have dictated the development and contours of International Relations Theory, have been transposed to Security Studies. As it stands, Security Studies is imbued with the same epistemological and methodological debates that arise from the opposing positions held by positivist/rationalist theory and post-positivist/critical theory or approaches. These entrenched positions can be summated by the ostensible conflict that exists between the ‘American’ and the ‘European’ approaches to security with the former being “...predominantly concerned with offensive versus defensive realism; the role of power; and institutions in order/empires...” and the latter “...on the emergence of various critical schools such as the ‘Copenhagen’, ‘Welsh’ (Aberystwyth) and ‘Paris’ Schools...” (Cavelty & Mauer, 2010:3). With regards to the analytical principles applied to Security Studies, positivist research in IR seeks to imitate as much as possible the practices of the hard science and migrate their processes to the social sciences. That is to say, positivist theory seeks to establish a causal relationship so as to render their claims falsifiable.

Adversely, post-positivists maintain that non-positivist theory is better suited to dealing with the complexities of the problems, in which the social sciences are invested. In terms of security, post-positivists engage with the conceptual processes of threats are created and imbued with meaning, which they maintain are "...better understood through an analysis of identity building and institutional transformation that does not lend itself to causality or quantification..." (Buzan & Hansen, 2009:35).

The other epistemological debate that continues to draw attention in both IR and Security Studies, points to the tensions outlined in Wolfers definition of security, that is to say between objective, subjective, as well as discursive understandings of security. By positing that "...security, in an objective sense measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked...", Wolfers serves to illustrate the friction that exists between objective and subjective conceptions of security (Wolfers, 1952:485). Whilst objective approaches strive, although don't always succeed, to define security in terms of material capabilities and the states capacity to threaten or intimidate enemies through material means, subjective conceptions of security underline the significance of ideational factors that impact the way threats are framed, such as history, relational contexts, norms and the psychological implications of fear and perception. Because the 'psyche' of states is not uniform (rather they are variegated and can range from paranoid to rational), post-positivist maintain it is mandatory to supplement material capabilities with non-material factors. "Subjective approaches do not, in other words, dispense with an objective definition of security, but contrast it with the 'filter' of the subjective..." (Buzan & Hansen, 2009:33). It is worth noting that subjective conceptions are inherently at odds with positivist approaches in that the subjective frame of mind is not quantifiable. Actors who seek to attain security are not amenable to controlled testing, thus it is not possible to conduct an analysis through scientific methodology (Kolodziej, 2005:19).

In contradiction to both these approaches, discursive conceptions assert that it is not possible to define security objectively, rendering both subjective and objective processes inherently erroneous. Rather than focus on the material or ideational factors concerning understandings of security, discursive approaches emphasise the importance of the intersubjective processes that serve to inform the manner in which threats are constructed and are linked to security concerns that have been inducted into political agendas. The manifestation of security is attributed to 'speech acts' and the discursive construction of threats. These threats are not

inherently objective; rather they assume a sense of objectivity only when political actors accept them to be threatening as such. Politicisation of security issues thus requires relevant audiences to be convinced that an issue is a threat in itself (Buzan & Hansen, 2009:34). Pronounced diversity amongst competing theories has served to benefit rather than hinder the development of the field, in that it has generated greater interest due to its broad spectrum of options on how to interpret security issues.

Mainstream Theoretical Approaches in Security Studies:

Research regarding security has been analytically rich and fertile, as competing schools of thought in IR have all sought to develop and validate theories and approaches within the sub-field of Security Studies. In the post-9/11 context, the already substantive body of work devoted to Security Studies has been afforded even greater attention. This section seeks to briefly outline the primary tenets of three of the prominent schools of thought in Security Studies, so as to ensure an indiscriminate account of existing theory is provided. The “...major trajectories of [I]nternational [R]elations theory throughout most of the twentieth century...” have been Realism, Liberalism and Constructivism (Choucri, 2012:14). Attention is afforded to these schools, not because of their portended dominance in IR, but because the theoretical focus of each represents a distinct ‘problématique’; which allows for a novel attempt to account for the complexities and abundance of theory in the field of Security Studies.

It is not feasible to develop a contemporary understanding of Security Studies without acknowledging the contributions of Realism. Realism imposes three core assumptions on the dynamics of the world, so as to demonstrate a relationship between political order and security. First, the assumption of ‘groupism’ is made in that politics must take place amid or amongst groups. For realists, the state is perceived as the most important and cohesive human group. The second tenet is based on ‘egoism’ and the assumption that individuals and groups are intrinsically driven by narrow self-interest, which will always serve to trump altruism when a given actor is placed under pressure or strain. The final assumption is based on ‘power-centrism’, wherein primacy is afforded to power and power-relations as the “...fundamental feature of international affairs and political life more generally...” (Gilpin, 1996:7-8).

Realists characterize human interactions in terms of inequalities of power, both social and material, and point to politics as the location wherein these interactions play out continuously with the possible use of coercive material power. In light of these primary assumptions, Realists have reached the conclusion that the world is anarchic and politics is inherently prone to conflict because in the absence of an omnipotent authority to enforce agreements, actors are reduced to a contingency wherein force is the most feasible means of pursuing goals. Thus the central realist argument is that "...anarchy renders security problematic, potentially conflictual and is a key underlying cause of war...", simply put "...insecurity is endemic to anarchy..." (Wohlforth, 2010:10). As such, much of the Realist research agenda in Security Studies is dedicated to understanding how security concerns materialise within inter-group relations. Debates and application of realist theory to the realities of the international context have led to the development of several sub-schools of Realism, most markedly Neorealism (Waltz, 1979), Offensive and Defensive Realism (Van Evera, 1999) and Neoclassical Realism (Rose, 1998).

Liberalism tends to be less pessimistic in its understanding of security. Liberals have greater faith in the pacifying effect of democratic and economically interdependent states and their potential to stabilise the global system (Rousseau & Walker, 2010:21). Much like Realism, there are three assumptions informing liberal claims. First, democratic peace theory assumes that democracy serves to reduce military conflict as it is less probable for a democratic state to instigate or escalate conflicts with other states. The second assumption is based on increased economic interdependence and the belief that as states become more connected by the flow of goods, labour, services, technology etc., the resultant interdependence will reduce the likelihood of military conflict and promote peace. The final assumption posits that democratic states are more inclined to reach solutions that mandate cooperation because of international institutions. International institutions are believed to decrease the probability of conflict and increase the probability of cooperation for reasons such as their capacity to monitor compliance, as well as mediate and arbitrate disputes (Russett & Oneal, 2001).

Thus, one of the defining facets of Liberalism is its optimistic claim regarding the capacity for human reason to encourage the dissemination of prosperity and peace in the world. Liberalism seeks to extend the security agenda beyond the state so as to include other organized social groups and firms. By refraining from placing an emphasis on military force, liberals seek to understand how different actors organise themselves in a manner that avoids

conflict. "...[L]iberalism believes in at least the possibility of cumulative progress, whereas realism assumes that history is not progressive..." (Keohane, 2002:45). Noteworthy sub-schools of Liberalism that have had a bearing on Security Studies include Commercial Liberalism (Moravcsik, 2001) and Neoliberal Institutionalism (Keohane, 1984; Axelrod, 1984).

Historically, both Realism and Liberalism have been dominant traditions in IR, however Constructivism has developed into an increasingly prominent theoretical approach in the field, particularly with regards to Security Studies. Constructivists have drawn from sociological approaches and augmented critical theory, to develop the argument that "...the world is constituted socially through intersubjective interaction; that agents and structures are mutually constituted; and that ideational factors such as norms, identity and ideas generally are central to the constitution and dynamics of world politics..." (McDonald, 2008:59-60). Although all Constructivists maintain a shared belief in the pervading importance of identity in the construction of security, there is variegation in how they establish the relationship between security and identity. Whilst there is pronounced disagreement amongst constructivists on the issue of how international politics should be studied, partisans of the tradition are unified in their critique of the perceived inadequacies of preponderant behavioural approaches and paradigms, which they maintain have failed to sufficiently understand and expound upon security (Kolodziej, 2005:7).

This is because, for Constructivists, security is a social construction that must be located in a specific context before meaning is derived and it is possible to analyse the impact on political practice. Security is perceived "...as a site of negotiation and contestation, in which actors compete to define the identity and values of a particular group in such a way as to provide a foundation for political action..." (McDonald, 2008:67). This relentless process of identity transformation, social construction and actor reaffirmation is crucial to understanding the rise and fall of specific security concerns. In the security context, the most revered school of thought to stem from the Constructivist approach is most certainly the Copenhagen School, which in itself is an exception in Constructivism. Rather than simply serving as a broader social theory of how analysts and researchers should approach the study of security, the Copenhagen School develops an explicit framework for understanding how security is constructed by means of 'speech acts' that delineate specific actors or issues as existential threats (Buzan, Wæver & de Wilde, 1998).

Credence has been given to Constructivism, Liberalism and Realism due to the substantial influence they display in the Security Studies research agenda. Yet the considerable contributions and quantity of literature produced by critical approaches to security must not be excluded. These critical approaches have developed views that seek to be more inclined to normative concerns, maintain greater political awareness and to be more sociologically and historically grounded. By introducing critical issues into the political agenda, critical perspectives in IR Security Studies have developed conceptions of security that can usually be defined as a commitment to emancipation. A sufficient overview of the most prominent critical perspectives in security issues calls for the inclusion of Human Security, Feminist Security, Post-colonial security and perspectives from the Welsh and Paris Schools. Of the numerous critical approaches to security that have been developed, it is the Welsh School that has explicitly sought to incorporate IR Critical Theory in its research agenda. In this approach, security is viewed as an epiphenomenon that is created intersubjectively through political discourse and differing worldviews.

Although scholars from the school have argued that it is necessary to broaden the security agenda beyond the military, they have done so whilst locating their assertions within the neorealist agenda. The Welsh school differs from the Copenhagen school in that although it seeks to broaden security conceptions by including those insecurities faced by different referent objects, it points to the need to 'politicise' rather than 'securitise' these issues. Whilst the Copenhagen school views desecuritisation as desirable, the Welsh school perceives security as a derivative concept that requires politicising and seeks comprehensive engagement with the realities of security (Booth, 1991). Those associated with the Paris school, have sought to develop a post-structural and more sociological approach that focuses on the operations and conduct of routine security activities such as border control and policing (Peoples & Vaughn-Williams, 2010:69).

Human Security argues that traditional conceptions of security have been narrow and have overlooked the legitimate security concerns of ordinary people in everyday life. There are two tenets guiding Human Security, the first points to the need for "...safety from such chronic threats as hunger, disease and repression..." whilst the second tenet necessitates "...protections from sudden and hurtful disruptions in the patterns of daily life..." (Paris, 2011:71). Because the scope of this definition is so vast, much of the literature in Human

Security has sought to narrow down and redefine security conceptions so as to remedy the expansiveness and ambiguousness of the term.

Feminist approaches to security have made gender the central category of analysis. Research in Feminist Security Studies has served to raise vital questions about the role of women in international security. By asserting and demonstrating that the experiences of men are privileged in security, research in the field has sought to increase the visibility and address the marginalization of women through gender structures that are apparent in both traditional and critical security studies (Tickner, 1992). Post-colonial perspectives in Security Studies have sought to bring about greater inclusion of the 'Third World' in security. Researches have argued that Security Studies are Western-centric and have almost exclusively focused on the experiences of the global North at the expense of the rest of the world. Both traditional and critical Security Studies are slated by Post-colonial approaches for their inability to recognize the inherent ethnocentrism of their research in the field (Acharya, 1997).

Securitisation Theory:

Having developed a succinct understanding of the Security Studies research agenda and of what 'security' means in International Relations, it is now possible to focus on the particular theoretical approach that has been selected to guide this investigation. This section puts forth the primary tenets of Securitisation Theory, as asserted by the Copenhagen School. What follows is a compendium of the assumptions, analytical tools, criticisms and contributions to IR of the Copenhagen School. As demonstrated in the previous section, Security Studies has proven to be one of the most dynamic and heavily contested fields of research in IR. Consequently, Security Studies has developed into a site in which "...some of the most vibrant new approaches to the analysis of international politics are being developed, and the realm in which some of the most engaged theoretical debates are taking place..." (Williams, 2003:511). This is most apparent in that despite 'security' being the forte of Realist and Neorealist theorising, it is arguably the foremost arena in which social constructivist approaches to theory have succeeded in challenging traditional assumptions. The contributions of the Copenhagen School's 'Securitisation Theory' is perhaps the most noteworthy and influential of these new approaches.

The Copenhagen School was borne out of a research project entitled 'Non-military Aspects of European Security', advanced by the Centre for Peace and Conflict Research in

Copenhagen (Huysmans, 1998:479).²² The framework for analysis applied by the Copenhagen School is somewhat radical in that it rejects the assumption that war and force is at the core of Security Studies. Instead, it opts to open up the security agenda to alternative types of threats (Buzan, 1997:13). At the outset, theorists associated with the Copenhagen School were opposed to the overtly normative approaches to studying security that had come to dominate the field in IR. Rather they posited that an attempt at an analytical approach was possible by applying the concept of ‘securitisation’, which serves to shift the focus of analysis towards understanding the implications that follow the invocation of the concept of security, particularly with regards to non-military concerns (Peoples & Vaughan-Williams, 2010:10). Barry Buzan and Ole Wæver are the theorists most revered and commonly associated with the school in that they are recognized as the founding fathers and developers of Securitisation Theory.

Barry Buzan’s *People, States & Fear: The National Security Problem in International Relations*, has served as the foundational text in Securitisation Theory (Buzan, 1983). In it, Buzan problematizes the conceptual underdevelopment of security and demonstrates how pervading understandings of the time were too narrowly founded, as they were limited to the scope of national security. With the goal of broadening the framework for security in mind, Buzan sought to develop a holistic view of security by remonstrating the need for further levels of analysis and the inclusion of social aspects of security, particularly pertaining to the manner in which threats are constructed. Wæver on the other hand is credited with introducing an understanding of security as a ‘speech act’, wherein the utterance of security itself serves to frame an issue as a threat. Security is instrumentalised through the process of ‘securitisation’, allowing political elites and the state to remove an issue from the normal realm of politics in that they alone claim a special right to deal with security problems. Moreover, Wæver coined the notion of desecuritisation;²³ which posits that securitising certain issues is not always an effective means to deal with the problem nor is it desirable in that it removes discussions on these issues out of the public domain (Wæver, 1995).

²² Established in 1985 by the Danish Parliament with the aim of nurturing and strengthening a multidisciplinary research agenda on peace and security. It has since developed into the Copenhagen Peace Research Institute (COPRI) (Huysmans, 1998:479).

²³ The shifting of an issue out of “...the realm of securitisation and emergency politics back into the realm of ‘normal’ political or technical debate (Peoples & Vaughn-Williams, 2010:76).

Drawing from their previous research, Buzan & Wæver have since collaborated with Jaap de Wilde to produce what now serves as the primary text informing Securitisation Theory, *Security: a New Framework for analysis* (Buzan, *et al.*, 1998). In this seminal work, Buzan, Wæver and de Wilde develop an innovative and encompassing framework of analysis with which to approach Security Studies. The chief mandate of the Copenhagen School has been to widen the security agenda beyond the narrow state-centric and military focus in a manner that would circumvent the inflation of the concept of security to the point that it encompasses all manner of threats to existence (Huysmans, 1998:482). Theoretical approaches to Security Studies that are derived from the Copenhagen school are concerned with asking the questions of why and how an issue is transformed into a security concern, as such the focus tends to be placed on concerns of domestic politics, principally those relating to insecurity and politics of threats (Cavelty & Mauer, 2010:3). It useful to note here that the claims of Securitisation Theory are specifically fixed to security issues in the international relations context, in that characteristics of security in this setting differ from its applications in daily language. Securitisation theory demonstrates the distinctive agenda of international security in that although it is instilled with some aspects of social security, "...international security is more firmly rooted in the traditions of power politics..." imbuing it with more extreme meaning (Buzan *et al.*, 1998:21).

The authors head traditionalist warnings that excessive widening of the agenda risks rendering the field intellectually incoherent, however they do not concede that retreating to the military core is the only way of dealing with concerns of coherency. Rather than confining their approach to the military sector, the authors investigate the logic of security itself in order to maintain continuity in their work. That is to say they seek to develop an understanding of what it is that serves to distinguish security and the process of securitisation from the realm of the political. Reconciling the dispute that exists between the traditionalists and the wideners thus calls for the construction of a concept of security that is imbued with more meaning than simply serving as a set threat or problem. Securitisation Theory accomplishes this by developing an understanding of security that takes into consideration social praxis and the framing of issues as existential threats.

Threats and vulnerabilities can arise in many different areas, military and non-military, but to count as security issues they have to meet strictly defined criteria that distinguish them from the normal run of the merely political. They have to be staged as existential threats to a referent object

by a securitising actor who thereby generates endorsement of the emergency measures beyond rules that otherwise bind (Buzan *et al.*, 1998:5).

Proponents of Securitisation Theory do not assume ‘security’ to be an objective condition, instead it is perceived as the outcome of a distinct social process. Much of its research focuses on the social construction of security and applies post-positivist approaches such as post-structuralism and critical theory, to challenge the assumptions of traditionalists and wideners alike. In line with Wæver’s earlier work (1995), Securitisation Theory seeks to transform security from a perception into a speech act. (Huysmans, 1998:492). By evoking the use of language theory and asserting that ‘security’ must be understood as a speech act, Securitisation Theory posits that

security is not of interest as a sign that refers to something more real; the utterance itself is the act. By saying it, something is done (as in betting, giving a promise, naming a ship). By uttering “security” a state- representative moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it (Wæver, 1995:55).

Securitisation Theory maintains that by examining the speech acts implicated in a given securitising move it is possible to discern the social constitution of a security issue; that is to say what or who is being made secure, and what are they being secured from. A distinction is made in that issues that have been ‘securitised’ (and henceforth are treated as security issues) become so because of speech acts and not because they describe an extant security condition. A threat is recognised as a security situation because it has been successfully represented as such through speech acts. By assuming this position, the Copenhagen School is able to “...argue simultaneously for both an expansion and a limitation of the security agenda and its analysis...” (Williams, 2003:513). Although regarding security to be contingent on a speech act could fundamentally allow for the indefinite extension of the Security Studies agenda, Securitisation Theory concomitantly limits the agenda by asserting that the concept of security is only expanded in so long as threats and referent objects are constituted in accordance to logic of urgency and extraordinary measures.

Securitisation is the casting of an issue as one of an ‘existential threat’. This serves as the distinguishing facet of the theory because it presents a specific rhetorical structure that links security to survival. Demarcation of an existential threat is possible by reviewing the level of response it garners, in that an issue regarded as an existential threat demands the use of

exceptional political measures (Peoples & Vaughn-Williams, 2010:76). Security discourse is evoked to dramatize and present an issue to be one of extreme concern and to take precedence over intersubjectively shared rules between the actor and the target audience. The label of security allows an actor to mandate exceptional measures to address an issue and prioritise action “...because if the problem is not handled now it will be too late, and we will not exist to remedy our failure...” Buzan *et al.*, 1998:26). By locating the survival of collective units and principles at the core of Security Studies, Securitisation Theory provides the foundations for the expansion of the security agenda beyond traditional military conceptions. Not only does the theory facilitate the application of security analysis to other sectors, it does so without degrading the concept of security itself (Buzan, 1997:15).

The authors of *Security: a New Framework for analysis* seek to demonstrate how the logic of securitisation can be applied across different sectors. In addition to the military sector, Securitisation Theory points to how the security of the human collective is also affected by the economic, political, environmental and societal sectors. Because there is no objective or universal standard of what can be considered a threat to individual human life, the theory asserts that “[e]xistential threat can only be understood in relation to the particular character of the sector and referent object in question” (Buzan *et al.*, 1998:21). Not only does the sector delineation render the analysis of securitisation more tractable, these sectors serve as an analytical lens with which to perceive the international system; in that they emphasise the attribution of specific relationship dynamics amongst its constituent units. By disaggregating security into different sectors, Securitisation Theory alerts researchers and analysts to the different referent objects threats and interaction that occur outside of the military core in security and it becomes possible to “...discern distinctive patterns or dynamics of security that are found in each...[and] to identify the likely securitising actors and prospects for securitisation...” (Peoples & Vaughn-Williams, 2010:80). These dynamics are summarised in the table that follows.

Table 2: Dynamics of Securitisation in accordance to Sector

<i>Sector</i>	<i>Type of interaction (Buzan et al.: 7)</i>	<i>Dynamic of securitization</i>
Military	Relationships of forceful coercion	Existential threat to state/populace/ territory/military capacity
Environmental	Relationships between human activity and the planetary biosphere	Existential threat to biosphere/species/ natural environment
Economic	Relationships of trade, production, and finance	Existential threat to markets/finance/ resources
Societal	Relationships of collective identity	Existential threat to collective identity/ language/culture
Political	Relationships of authority, governing status, and recognition	Existential threat to sovereignty/ organisational stability/ideology of a social order

Source: (People & Vaughn-Williams, 2010:80)

In addition to the inclusion of sectors as an analytical tool, Securitisation Theory engages with the debates pertaining to levels of analysis that have been central to IR theory. The argument here reasserts the aim of a more holistic and inclusive analytical process in security. As a project, Securitisation Theory was developed with the aim of introducing more diversity of security units to the Security Studies agenda. It rejects the position of privilege afforded to the state as a unit of analysis and maintains that IR should be wary of reinforcing state-centric thinking (Buzan *et al.*, 1998:7). Securitisation Theory asserts that security at the level of the individual is intertwined with security at the level of the state and the international system, thus the argument is made that not only would it be folly to pursue a research strategy that removes security from any single level, it is not conceptually possible to do so (Baldwin, 1997:7). For Securitisation Theory, it is essential for any concept of security to stipulate a referent object or be rendered meaningless. However, as there are numerous ‘states’ and ‘individuals’, it is not sufficient to simply indicate that which is concerned. Instead it is argued that the “...search for a referent object of security goes hand-in-hand with that for its necessary conditions...” (Buzan, 1983:13). Speech Act Theory serves to demarcate such conditions.

Securitisation Theory draws upon Speech Act Theory, as developed by John L. Austin²⁴ to demonstrate that utterances have a direct correlation to actions. Certain speech acts are to be regarded as ‘performatives’ which points to what is effectively the ‘social magic’ that occurs when saying specific words or phrases, which in themselves accomplishes an action; such as the act of christening of a ship. What is of particular importance to ensuring the widening of the Security Studies agenda does not go unbridled is the consideration of ‘felicity conditions’ necessitated by Speech Act Theory, that is to say the specific conditions that must be met in order for a performative speech act to be successfully accomplished (Peoples & Vaughn-Williams, 2010:77). These considerations are accounted for in Securitisation Theory, which holds that the success of a speech act is determined by external and internal conditions, that is to say “...a combination of language and society, of both intrinsic features of speech and the group that authorises and recognises that speech...” (Buzan *et al.*, 1998:32).

Although in principle any securitising actor with reference to whatever referent object can instigate the securitisation process, in practice there are pervading limitations that stem from variegation in the capacity amongst actors to assert claims about threats that are socially effective. Actors who assume powerful positions and garner greater authority in a system are imbued with more social capital and are thus more effective at convincing a relevant audience to recognise and accept a specific issue as an existential threat; hence the social capital of an actor serves as a felicity condition. It is imperative to note however that although the field of security is structured or biased, in that some actors are assigned what can be considered positions of power “...by virtue of being generally accepted voices of security, by having the power to define security...”, this power is not absolute (Buzan *et al.*, 1998:31). No actor can conclusively claim that they have the ability to convince an audience of the need for security action, nor is any actor omitted from attempting to put forth alternative understandings of security. Further conditions point to the context and pre-established rituals or conventions that a speech act is contingent upon. A speech act is more likely to be successful if it fits appropriately within an existing conventional procedure, and is executed in accordance to the established practices of the particular procedure, i.e. the speech act follows the ‘rules’ within a certain social convention (Williams, 2003:514).

²⁴ Language philosopher most recognized for his formulating of a theory of speech acts published in his highly regarded book *How to do Things with Words* (Austin, 1971).

By transforming security into a self-referential practice,²⁵ the need for a speech act serves to reveal one of the primary tenets in Securitisation Theory; namely securitisation is not controlled by the individual. The success of a securitising move is not determined by the securitising actor, but by the audience subjected to the security speech act. Hence the cognitive structure of logic of security cannot be isolated in the mind of an individual. Because securitisation is the construction of a security issue through a speech act, "...it is a social quality, a part of a discursive, socially constituted, intersubjective realm..." (Buzan *et al.*, 1998:31). In Securitisation Theory the politics of an existential threat is placed at the heart of Security Studies; it is not the mere utterance of 'security' but rather the acceptance by a relevant audience of the claim to emergency action that serves to define a security speech act. Effectively security does not lie with objects or with individual subjects, it rests *among* subjects. "Both the successful performance of the speech act and the logic of security are ultimately internal to the interplay of social practices...", essentially reducing security to a particular form of social praxis and offering an alternative to materialist threat analysis (Huysmans, 1998:493).

It is this emphasis on the intersubjective and the rejection of the pervading objective/subjective dichotomy in security conceptions that serves to anchor Securitisation Theory to a radical social constructivist approach of Security Studies. However, although their understanding of security is radically constructivist, the Copenhagen School's interpretation of social relations is not. Securitisation Theory explicitly states that because some socially constituted practices are so deeply sedimented and entrenched as structures; constructivism is not uniformly distributed. Although it is still maintained that change is possible, this leads the theory to place a greater emphasis on "...collectivities and on understanding thresholds that trigger securitisation in order to avoid them..." (Buzan, 1997:21). This methodological collectivism is at odds with critical theories that tend to place focus on the individuals and place emancipation at their core, whereas Securitisation Theory is more intent on understanding the modes of functioning of existing actors and maintain future attempts to manage security must include a handling of these actors. Hence Securitisation Theory draws correlation with traditional approaches in that they attempt to comprehend security constellations whereas critical approaches tend to point towards the overthrowing of current power holders. "Rather than emancipation and security being two

²⁵ For an issue to be securitised, it does not need to pose an existential threat, it just needs to be presented as such (Buzan *et al.*, 1998:24).

sides of the same coin...” proponents of Securitisation Theory argue that the application of a logic of security to certain non-military issues would be counter-intuitive and misguided; instead it is more appropriate that certain issues on the agenda are ‘desecuritized’ (Peoples & Vaughn-Williams, 2010:30).

Desecuritisation in Securitisation Theory is the shifting of an issue out of the realm of emergency politics back into the territory of normal political, public or technical debate. Unlike traditional assumptions that portray security as intrinsically good, the logic of Securitisation Theory demonstrates security should not be idealized in that threats could be exploited by power holders to create opportunities for less democratic control in domestic contexts (Buzan *et al.*, 1998:29). For this reason, Securitisation Theory is wary of the widening agenda in that it tends to depict security as a desirable condition whereas ideally an issue should be dealt with in accordance to routine procedures and should be opened to debate and the haggling of politics. “At best, security is a kind of stabilization of conflictual or threatening relations, often through emergency mobilization of the state...” (Buzan, 1997:11). Furthermore, greater security is not necessarily better in that by bringing with it the required mode of emergency politics and militarized thinking, it serves to limit the time and political space “...allowed for deliberation, participation, and bargaining...”, which could be of pronounced detriment to particularly complex issues (Peoples & Vaughn-Williams, 2010:83).

Contemporary Security Context:

The previous sections in this chapter sought to provide a coherent understanding of the Security Studies agenda and Securitisation Theory. In doing so, it is now possible to project the assumptions and approaches of the Copenhagen School to the current global security context. Globalization and the advent of the information age has irrefutably redefined the security landscape of international relations, yet IR Theory has proven flexible and has succeeded in adapting to the changes wrought on the global system. This section will carry through the Security Studies agenda, by demarcating these changes and demonstrating the efficacy of Securitisation Theory in understanding them as well as analysing security as it relates to cyberspace and the Internet. By highlighting the limits of mainstream IR theory, this section seeks to assert that Securitisation Theory is most readily imported to the cyber domain.

When the Cold War collapsed, so too did the degree of stability afforded to the global system by the superpower nuclear balance of terror. Global trends have suggested the increased proliferation of emerging power centers, state and non-state actors alike. With no one left in charge of presiding over and organizing global affairs; projections of the future of international security have been somewhat grim, as a growing number of technologically empowered individuals and groups such as terrorists cells now boast the capacity to attack and provoke even superpowers in the international system.²⁶ Other predictions point to an equally dismal future characterized by intractable conflicts amongst the worlds contrasting cultures. Imbued with strong emotional ties and values; "...[c]ulture is portrayed as a force working through its adherents and driving global politics..." (Kolodziej, 2005:13).

The hypothesis put forth by Huntington in *The Clash of Civilizations*; that people's cultural and religious identities will be the primary source of conflict in the post-Cold war, rings ever more true in the wake of globalisation (Huntington, 1997). Conflicts over religion, ethnicity, nationality, and race (that were already widely spread and long since established); have been exacerbated by the shrinking of the world.²⁷ It is irrefutable that in current era, cultural conflict is rampant. Numerous examples of ethnic and religious conflict are apparent throughout the world. In light of the subject matter of this study the rise of Islamophobia on a global scale is the most relevant example.²⁸ As boundaries to interaction are continuously reduced by technology, diverse and divided people of the world increasingly clash leading to the view that "...globalisation spurs, not stifles, cultural conflicts..." (Kolodziej, 2005:13).

The introduction of technology, to the Security Studies repertoire has not been uniform. Originally concerns regarding computer security were rejected by the research agenda. The view was that issues regarding computer hardware/software and malicious viruses or outside attackers threatening a computer system, lacked the urgency requisite of national or international security issues. The response from Security Studies was that these issues were linked to domestic and individual concerns, thus they were "...'technical' rather than political-military threats..." (Buzan & Hansen, 2009:15). Securitisation Theory concedes that

²⁶ IS and its affiliates have conducted numerous physical attacks in Europe and the US, with global death toll outside of Syria and Iraq reaching 1200 as of July 2016 (Yourish *et al.*, 2016), provoking powerful western states into what has been coined the global 'war on terror'.

²⁷ "...[S]trides in the efficiency and effectiveness of modes of transportation, communications, and computer technologies..." wrought by globalization have both metaphorically and physically reduced boundaries to interaction, leading to the view that the world is shrinking (Kolodziej, 2005:13).

²⁸ The closed-minded prejudice against or hatred of Islam and Muslims.

security cannot be reduced to a static understanding derived from its bearing on the national or the international. What's more, as demonstrated by the historical narrative of Security Studies developed at the beginning of this chapter, proponents of Securitisation Theory assert that the field of security is highly dynamic and what can be accepted as a legitimate issue in international security theory is constantly changing (Buzan & Hansen, 2009:15). For example, whereas the environment was excluded from the Security Studies agenda until the closing years of the Cold War, it is difficult to conceive of a robust agenda that would exclude it now.

These fluid and dynamic security contexts are best illustrated in the transformed perceptions regarding information technology and how it relates to international security. Since the 9/11 attacks, computers and information technology have been afforded mounting attention on the security agenda. Earlier writings from the Copenhagen School ruled out concerns of cybersecurity and dismissed it as an attempted securitisation. The example of the threat posed by hackers made by the Pentagon was used to assert that although cybersecurity "...could possibly lead to actions within the computer field..."; as it would have "...no cascading effects on other security issues...", it would not be adopted into the Security Studies agenda (Buzan *et al.*, 1998:25). As demonstrated in the literature review, questions of "...digital infrastructure protection, electronic surveillance, the terrorist use of hacking and the Internet as networked platform for communication across and against states..." have been catapulted to the forefront of national security agendas (Hansen & Nissenbaum, 2009:1156). This is most evident in non-democratic regimes, which have sought to close off domestic access to features of the Internet that are seen to threaten political and societal stability.

Both in the broader discipline and the sub-field of Security Studies, Realism and Liberalism have served as the dominant theoretical approaches of IR for most of the 20th century, however they have not readily imported into the cyber-domain and the information technology beset world of the 21st century (Choucri, 2012:14). To elucidate, whilst Realism and all its derivatives all but dictated the Security Studies agenda in the epoch that followed the end of WWII, it now risks being superseded by those approaches, which have posited the critical reframing of security. This is because the Realist fixation on material capabilities, specifically the pursuit of wealth and power, is not wholly compatible with the factors that weigh on cybersecurity and the potential for conflict or threats to arise in the cyber-domain. Furthermore, Realism's epithet of major power politics is undermined by the ubiquity of

cyber-venues and that access to them is potentially available to anyone. Whilst Liberalism, particularly its Neoliberal variant, has garnered significant sway in Security Studies it has been limited by its tenet of institutionalism. Although useful in that it could discern possible implications and modalities for managing cyber-venues, institutionalism is undermined by its logic informing interstate interactions in that it is state based, and does not sufficiently account for the private sector, which of course regulates cyberspace.

A facet of Securitisation Theory that is considered important to this study stems from attempts made by the Copenhagen School to expand traditional conceptions of securitisation beyond referent objects framed at the level of the state, to include ‘macrosecuritisations’. Macrosecuritisations are bound to the same rules and process that define other securitisations; namely the need to intersubjectively identify an existential threat to a referent object that legitimises the use of extraordinary measures, yet it is essentially different in that they are conducted “...on a larger scale than the mainstream collectivities at the middle level (states, nations) and seek to package together securitisations from that level into a ‘higher’ and larger order...” (Buzan & Wæver, 2009:257). The Copenhagen School argues that due to improvements in communication facilitated by technological development, macrosecuritising collaborations are becoming increasingly apparent. As demonstrated by Chapter 2, there exists a plethora of actors both from the private and public sector involved in issues of Internet governance and cybersecurity. What is important here is that the challenges presented by the Information age are transnational and cannot be overcome by singular political units who pursue their own egotistical interests. Macrosecritisation is useful in that “...[s]uch a regime adds an enlarged dimension to the relationship between the securitising actors by bringing into play a variety of possible multilateral partnerships...” and multiparty security arrangements, with the goal of structuring international politics and security at a larger scale (Kingsmith, 2013:4).

This study thus asserts that on the matter of cybersecurity, traditional theories hold modest explanatory power due to their focus on state actors. Because of its inherent complexities and the unsubstantiated characteristics of cyber-threats, an approach that incorporates a subjective ontology and constructivist logic is seen as most appropriate for the analysis of cybersecurity. Despite being the product of the two different meta-theoretical positions assumed by its founders; namely Wæver’s post-structuralism (locating him in a post-positivist agenda) and Buzan’s neorealism (locating him in a positivist agenda), Securitisation Theory is perceived

as a Constructivist meta-theory in that it takes into account the numerous factors implicated in the formation of security policy agendas (Cavelty, 2007:25).²⁹ In this study, Post-positivism is favoured (specifically on the issue of cybersecurity and the Internet) due to the emphasis it places on the conditions and consequences of framing something as a security issue, whereas traditional theory is perceived as limited because "...it views threat images as a given and measurable and assumes that security policies are responses to an objective increase of threats and risks..." and thus can not account for the implications of security in terms of political agenda-setting and political relations (Cavelty, 2007:8). In this regard, Securitisation Theory is preferred because its emphasis on speech act enables it to account for the various factors informing the development of security policy agendas.

What is of particular interest to this study are the conceptual tools/apparatus for analysis developed by Securitisation Theory. This study does not seek to prove or disprove the theory; rather utility is seen in the exploratory and predictive power of Securitisation Theory. Cyberspace is a phenomenon intrinsically linked to globalisation. It has become one of the pivotal features of an progressively complex international system in that; not only is its operation and management subject to the control of an extensive range of non-state actors, but also the "...global, often nontransparent interconnections afforded by cyberspace have challenged the traditional understanding of leverage and influence, international relations and power politics, national security, borders, and boundaries..." (Choucri, 2012:3). The starkly defined concepts in Securitisation Theory cater to the complexities of the subject matter in that it allows for a holistic approach that can sufficiently account for the different actors and levels of analysis inherent in the subject.

²⁹ It is interesting to note the irony evident in that of the existing theory in Security Studies; it is positivist theories that strive for falsifiability, yet it is Securitisation Theory, located in Constructivism and regarded as post-positivist, that seems best suited for this. In order to be falsifiable, theory must demonstrate causality, which mandates that variables identified in the study be temporally and analytically separated. Theories in Security Studies are not falsifiable as concepts can only be approximated. Yet positivists argue that researchers "...should strive to concord with positivist principles to the greatest extent possible..." whereas post-positivists counter that "...many of the problems with which the social sciences engage, including the one of security, are better dealt with through the use of non-positivist theories..." (Buzan & Hansen, 2009:35). This post-positivist sentiment is clearly evident in Securitisation Theory in that it demonstrates bias towards desecuritisation and maintains that security conditions are not always suited to dealing with the complexities apparent in certain issues. However despite rejecting positivism, *Security: A New Framework for Analysis* has come the closest to developing a causal theory in Security Studies. Securitisation Theory provides a framework that clearly demarcates variables involved in analysis; namely the conceptual apparatus and tools incorporated in securitisation such as the referent object, the speech act etc. By providing a framework for conceptualising variables and the different roles and interests of actors, the different concepts can be analytically isolated. And because securitisation occurs sequentially, it is temporally separated.

The intention of this study is thus not to determine the success of the securitisation attempt, but rather to investigate the implications of the security measures that are evoked in reaction to a securitising move. Evaluation of the implications of securitising the Internet, in terms of the policies and countermeasures decision makers create as a response to perceived threats, is possible because Securitisation Theory allows the researcher to view security as a practice rather than an objective condition. Securitisation theory is evoked here as an instrument of policy creation; this study seeks to understand what use if any, securitisation will have in preventing terrorists from exploiting the Internet.

Conclusion:

The purpose of this chapter was to provide a concise theoretical understanding of Securitisation Theory within the discipline of IR. Familiarisation with the theoretical literature is deemed imperative should findings prove robust and spurious correlation be avoided (Barakso *et al.*, 2014:59). The chapter began by outlining the development of Security Studies so as to link the field to IR; after which, epistemological debates and mainstream theoretical approaches in Security Studies were identified. This ensured the study took into consideration all possible research avenues before selecting a theory to apply to the case of IS and cyberjihad. After deciding on Securitisation Theory, the study proceeded to highlight the primary tenets and assumptions of the theory so as to inform subsequent research. Justification for selecting Securitisation Theory was then made by attempting to illustrate how it is well-suited to cope with the changes wrought by the Internet in the contemporary security context.

With regards to the research questions and problem, the logic for applying Securitisation Theory in this study is grounded in its exploratory capacity and its readiness to be applied to concepts that exceed positivist limitations of state centrism and military concerns. Securitisation Theory points to the application of extraordinary measures which this study believes would be useful in helping to overcome the challenges to effective countermeasures to preventing terrorist exploitation of the Internet. Incorporation of a strong theoretical dimension into study allows for wider application of findings (Burnham *et al.*, 2008:64). It is not just IS or jihadist organisations that have sought to exploit the Internet for terrorist applications. Furthermore, should IS eventually be eradicated it is highly unlikely that other organisations or individuals will fail to integrate the Internet into their strategies. Thus, grounding the research in Securitisation Theory will allow findings to be transposed to other

cases. The chapter that follows develops the case of IS and cyberjihad to illustrate the dangers of terrorist exploitation of the Internet and the need to develop effective countermeasures to prevent it. Extrapolating Securitisation Theory assertions and assumptions allows the study to explore how securitising the Internet could be realised. Securitisation of an issue warrants the application of extraordinary measures to address an existential threat. In this regard, Chapter 4 attempts to explore the possible benefits, or shortcomings, of Internet securitisation.

CHAPTER 4: Terrorist Exploitation of the Internet – The Case of Islamic State and Cyberjihadist Strategies

Introduction:

In this, the penultimate chapter, the study combines the research conducted on literature and theory in an attempt to demonstrate how securitisation of the Internet can serve to benefit counter-terrorist measures that aim to prevent terrorist exploitation of the Internet. A single case study of IS and its integration of cyberjihadist strategies is developed in an effort to illustrate the potential benefits of securitisation. The chapter begins with a section that provides a background to IS and its operations, followed by a section that outlines cyberjihadist strategies. Demarcation of these strategies reveals that IS has exploited the Internet to fulfil various different purposes, identified by this study as; propaganda; recruitment and radicalization; strategic operations; operational training; and fundraising. Together, these two sections combine as the case in this research.

The study then goes on to outline the various different measures adopted by the international community to prevent terrorist exploitation of the Internet and the challenges they face. Review of the different measures reveals that they can be framed under two overarching approaches, content-based measures and strategic communication measures. Again, the UN is employed as a focal lens to narrow the scope of the study. Thereafter, factors that serve to undermine effective application of these counter-measures are outlined. This study groups together various pervading issues so as to identify three primary challenges to preventing terrorist exploitation of the Internet, delineated as; issues of cooperation and coordination; concerns of human rights and liberal principles; and establishing strategic value and causality. After developing the case and contextualizing the challenges to effective countermeasures, the study proceeds to unpack the assertions of Securitisation Theory in relation to the Internet. Application of theory reveals that securitizing the Internet mandates a three-step process; beginning with a securitizing move; followed by acceptance of a threat by a given audience; and finally, the uptake of extraordinary measures. The final section of this chapter represents the culmination of this body of research, as it attempts to illustrate the potential benefits and shortcomings of Internet securitisation as a method of countering cyberjihad.

Background of Islamic State:

The rise of IS is attributed to a number of complex circumstances independently shaping the collapse of the Syrian and Iraqi states. IS was borne from a Sunni³⁰ extremist group, al Qaeda in Iraq (AQI), that was originally established to fight against US forces in the 2003 invasion of Iraq. The group was almost wiped out in 2006³¹ but managed to persist in the post invasion chaos until 2011, when they succeeded in capitalising on the anarchy that followed a revolt against the Assad regime in Syria. As the revolt deteriorated into civil war "...the group took advantage of the chaos, seizing territory in Syria's northeast, establishing a base of operations, and rebranding itself ISIS..." (Cronin, 2015:89). Subsequent to the withdrawal of US forces, IS has continued to draw strength from the complexities that continue to debilitate the Syrian and Iraqi states, such as authoritarian leadership and sectarian cleavages (Lewis, 2014:4).³² After days of fighting with opposition groups, IS succeeded in taking control of the Iraqi city of Fallujah and the Syrian city of Raqqa in early January 2014. Analysts predicted that the group would be unable to maintain the territory it had gained and its expansion efforts would cease as state security forces proceeded to contain the threat (Cronin, 2015:89). But following mass desertions by the Iraqi army, the group was able to continue capturing territory throughout Iraq and Syria,³³ culminating in the declaration of a new Islamic Caliphate on 29 June 2014 by IS leader, Abu Bakr al-Baghdadi who went on to establish himself as the Caliph and the successor of the prophet Mohammed (John, 2015).

After declaring the establishment of a Caliphate to claim dominion over Muslims around the world, IS proceeded to dominate the global stage in pursuit of its grand strategy "...as predicated upon military force to establish physical control before political and religious authority are attained..." (Lewis, 2014:10). IS has since supplanted all other terrorist groups to establish itself as the most concerning jihadist threat. IS has amassed success that would seem unfathomable to other groups, energising tens of thousands of people to join and inspiring many more to support it (Barrett *et al.*, 2015:21). Following the unprecedented territorial gains it made in 2014, IS has systematically lost control of territory in Iraq and Syria. A study conducted by Information Handling Services (IHS) revealed that in 2015,

³⁰ 'Sunni' is the largest denomination of Islam, constituting 80% of the worlds 1.6 billion Muslims (The Economist, 2013).

³¹ The AQI leader Abu Musab al-Zarqawi was killed by US airstrikes and Sunni tribes joined forces with the Americans to tackle the jihadists (Cronin, 2015:89).

³² Following the US withdrawal; the Nouri al-Maliki the Iraqi Prime Minister served to further alienate Sunni Arabs in Iraq by pushing a hard line pro-Shiite agenda (Cronin, 2015:89).

³³ For a complete timeline of events that contributed to the rise of IS, see (John, 2015).

territory under the control of IS shrunk by “...12,800 km² to 78,000 km², a net loss of 14 percent...”, this shrunk by a further 12 percent in the first half of 2016 so that; “...[a]s of 4 July 2016, the Islamic State controls roughly 68,300 km² in Iraq and Syria...” (IHS, 2016a). Territorial losses have had a massive impact on the internal cohesion of IS and have resulted in declines in revenue sources. In order to fund its army and the pursuit of its primary goal of establishing a pseudo-state, IS has had to amass significant funds; and indeed it has done so. In 2015, it was estimated that IS had “...cash on hand and revenues of at least \$1.5 billion...” (Nicks, 2016). IHS estimates that 50 percent of IS’s revenue comes from taxation and confiscation, 43 percent from oil revenue, with the remainder compiled by a mix of illicit activities (drug smuggling, donations, and the sale of electricity (IHS, 2016b). The two primary sources of revenue are intrinsically linked to IS capacity to maintain territory, hence the loss thereof has contributed significantly to the IS’s financial decline.

Not only are there fewer people to tax,³⁴ but territorial losses of oil fields and intensified efforts by foreign actors and coalition forces to reduce IS oil production capacity has resulted in a decline in overall decline in production from an approximate 33, 000 barrels per day to 21, 000 barrels per day.³⁵ The culmination of all these factors has led to an estimated decline in IS overall monthly revenue; in 2015 it was estimated to be around \$80 million and as of March 2016 IS’s monthly revenue is estimated to have dropped to \$56 million (IHS, 2016b). Although IS is still a terrible force in the region, declines in revenue will affect the group’s capacity to run and administer its Caliphate in the long term, whilst loss of territory and military setbacks have led to “...a marked increase in defections and desertions since January 2016...” (IHS, 2016a). Although loss of territory and increased fragmentation would seem to suggest that as a governance project IS is failing and overtime this will lead to the gradual defeat of IS as conventional force; even if IS “...is a failing enterprise in steady decline, it will be able to influence the actions of its adherents, and it may become more dangerous as it dies...” (Barrett *et al*, 2015:21).

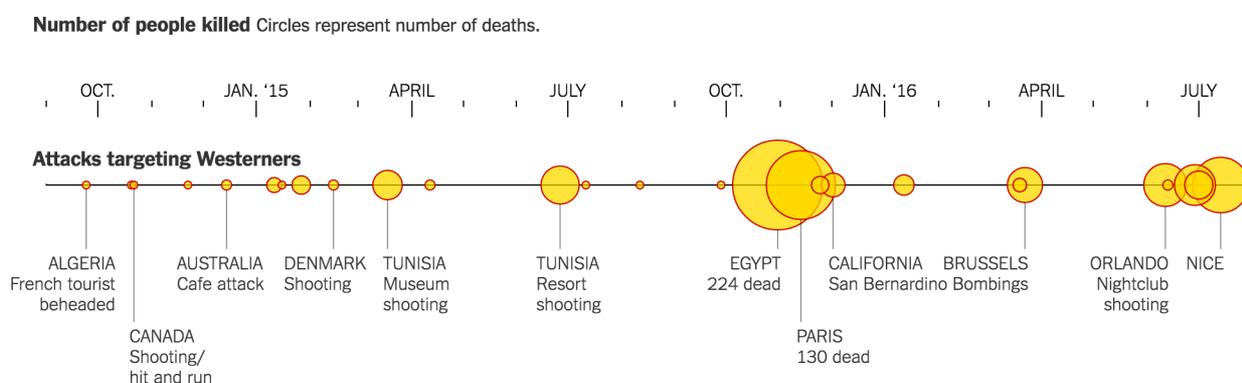
The success of the Caliphate is becoming increasingly tenuous, however IS has sought to change its message and strategy by giving greater attention to conducting terrorist attacks outside of its territory. For jihadist groups like IS, the ideological battle is of equal

³⁴ Loss of territory suggests dominion over fewer people; also many have fled the region since 2014.

³⁵ Significantly, decline in production is not attributed to any reduction in demand for the oil in the Syrian and Iraqi black markets (IHS, 2016b).

importance to military confrontation. Set backs in the field have led to a shift in focus from territorial control and consolidation, to a greater emphasis on insurgency and efforts to attack foreign enemies in their states. Successful attacks outside of the Caliphate core, allow IS to claim success and maintain support in the battle for hearts and minds, despite territorial losses in the Caliphate. Thus the threat to the international community remains, as it would appear the decline in IS territory and revenue is inversely related to the increase in terrorist attacks outside of the region in which IS operates. This can be illustrated by the increased frequency and impact of attacks committed by IS at the close of 2015 and in 2016.

Figure 4: Timeline of IS attacks outside of Iraq and Syria



Source: (Yourish *et al.*, 2016).

Dismantling the Caliphate will not suffice in the battle against IS, in that terrorist organisations rely less on traditional organisational structures. Modern communication technologies have facilitated the shift away from hierarchal organisation as increased networking capacity allows jihadist groups to operate as delocalised cells. This makes dependence on military force alone problematic as a counter strategy because it has become increasingly difficult to single out targets to attack (Brenner, 2005:111-112). What's more, in the case of IS the group has succeeded in creating a powerful Salafist³⁶ narrative that has inspired radicalisation on a scale unseen with other jihadist movements; making 'lone-wolf' attacks more common which presents a threat regardless of location. Individuals who sympathise with IS are encouraged to carry out insurgent attacks. Often these attacks are committed by Western nationals in their homelands, making the IS ideology as dangerous as

³⁶ Salafism is an ultra-conservative fundamentalist approach to Islam that developed from a twentieth century movement that has sought to restore and validate 'pure' Islamic doctrines in modern times (Esposito, 2003:275).

its army. This would suggest that even if IS loses territory, "...it is likely to survive in some form for a considerable time to come..." (Barrett, 2015:21). This form of transnational global terrorism is completely reliant on the Internet and cyberjihadist strategies to endure.

Contextualization of Cyberjihadist Strategies:

IS has fervently adopted cyberjihadist tactics so as integrate ICTs into its overall strategy for conducting global jihad. IS "...enthusiastically embraces web forums and social media to create a wireless Caliphate—fighting enemies on the ground as well as on the web..." (Liang, 2015:5). Several intrinsic features of the Internet make it an ideal tool for facilitating terrorists activities and global jihad. To elucidate, the Internet offers; rapid communications and the speedy flow of information; easy access; a low cost communication system and an inexpensive means of developing and maintaining a online presence; a multimedia environment that allows for the dissemination of complex information; a global cyber presence facilitated by the ubiquity of the Internet, providing access to a potentially massive global audience; negligible government interference in terms of regulation and censorship; and most important; a means of communicating and conducting other illicit activities anonymously (Lachow, 2009:454-455; Weimann, 2004b:3).³⁷ What follows is a summary of cyberjihadist activities and IS applications and exploits of the Internet.

Propaganda Creation and Dissemination:

Cyberspace has long since been established as the pivotal arena for propagating jihadist ideologies and for targeting internal and external audiences alike, whilst the Internet has been successfully exploited as a powerful and effective tool for IS propaganda dissemination. Cyberjihad strategies quickly recognized the usefulness of the Internet in that the anonymity it affords coupled with its global reach allows for terrorist messages to spread at an unprecedented pace to all corners of the globe; with a marginal risk of detection (McNeal, 2007:800). Terrorist websites and social media accounts are used to control the image of organizations in the eyes of specific audiences and the media. Information regarding a group such as its historical background and accomplishments are distributed through a variety of online media outlets to promote their ideology. However, because Internet postings are unregulated, websites and social media outlets often post inaccurate information so as to manipulate perceptions regarding the organization. Propaganda dissemination has been

³⁷ "[M]odern encryption technologies allow Internet users to surf the Web, transfer funds and communicate anonymously..." (Lachow, 2009:455).

crucial to maintaining support from sympathizers as the Internet “...allows extremists to deliver well-coordinated propaganda campaigns that increase the levels of support among the general public...” and lets jihadists operate freely in these societies (Lachow, 2009:455).

The dissemination of jihadist material online fulfills several propagandist objectives. Propaganda online is operationalized in that it allows jihadists to inform sympathizers of their developments, garner support and rally individuals to their cause, and lastly undermine public opinion in states that are perceived to be enemies. IS has managed to use the latter tactic to shocking effect against the global populace, particularly Western audiences, through its documentation of execution videos. In 2014, “...with the beheading video of US photojournalist James Foley,...IS initiated a hostage video campaign drawing tremendous attention by the mainstream media...” (Tinnes, 2015).³⁸ The group released a series of high production value videos, laden with symbolism that served simultaneously as high-impact propaganda and as a psychological weapon in IS’s ‘War of Ideas’.

These videos were created not for the sake of mere violence or murder; rather they are the product of a rationally deliberated strategy of communication, which simultaneously exerts a massive impact on various target audiences. Sympathizers are rallied, fear in the public audience is aroused, and the enemy is alerted to the lengths to which the organization is willing to go to reach their desired outcome.³⁹ The “...psychological dimension offered by the Internet is unparalleled in its ability to achieve mass penetration and create the impression of a sustained terror threat...”, this is particularly true of IS in that its numerous beheading incidents followed in quick succession from August 2014 through to August 2015 (Maher, 2007:146).⁴⁰ The underlying mandate of IS beheading videos is to be reproduced and watched by an audience much larger than those directly involved. Due to the Internet’s near seamless global connections and modern modes of reproduction and communication, once

³⁸ Cases of IS beheadings preceded the Foley incident, but did not receive as much attention from the world’s press (Al Jazeera, 2014; Crane *et al.*, 2014). There have since been numerous cases of IS beheadings, which are not included in this study.

³⁹ In the case of the Foley incident, IS intent was very deliberate as the video was entitled ‘A Message to America’, whilst the central message of the IS Western hostage video campaign was to “...deter the U.S. and its allies (mainly via generating pressure from the general public) from direct military intervention against IS targets in Iraq and Syria...” (Tinnes, 2015).

⁴⁰ In July 2014, IS “...distributed 11 [video] releases in English (a new release every 3 days)...” (Liang, 2015:6).

jihadist media is posted online it is almost impossible to control.⁴¹ The beheading videos serve to “...blatantly encapsulate how active combatants may exploit new media technologies and the ensuing increased visual interconnectivity for strategic purposes...” (Friis, 2015:729).

Not only has IS incorporated the Internet into its sophisticated strategy for multidimensional propaganda dissemination, it has also demonstrated unprecedented success in populating and operationalizing social media platforms, so as to attract a “...global network of supporters that articulate, magnify and circulate its violent extremist messages worldwide...” (Liang, 2015:1). Online social media platforms such as Twitter, Facebook and YouTube are established as the most popular medium of communication for young people in the digital age. The IS cyberjihad strategy has sought to penetrate these platforms so as to strategically target young men and women, who tend to be the most vulnerable demographic,⁴² for worldwide recruitment. The extent of IS social media operations is mind boggling. To elucidate, as of November 2014 it was estimated that there was between 46, 000 and 70, 000 Twitter accounts supporting IS, with an average number of 1,004 followers per an account, tweeting an average of 7.3 times per day (Berger & Morgan, 2015:9).

IS uses Twitter for various purposes, be it organization, provocation, or the facilitation of real time debate. By making use of Twitter’s hashtag⁴³ feature, IS often hijacks trending topics to elevate the organization into discussion, for example #Brazil_2014 or #AllEyesOnISIS. IS members “...are effective keyboard warriors, tweeting terror before their boots even hit the ground...” (Liang, 2015:5). Other examples of IS exploitation of social media include; the use of Facebook as a platform for foreign fighters to recruit their friends to join jihad, and uploading videos with extremist content ranging from content praising martyrdom to footage

⁴¹ Not only do mass communication outlets allow for propaganda to be disseminated instantaneously and spread extremely fast, but also the issue of control pertains to how jihadist material is interpreted. Once the material is posted the producers are no longer in control of how it is used. Other agents may also use the video politically for purposes other than its original intentions (Friis, 2015:730). In the case of IS, this is evident in that the beheading videos can be used to fuel a bad ‘PR’ effect as the videos are excessively violent and can be framed as breaking Islamic law.

⁴² Younger audiences are targeted for their naivety. Following the September 11 attacks, Muslim millennials have grown up in an era where they have had to face intense scrutiny because of their religion. This identity crisis has led many to look inward to find answers regarding what their faith means to them. “In today’s insular communities there is less religious support, leading some young Muslims to turn to the Internet for answers, where they encounter recruiters and ‘religious’ sanctioners who offer specifically tailored answers that are appealing and offer real meaning to this troubled generation...” (Liang, 2015:3).

⁴³ A label or metadata tag indicated by the symbol ‘#’ and used before a relevant keyword or phrase. Used on social media sites to make it easier for users to locate content with specific themes (Twitter, 2016).

of suicide bombings on YouTube (Liang, 2015:5-6).⁴⁴ Social media forums are used as ‘radicalization echo chambers’ for spreading the IS ideology. Although other platforms are used extensively, Twitter is by far the most used social media outlet for IS.

While the power of the Islamic State’s social media outreach is undeniable, it appears more often to prepare the ground for persuasion, rather than to force the decision. There are few places on earth in which the group’s message and imagery cannot be seen or heard, and its ubiquitous reach has led to the recruitment of individuals from Algeria to Uzbekistan (Barrett *et al.*, 2015:10-11).

Often individuals who develop an interest in IS through social media subsequently strengthen their commitment and internalize the IS narrative through direct contact, making online and offline dynamics complementary. It is not possible to attribute the success of IS to its social media and propaganda campaigns alone. There is extreme variegation and diversity of background amongst IS supporters, rendering self-radicalization an anomaly. Whilst radicalization is certainly an extremely complex and individualized process, ideological motivations are certainly discernible in that those who embrace IS tend to be “...disenfranchised individuals seeking ideological, religious and personal fulfillment... (Vidino & Hughes, 2015:15-16).

Recruitment and Radicalization:

One of the most essential functions the Internet serves in the cyberjihad strategy is its role as an inexpensive tool that facilitates the recruitment and radicalization of individuals from all corners of the globe. Because of the widespread dissemination of ICTs, the Internet can be easily accessed by those at home or in public; ultimately increasing the pool of potential recruits for terrorist organisations. As such, the Internet has allowed for the exponential increase of potential recruits as “[w]ebsites and chat rooms provide an instant connection between recruiters and interested sympathisers...” (McNeal, 2007:794). The success of IS is dependant on its ability to attract interested outsiders to become active members and direct supporters of its cause; which centres on the primary goal of establishing an Islamic Caliphate. Bringing about the Caliphate requires that IS must “...establish, construct or preserve, and defend a community of believers within land that is acquired through military conquest...” (Lewis, 2014:11). For this, IS needs fighters to physically commit to defending and expanding the territory of the Caliphate, rendering mass recruitment essential to the

⁴⁴ Other less formal examples include the use of Instagram by IS to post pro-IS memes or lifestyle content such as images of food or designer clothes. This strategy depicts an attempt by IS to normalize radical ideas and appeal to a greater support base (Carman, 2015).

success of the group. Prior to the advent of ICTs the recruitment process was reliant on face-to-face contact, which greatly limited the scope and success of recruitment efforts. The Internet on the other hand has made instantaneous recruitment simple, by reducing boundaries to interaction and allowing IS to identify potential members and “...maintain fervour in those already dedicated to the cause, on a global scale...” (Lachow, 2009:456).

The Internet is used by extremists as a means to reinforce powerful narratives and ideological messages; it allows for the inclusion of multimedia content such as videos and images that are masterfully used to substantiate jihadist political claims (Vidino & Hughes, 2015:17-18). IS makes use of various medium such as texts from the Quran and religious symbolism to supports its actions. Instantaneous access to this content makes the jihadist message more visceral and compelling. The Internet has exacerbated IS capacity to proliferate extremist literature and broadcast a powerful narrative to a global audience. More than simply allowing for outward communication, cyberjihad has instrumentalised the creation of virtual transnational communities that allow geographically isolated militants to unite and binds together global jihadist movements.

IS has targeted younger members of society by using web based media such as videos and digital imaging to indoctrinate individuals with “...virtuous messages of jihad and martyrdom that justify and legitimize violent action against non-Muslims...” (Davis, 2006:146). Mounting Islamophobia in the current global context has led to greater alienation and isolation of Muslim youths in Western societies, who are ostracised for their religious beliefs. This environment has served to foster the ‘autonomous radicalization’ of Muslim youths who have proven more susceptible to radical, dialectic jihadist narratives. The anonymity afforded by the Internet allows terrorist organisations to foster higher levels of violence in people, in that it lets individuals act unfettered by a fear of consequences (McNeal, 2007:795). By providing a reasonably safe environment for potential recruits to discover, interact and ultimately network with likeminded individuals; the Internet provides a platform that allows for integration and assimilation into more formal organisations. It “...creates a new social environment in which otherwise unacceptable views and behaviour are normalised...”, as the encouragement and support of peers “...beyond an isolated group of conspirators...” make it easier to join (Vidino & Hughes, 2015:18). Web-based interaction provided by the online cyberjihad community creates an environment where “...radical youths can identify with,

connect to and emotionally share the intensity and suffering of fellow Muslim victims and the cause of the mujahedeen⁴⁵ around the globe...” (Ranstorp, 2007:46).

The group attracts followers yearning for not only religious righteousness but also adventure, personal power, and as sense of self and community. And of course, some people just want to kill – and [IS] welcomes them, too. The group’s brutal violence attracts attention, demonstrates dominance, and draws people to action (Cronin, 2015:94).

It is difficult to ascertain the number of foreign fighters who have migrated to Syria and Iraq in support of IS. As of September 2015 estimates are placed upwards of 30, 000 from over 100 countries (Barrett *et al.*, 2015:5).

Strategic Operations – Communication, Organization & Planning:

Terrorist groups and their affiliates have long since acknowledged the operational advantages of interfacing with ICTs; displaying remarkable ingenuity and skill in exploiting the Internet as a platform for communication, control and command. Due to rapid technological innovation in ICTs and global access, the Internet as a medium for communication is becoming perpetually faster and cheaper. Because the Internet is so ubiquitous “[t]he ease of accessibility and information exchange make websites ideal for serving some of the administrative functions of terrorist organizations...” (McNeal, 2007:797). Terrorists in the Information age rely heavily on the Internet to plan and co-ordinate specific attacks.⁴⁶ Operatives can communicate on a variety of online platforms such as free web-based email accounts; which allow for the easy dissemination of instructions, maps, photographs or technical details pertaining to a target. Several factors serve to outline the substantial utility afforded to terrorists by exploiting the Internet as a tool for communication in the cyberjihadist strategy.

First, new technologies have greatly reduced transmission time, enabling dispersed organizational actors to communicate swiftly and to coordinate effectively. Second, new technologies have significantly reduced the cost of communication. Third, by integrating computing with

⁴⁵ The term mujahid is used to denote one who is engaged in jihad. Mujahedeen is the plural form of the term.

⁴⁶ This claim is illustrated by the extensive use of the Internet by al Qaeda operatives in planning the September 11 attacks. “Thousands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the September 11 attacks...To preserve their anonymity, the al Qaeda terrorists used the Internet in public places and sent messages via public e-mail...” (Weimann, 2004b:10).

communications, they have substantially increased the variety and complexity of the information that can be shared (Weimann, 2004b:9).

Another factor to consider is the anonymity afforded by the Internet. Before the advent of the Internet, terrorists were limited to communicating through mediums such as telephones and radios, which exposed jihadists to a greater risk of detection as these mediums were more vulnerable to surveillance tools, like wiretaps. The anonymity provided by the Internet has served to dismiss this concern. Cyberjihadists make use of numerous methodologies to hide their messages, for example they employ complex encryption keys to render messages almost indecipherable, or use spamming tools online to mask messages in bulk commercial emails (McNeal, 2007:797).

The Internet has also provided terrorist organisations with an advanced intelligence-gathering tool to incorporate into jihadist strategic planning. The Internet offers users an infinite digital library, with billions of pages of information readily and freely accessible to the public. This has allowed cyberjihadists to make use of data mining that lets them gather intelligence on potential targets, as detailed information such as structural layouts or transportation services can facilitate the planning of an attack. Like the rest of the online community, "...terrorists have access not only to maps and diagrams of potential targets but also to imaging data on those same facilities and networks that may reveal counterterrorist activities at a target site..." (Weimann, 2004b:7). A resounding example of the potential application of such services rests with 'Google Maps', which is an advanced web mapping application that provides high resolution satellite imagery, road maps, route planning for different modes of transport, real-time traffic conditions and even 360° panoramic views of streets, available to the public for free.

Arguably the most crucial contribution of the Internet in the cyberjihad strategy, points to the manner in which it has facilitated the complete reform of organisational structures. By providing instantaneous communication, ICTs have served to eradicate most geographical constraints allowing jihadist groups to becoming increasingly decentralised and dynamic. Increased networking capacity in the information age has allowed jihadist groups to shift away from hierarchal organisational structures that rely on "...'great man' leadership..." towards "...flatter decentralised designs..." (Lachow, 2009:457). This shift to a more horizontal structure has allowed for loosely inter-connected, semi-independent cells to form

as the benefits afforded by modern ICTs have allowed terrorists groups to establish and maintain transnational networks.

Operational Training:

Beyond communications, propaganda and recruitment, terrorist organisations have sought to use the cyber domain as a site for training. Terrorist organisations have used the Internet to convert cyberspace into a virtual classroom for training the online jihadist community (McNeal, 2007:797). Multimedia tools are used to produce and distribute training materials online; ranging from pamphlets and manuals, to video tutorials. Information is provided on a litany of subjects pertaining to both traditional and cyber jihadist activities. Examples include "...how to produce and construct weapons ranging from simple IEDS [improvised explosive devices] to...chemical weapons...; they also learn how to mine the Internet for information, protect their anonymity online...and use the Internet to benefit the global jihadist movement..." (Lachow, 2009:456). Information made available by tutorials is sought out not only by committed affiliates but also by IS sympathisers and disaffected individuals, increasing the potential for a 'lone-wolf' attack. Recent examples of IS employing this cyberjihadist strategy are evident in the cases wherein it was discovered that the group was conducting online bomb-making tutorials over Skype to recruit potential suicide bombers in Mumbai (Logan, 2016), and an IS sympathiser was offering online tutorials on hacking so as to encourage supporters to target Western intelligence agencies (Ashok, 2016).

Fundraising:

Another pivotal role the Internet fulfils in cyberjihad strategies points to its use as a tool for fundraising. Jihadists operating online have successfully exploited the Internet so as to raise funds to finance their activities. Terrorist organisations employ four primary methodologies for soliciting and collecting funds.

1. They solicit donations, indoctrinate adherents, share information, and recruit supporters directly via websites, chat groups, and targeted electronic mailings;
2. They take advantage of charitable organizations, soliciting funds with the express purpose of clothing, feeding, and educating a population, but with the covert intent of exploiting contributors' largesse to fund acts of violence;
3. They perpetrate online crimes such as identity and credit card theft, intellectual property piracy, and fraud, and support their mission with the proceeds of such crimes; and
4. They use the Internet as a pervasive, inexpensive, and anonymous medium of communication to organize and implement fund raising activities (Hinnen, 2004:9).

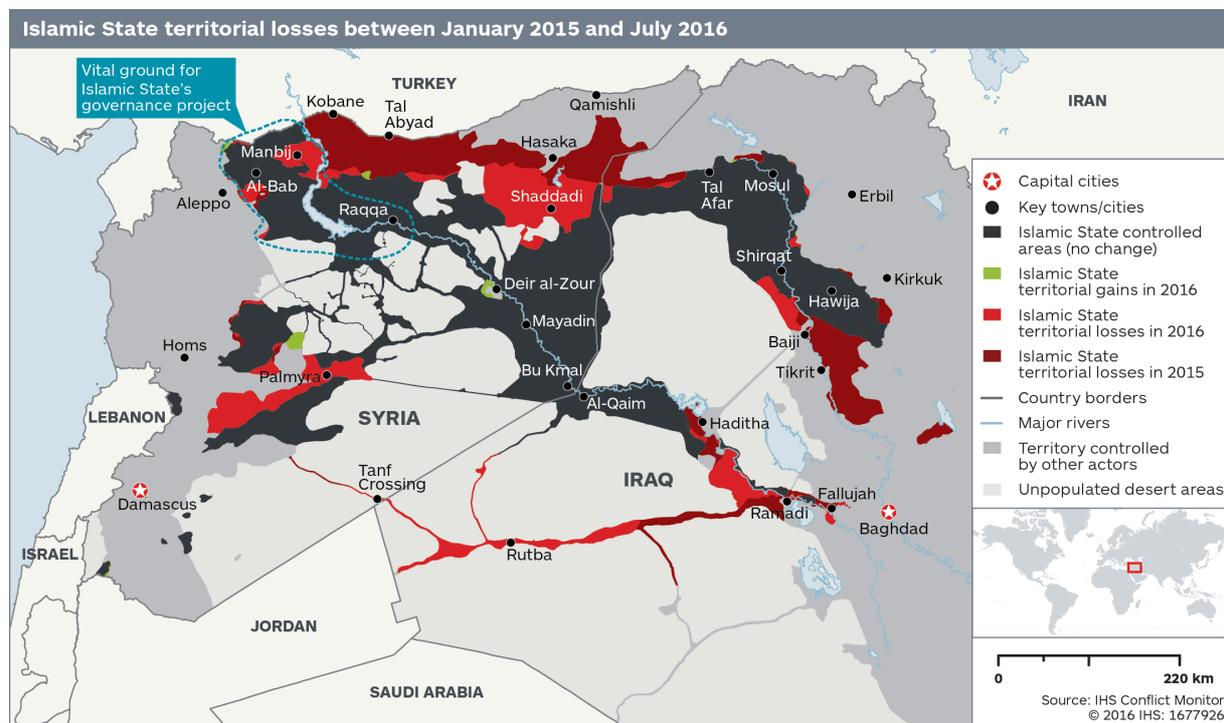
Often, contributors are not even aware that they are donating to terrorist organisations as cyberjihadists have become increasingly adept at soliciting funds. IS has made use of fundraising pleas on social media to appeal to its supporters to make financial contributions (US Department of the Treasury, 2014).⁴⁷

Counter-Terrorism Efforts Pertaining to Exploitation of the Internet and Challenges to their Success:

Having demarcated cyberjihadist strategies, it is impossible to refute that the Internet has evolved into an essential operational tool for the global jihad; and is critical to the survival of IS and its ideology. In its acknowledgement of this reality, the international community has sought to augment existing counter-terrorist measures so as to adapt to these changes. This section will outline the instruments and methods that have been developed as counter-measures to terrorism within the specific context of cyberjihad. Counter-terrorism pertains to the operations and measures taken in an effort to neutralize or undermine terrorists, terrorist networks and terrorist organizations. With regards to this study, counter-terrorist measures would suggest those activities that seek to render IS incapable of operationalizing or exploiting the Internet; to instill fear in the international community, coerce governments, achieve its goals (establish a Caliphate, encourage sympathizers to join/migrate to the Caliphate and thereafter consolidate political authority over dominion) or perpetuate its ideology.

In the case of IS, counter-terrorist measures have placed significant focus on classic military efforts that have sought to wrest physical control of territory away from IS and dismantle the Caliphate, as well as efforts to undermine IS's "...political capacity to provide essential state functions..." within its territory (Lewis, 2014:5). With regards to the former, these efforts are demonstrated in the substantial 'shrinking' of the Caliphate, which is depicted by the territorial losses in the image that follows.

⁴⁷ An example of outside contributions is illustrated in that the US Treasury Department imposed sanctions on 'Abd al-Rahman Khalaf 'Ubayd Juday' al-'Anizi for transferring funds to IS from Kuwait and for paying for the travel expenses of foreign fighters travelling to Syria (US Department of the Treasury, 2014).

Figure 5: IS territorial losses between January 2015 and July 2016

Source: (IHS, 2016a).

And with regards to the latter, much of IS's political capacity is linked to its ability to finance the Caliphate and its organizational structures. Counter-measures thus point to intensified efforts by foreign actors to undermine IS revenue; demonstrated in that "[a]lmost all the main oilfields operated by the group have been targeted by airstrikes, predominantly by the US-led coalition, resulting in reports of extensive structural damage..." and a marked decrease in oil production (IHS, 2016b). Although attacking the physical and political centres of gravity are essential to the fight against IS (Lewis, 2014:5), they alone will not succeed in defeating the group as they do not address the issue of cyberjihad. What is essential here is that IS has progressed away from an organisation and developed into more of a system. The networking and operational capacities afforded by the Internet have allowed for the deterritorialization of jihadist warfare, with the new global jihad pointing to increasingly individualised and autonomous terrorism. Dissemination of the IS ideology and greater integration of cyberjihadist strategies have meant that even should the Caliphate collapse, IS will persist. The template for the global jihad is readily available for anyone online, so that any sympathiser can contribute towards IS's goals. The survival of IS is ensured in that the

Internet has allowed for a shift towards horizontal organisation; meaning that individuals and independent groups, tied together by their common ideology, can serve as self-ressurecting cells (Ranstorp, 2007:37).

Countermeasures to Prevent Terrorist Exploitation of the Internet:

Although the efforts to tackle IS have not focused specifically on cyberjihad, this does not mean to suggest that actions have not been taken to implement countermeasures that do so. “Worldwide, governments are beginning to realize that the Internet has become an effective tool for terrorists...”, as such “[t]hey are now intensifying countering violent extremism (CVE) efforts...” (Liang, 2015:7). ‘Countering violent extremism’ is an expansive umbrella phrase used to denote the various measures employed to counter the radicalization of vulnerable populations to extremist violence. Greater integration of cyberjihad strategies into terrorist operations has led to increased recognition amongst policy-makers and academics alike “...that the de-radicalization and countering violent extremism programmes can be a more effective way of tackling extremism than purely militaristic approaches...” (Avis, 2016:1). Much like all activities, instruments and policies pertaining to issues of cybersecurity and Internet governance; measures taken to address cyberjihad have been highly variegated. Broadly speaking the countermeasures adopted by international organizations and states can be categorized into two types of methods. This study demarcates these measures as either being content-based or geared towards strategic communication.

Content-based measures to counter terrorist exploitation of the Internet focus on repressive and punitive efforts that deny access to extremist narratives disseminated by cyberjihadists and IS sympathizers, “...by taking down websites or blocking messages, as well as the prohibition of communicating and spreading radical content, and henceforth criminal prosecution of those behind it...” (van Ginkel, 2015:4). These measures point to efforts that will block/filter/remove/censor IS content online; such as the suspension of social media accounts associated with or sympathetic to IS and the removal of beheading videos. An example of such an effort is illustrated by the establishment of the Counter Terrorism Internet Referral Unit (CTIRU) in Britain which is charged with the removal of “...unlawful terrorist related material from the [I]nternet where possible and coordinate prosecutions against those found to be committing offences...” (Holden, 2010).⁴⁸ In democratic states these efforts must

⁴⁸ The CTIRU provides a platform for the public to anonymously refer material that they feel falls under the units remit (Holden, 2010).

employ legal instruments to evoke content-based measures. These measures are located within the framework of Internet Filtering Governance described in Chapter 2's literature review; with the rationale derived from concerns pertaining to both security and the preservation of moral and societal norms. Legal responses by states to the phenomenon of terrorist exploitation of the Internet are extremely variegated and differ in procedural instruments, strategic approaches and the formulation of criminal legislation. Review of legal responses reveals three key trends; "...some countries apply existing cybercrime legislation to terrorist use of the Internet; some countries apply existing counter-terrorism legislation to Internet-related acts; and, some countries have enacted specific legislation on terrorist use of the Internet ...” (CTITF Working Group Compendium, 2011:ix).⁴⁹

The second category of countermeasures outlines those efforts that are undertaken to integrate strategic communication methods to counter cyberjihadist narratives and propaganda. Tentative claims linking the growing phenomenon of radicalization to extremist narratives online has led to the realisation by states that militaristic measures will not suffice in the "...battle of ideas taking place on the [I]nternet with jihadist organisations...” (van Ginkel, 2015:5). The influx of foreign fighters to Syria and Iraq and growing frequency of lone-wolf terrorism in the west have forced governments and international organisations to acknowledge the need for CVE programmes that make use of 'soft measures' to facilitate de-radicalization in vulnerable populations. These measures point to need for a strategic balancing of counter-narratives against extremist narratives (Liang, 2015:10); with efforts falling under the broader umbrella term of strategic communications.

Strategies employed by strategic communication include public information campaigns, alternative narratives, counter-narratives and media functions. Public information strategies seek to articulate state foreign policy positions on sensitive matters and counter misinformation; usually the narrative is imbued with Western values.⁵⁰ Alternative narratives are concerned with challenging extremist narratives; these methods rely on the involvement

⁴⁹ The development of specific legislation to address terrorist use of the Internet proves to be the most advanced approach, yet the majority of states have opted for the other two approaches. This is problematic in that "...legal frameworks addressing terrorism were developed during a time when the threats relating to terrorist use of the Internet were not immediately apparent...” (CTITF Working Group Compendium, 2011:ix).

⁵⁰ An example of a the use of this strategy is evident in the establishment of the Centre for Strategic Counter-Terrorism Communications (CSCC) by the US government in 2010. Efforts under the CSCC include the #Thinkagainturnaway campaign which serves two primary purposes; "...tweeting counter-messaging material in response to the jihadi propaganda that is spread on the [I]nternet and entering into direct conversations with holders of prominent jihadist accounts...” (van Ginkel, 2015:5).

of credible individuals such as Islamic scholars and community/religious leaders who provide an alternative path to those seeking guidance in their lives, by promoting mainstream moderate understandings of Islam.⁵¹ Counter-narrative strategic communication methods aim to directly counter and undermine extremist content; this is done by ‘...debunking myths, responding to misrepresentations of facts, showing the atrocities committed, and piercing the aura of heroism and camaraderie...’ online (van Ginkel, 2015:7). The final strategic communication method outlined pertains to concerns of the role of the media in disseminating jihadist propaganda. This issue is contentious in that although it is important for the press and conventional media outlets to report on issues objectively and independently, they are inadvertently providing a platform for terrorist organisations to spread extremist messages.⁵² A plethora of CVE measures and initiatives have been evoked to counter IS cyberjihadist propaganda, hence it is far beyond the scope of this study to expound upon each project. As it not possible to put forth a comprehensive audit of the various measures in place; the following table aims to provide an overview of some of the efforts taken.

⁵¹ These efforts seek to contribute to the capacity for individuals to think critically and aim to educate individuals who are religious illiterates (van Ginkel, 2015:6).

⁵² The issue of self-censorship and the manner in which topics are framed raises the question media responsibility on the issue of jihadist propaganda (van Ginkel, 2015:7-8).

Table 3: Selected international, government and civil society CVE initiatives

What	How
Against Violent Extremism (AVE)	Google Ideas and the Institute for Strategic Dialogue connect formers, survivors and projects to exchange and disseminate information to tackle violent extremism.
Al-Sakina	Online repository of information and intervention programmes to answer questions on Islamic belief and to bring radicalised individuals back into the mainstream.
Bold Creative	Empowers credible moderates to proactively counter violent extremist messages and messengers through the Internet and social media.
Center for Strategic Counterterrorism Communications (CSCC)	Coordinates, orients, and informs strategic government communications to counter the appeal of violent extremism at audiences abroad.
The Clarion Project	An independently funded, non-profit organisation dedicated to exposing the dangers of Islamic extremism while providing a platform for the voices of moderation and promoting grassroots activism.
EXIT Deutschland	Provides support structures to enable individuals to leave extreme right-wing movements through on and offline engagement.
EXIT Fryshuset	Provides support structures to enable individuals to leave extreme right-wing movements through on and offline engagement.
Fatwa on Terrorism	Highlights arguments that terrorists use to misuse Islamic teachings. Fatwa on Terrorism contains clear-cut rebuttals of those arguments, declaring those who commit terrorist acts as disbelievers.
The French Council of the Muslim Faith	National elected body that serves as an official interlocutor with the French state in the regulation of Muslim religious activities.
Global Center on Cooperative Security	Works with national, regional, and international stakeholders to promote holistic and integrated responses to violent extremism that underscore the critical importance of human rights, the rule of law, and community engagement.
Global Survivors Network	Provides a platform for survivors of terrorism to share their experiences in their own words, working to spread their messages in vulnerable communities.
Harvard Berkman Center for Internet & Society (Viral Peace Programme)	A network of experts, educators, practitioners, and ambassadors that facilitate, promote, and strengthen collaboration to counter youth-oriented hate speech online.
Hedayah	Established to serve as the premier international institution for training, dialogue, collaboration, and research to counter violent extremism.
Institute for Strategic Dialogue (ISD)	ISD created www.counterextremism.org , an online resource for policy makers working on radicalisation. It includes an up-to-date repository of government policies and programmes.
Islam Against Extremism	Presents profiles of prominent British Islamist extremists and organisations with a view to exposing them as deviants who are not actually following the path of Islam.
MyJihad	Promotes a moderate understanding of the term "Jihad" and derives a new user-generated, centre-ground narrative on matters of religion and faith.
Sabahi/Magharebia	Two websites providing independent and impartial coverage of news and current affairs, to promote alternative news sources to counter misinformation.
Women without Borders	Women without Borders promotes the role of women in the security sphere, encouraging them to become active participants in their communities.

Source: (Liang, 2015:9).

UN Countermeasures to prevent Terrorist Exploitation of the Internet:

Having outlined the measures adopted by states and international organizations to counter cyberjihad, it is clear that efforts and initiatives are highly diverse. The lens of the UN is used once again to focus the scope of legal instruments that serve in the battle against IS on the

Internet. In 2005, the UN established the Counter-Terrorism Implementation Task Force (CTITF) so as to facilitate the co-ordination of counter-terrorist efforts that take place amongst all relevant UN organs and specialized agencies (CTITF Working Group Compendium, 2011:v). The work of the CTITF has been substantial and has culminated in two landmark developments; that have a significant bearing on efforts to counter cyberjihad. The first is UN General Assembly Resolution 60/288 and the second is UN Security Council Resolution 2178.

Resolution 60/288, adopted by the UN General Assembly in September 2006 placed on the agenda ‘The United Nations Global Counter-Terrorism Strategy’. Resolution 60/288 drew upon existing instruments such as Resolution 1624⁵³ and the UN Charter to establish the groundwork for criminalising terrorist exploitation of the Internet. The unanimous adoption of the Resolution represents a milestone in multinational counter-terrorism efforts; committing member states to the unequivocal condemnation of terrorism and urging international co-operation to take measures to combat and prevent it. Most notably Resolution 60/288 invites member states to collaborate with the UN

with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to: (a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard (UN, 2016).

The second development points to the adoption of Resolution 2178 by the UN Security Council in September 2014, which “...represents a watershed in the global civilian effort to reduce the threat from foreign fighters...in Syria and Iraq...” (Liang, 2015:8). The Resolution was borne out of growing concerns that ICTs, the Internet in particular, were increasingly used by terrorists and their supporters for numerous activities including recruitment, radicalization, financing, inciting others to commit attacks and conducting travel arrangements for foreign fighters. Resolution 2178 underlines

the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights

⁵³ UN Security Council Resolution 1624 reaffirms previous Resolutions on Terrorism, and calls on member states to strengthen border security (UN, 2005).

and fundamental freedoms and in compliance with other obligations under international law (UN, 2014).

The Resolution calls for greater international co-operation in its request to member states to increase national measures to prevent terrorists from exploiting technology in pursuit of their goals. Emphasis is placed on addressing the growing phenomenon of foreign fighters, and the Internet's role in "...financing and facilitating [their] travel and subsequent activities..."; IS is explicated as an entity of particular concern in this regard (UN, 2014). As such, the Resolution necessitates that state members boast laws that facilitate the prosecution of individuals who travel or attempt to travel for terrorist purposes.

Factors Undermining Effective Internet Related Counter-Terrorism Efforts:

Strategic communication efforts and content-based measures are essential to the fight against IS online, yet numerous challenges to effective countermeasures persist. This study has grouped together various pervading issues so as to identify three primary challenges to preventing terrorist exploitation of the Internet; the first encompasses issues of co-operation and co-ordination; the second pertains to concerns of human rights and liberal principles; and the last challenge relates to strategic value and causality. The challenge presented by co-ordination and co-operation to effective countermeasures stems from the very nature and the decentralized structure of the technology associated with the Internet. The 'flattening' of organizational structures and the shift to global jihad brought on by the omnipotence of the Internet has meant that cyberjihadist can operate with little regard for borders. As such, governments and international organizations alike have asserted that "[t]errorist use of the Internet is a transnational problem, requiring an integrated response across borders and among national criminal justice systems..." (UNODC, 2012:15). Although international recognition of the threat posed by exploitation of the Internet by terrorist organizations has certainly grown; a universal instrument that specifically addresses this pervasive feature of jihadist activity has yet to be developed.

This renders countermeasures "...difficult to design, implement, and evaluate..." (Fidler, 2015:2). There is no international legislation or policy to uniformly and coherently address the issue of countering the dissemination of jihadist material online and so these measures are enacted at the political level through means of a plethora of different laws and approaches. States have not reached consensus amongst themselves on what constitutes terrorist related

content online and national criminal justice systems differ substantially on processes for investigating and prosecuting terrorist cases. As such countermeasures to cyberjihad have not been coordinated amongst states owing to the challenges presented by issues of law enforcement and criminal justice authorities. The problem can be demonstrated in that even if content is illegal in a particular state, it could be hosted in another (Avis, 2016:6). Efforts and measures that are taken to remove or censor jihadist content are negated in that cyberjihadists could simply republish the material on a different Internet domain where content-based measures are not taken. Another area that has proven problematic in relation to international co-operation points to the issue of “...satisfying the dual criminality requirements in extradition and mutual legal assistance requests...”⁵⁴ (UNODC, 2012:15). It is not only content-based measures that are hindered by lack of coordination as developing international cooperation is essential to support the production and dissemination of credible counter extremist narratives and positive alternatives to radical content both on- and off- line (Liang, 2015:1).

Whilst distinct challenges to effective countermeasures arise from want of a proactive and coordinated response from states and lack of capacity of national justice systems to implement the provisions of existing international legal instruments against terrorism, the absence of collaboration between the public and private sectors has also served to hinder efforts. Although the responsibility for countering jihadist exploitation of the Internet ultimately lies with state actors, the social media platforms and “...most of the technical infrastructure upon which terrorists are planning, financing and supporting their illegal activities is owned wholly or in part by private entities...”, which renders cooperation with private sector stakeholders crucial to effective execution of countermeasures (CTITF Working Group Compendium, 2011:x). However, due to the nature of the web business, private sector actors have demonstrated that “...they can neither be forced nor expected to police the hundreds of thousands of websites...” and accounts with which cyberjihadists are affiliated (McNeal, 2007:804). Whether stakeholders from the private sector are either

⁵⁴ The Counter-Terrorism Implementation Task Force Working Group on Countering the Use of Internet for Terrorist Purposes notes that there has been a number of “...cases in which mutual legal assistance or extradition requests had been delayed or refused because of problems satisfying dual criminality requirements. In some cases, that had been a result of the incompatibility of criminal offence provisions, but in others it was the result of an unduly restrictive approach to judicial interpretation of corresponding criminalization provisions by the judiciary. Several experts considered that this situation highlighted the need for training for members of the judiciary on international cooperation issues...” (UNODC, 2012:91).

unwilling to cut off their clients or simply unaware that they are hosting jihadist material, lack of cooperation between the private and public sectors has certainly hampered efforts to counter terrorists use of the Internet (CTITF Working Group Compendium, 2011:x).

The second challenge to effective countermeasures identified in this study is derived from concerns regarding the preservation of human rights and liberal principles. These challenges are essentially linked to content-based measures that seek to censor and criminalize the dissemination of extremist material online. As such, content-based measures could result in the violation of fundamental human right to freedom of expression (van Ginkel, 2015:4). The values enshrined by the UN and democratic states are intrinsically at odds with censorship. In the UN Global Counter-Terrorism Strategy, member states reaffirmed that human rights obligations served as an integral facet of the international legal counter-terrorism framework; "...both through the obligation imposed on states to prevent terrorist attacks, which have the potential to significantly undermine human rights, and through the obligation to ensure all counter-terrorism measures respect human rights..." (UNODC, 2012:19).

Liberal principles could also be compromised in that content-based measures often mandate the use of covert surveillance so as to monitor IS communication and social media activity online. Not only does robust state surveillance pose potential implications for freedom of speech, it also serves to challenge the right to privacy (Fidler, 2015:3). Because there is no consensus on what serves to denote terrorist content, principles of legality come into question as it becomes necessary to determine whether material or statements do in fact intend to radicalize or incite global jihad (van Ginkel, 2015:4).. Transparency issues arise in that removal of terrorist content in democratic states happens mainly through the private sector; companies censor material or terminate accounts that violate their user policies. This is demonstrated in that on 2 April 2015, Twitter claimed to have suspended 10, 000 accounts linked to IS in one day for "...tweeting violent threats..."⁵⁵ (Gladstone, 2015). Without greater transparency, it becomes difficult to determine the legitimacy of these activities, "...especially when companies act on requests from governments or in response to criticism from public officials and politicians..." (Fidler, 2015:3).

⁵⁵ This claim cannot be verified because Twitter does not make its data public (Gladstone, 2015).

The final challenge to effective countermeasures stems from uncertainty regarding the strategic value and causal relation of content-based and strategic communication measures. Self-radicalization and recruitment through the Internet is an anomaly. "...[M]ost experts agree that radicalization is a highly complex and individualized process, often shaped by a poorly understood interaction of structural and personal factors..." (Vidino & Hughes, 2015:15); so despite numerous studies on the phenomenon, the complexities that are involved in the process render it extremely difficult to make strong policy prescriptions (Fidler, 2015:3). A 2013 study by the RAND Corporation posits that whilst the Internet certainly does create more opportunities for radicalization, its research did not establish a direct causal link demonstrating the role of the Internet in accelerating the process or its role in self-radicalization without any physical contact (von Behr *et al.*, 2013:xii).⁵⁶

With regards to strategic communication; demonstrating the success of preventative work and that efforts have been effective will always be difficult. Although making vulnerable populations resilient to extremist narratives is essential to the long term battle against cyberjihad, current measures taken to stymie IS's appeal have been criticized as ill-conceived as states and international organizations have failed to turn the tides in the battle of ideas (Fidler, 2015:3). The growing number of Islamic extremist websites and content online and the spread of self-generating cells and lone-wolf attacks in Western states would seem indicative of an expansion in "...the radical and violent segment of the West's Muslim population..." (Vidino & Hughes, 2015:18). Whilst IS continues to lose territory, its ambition and allure seems to inversely grow as efforts to expand its global presence are heightened.

Although there has been increased recognition of the need to exercise content-based measures, with some states deeming them essential to the battle against cyberjihad current efforts have been ineffective. Censorship efforts are dwarfed by the sheer volume of extremist content online. What's more any actions taken to remove content and websites or suspend social media accounts are usually negated by cyberjihadists, who just immediately

⁵⁶ The RAND Corporation is an independent non-profit organization that conducts policy research with the aim of improving policy and decision-making practices through analysis and research in the interest of the public. The study conducted on 'Radicalisation in the digital era' tested 5 hypotheses developed from a literature review against primary data collected from 15 case studies on terrorism and extremism (von Behr *et al.*, 2013:xi). It is worth noting that this study was conducted before IS had claimed notoriety in 2014. As IS social media campaign has enjoyed success far beyond that of other terrorist organizations, the primary data collected from the case studies no longer provides an adequate sample.

repost material or create new websites or accounts. “IS supporters on social media are like the hydra; cut off one head and two more shall take its place...” (Liang, 2015:10). Further strategic difficulties to content-based measures stem from criticism that they serve to be counter-productive. The argument lies in that when jihadists operate in the public, there activities can be tracked and monitored. Removing jihadist websites or social media accounts would mean investigators would no longer be able to do so; and should IS supporters opt to create new accounts and websites, investigators would first have to locate them before repeating the process reducing efforts to an eternal and time consuming game of cat and mouse (van Ginkel, 2015:4). Another concern is that greater censorship efforts will lead jihadists to turn to the Dark Web,⁵⁷ which would make locating content and surveillance astronomically more difficult.

This section has made it abundantly clear that despite widespread recognition of the continued threat posed by IS to international security and peace, current efforts to counter jihadist activity will not suffice. Although substantial gains have been made against IS in terms of military victories and loss of extremist territory and revenues, these efforts alone will not result in the defeat of the group in that its successful exploitation of the Internet has facilitated the establishment of a cyber-Caliphate that will ensure the survival of IS through the perpetuation of its ideology and the flattening of its hierarchal structure to include decentralized self-resurrecting cells. Although substantial challenges have served to undermine the effectiveness of countermeasures against terrorist exploitation of the Internet, efforts can be taken to ensure that these measures are executed in a more efficacious way. The provisions made by Securitisation Theory allow for exceptional measures to be adopted when addressing a security concern that has been identified as posing an existential threat to a referent object of value. These extraordinary measures justify the use of actions that take place “...outside the normal bounds of political procedure...” (Buzan *et al.*, 1998:24); hence

⁵⁷ The Dark Web (sometimes Deep Web or Darknet), refers to the parts of the Internet that are not considered part of the surface world wide web. Although they are public, websites and forums are hidden and can't be discovered by standard search engines. The Dark Web hides IP addresses of the servers that run them making it extremely difficult to figure out who is behind the sites. Websites make use of dynamic pages and encryption networks, so that it is not possible to access them unless a pathway to the page and a password is provided. A study by the Dutch Intelligence Service in 2012 asserted that “...99.8 percent of online terrorist activities take place at the hidden levels of the [I]nternet...” (van Ginkel, 2015:2). When individuals participate actively in jihadist narratives, recruiters invite them to join the Dark Web forums. “Pathways to chat rooms can be found on social media accounts of extremist groups and their supporters...” (Liang, 2015:2).

they may potentially serve to overcome the challenges posed to effective countermeasures against terrorist exploitation of the Internet.

Application of Theory – Securitising the Internet:

This section seeks to apply the theory describing the securitisation process to the case of IS and cyberjihad. Application of theory serves to delineate the steps that need to be taken in order for securitisation to be realised. "...[T]he exact *definition* and *criteria* of securitisation is constituted by the intersubjective establishment of an existential threat with a saliency to have substantial political effects..." (Buzan *et al.*, 1998:25). Extrapolation of the theory reveals that securitisation is a three-part process. The first step in the process is the securitising move wherein analysis of discourse reveals that an existential threat to a referent object has been presented. The second step identifies evidence of acceptance of the threat by a given audience, where after an issue is successfully securitised. Finally, the third step is the uptake of extraordinary measures and restrictive responses aimed at increasing security. As this is an exploratory study, existing policies and efforts used to tackle terrorist exploitation of the Internet are combined with Internet governance modalities and legal tools evoked in cybersecurity to envision the securitisation process and outcomes.

Identifying Security Discourses and Threat Construction:

Delving into developments in Internet governance, cybersecurity and counter-terrorist strategies reveals that the issue of terrorist exploitation of the Internet and consequently, cyberjihad, is located at the intersection of numerous security discourses. Security discourses pertaining to the threat of terrorism are overt and explicit. The so called 'Global War on Terror' demonstrates a rare case of a successful macrosecuritisation as the events of 9/11 energised the Bush and Blair administrations to pursue global alliances and international partnerships against what is perceived to be the universal threat of terrorism (Buzan & Wæver, 2009:254). Macrosecritisations represent top-ranking threats in that the audience at the global or system level is usually states. Convincing the audience that parochial securitisations will not suffice is a monumental feat mandating an existential threat of momentous notoriety.⁵⁸ Identifying the discourse is simple in that the all-encompassing 'Global War on Terror' "...amalgamates over 100 national security policies into an international anti-terrorist cooperative..." (Kingsmith, 2013:4). Evidence of securitisation at

⁵⁸ Examples of other macrosecritisations include top-ranking threat issues such as nuclear proliferation and increasingly, concerns of global warming and climate change.

the system level is illustrated by the cumulative efforts of the UN's CTITF and its Global Counter-Terrorism Strategy; such as the passing of Resolution 2178 by the UN Security Council, which reaffirms

that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever and by whomsoever committed, and *remaining* determined to contribute further to enhancing the effectiveness of the overall effort to fight this scourge on a global level... (UN, 2014).

Although terrorist exploitation of the Internet is certainly included in security discourses regarding terrorism, there is no explicit policy or strategy addressing the issue. Much like the discourse surrounding terrorism, security speech acts in cybersecurity issues are easy to locate. Cybersecurity usually focuses on the role of the Internet as a critical infrastructure and the need to ensure its safety so as to preserve the security and economic interests of the nation state. Beyond the recognition of the Internet as essential to the functioning of the state, cybersecurity discourse has incorporated concerns of cyber-threats that stem from vulnerabilities that manifest from use of information technologies such as cyber-terrorism, cyber-crime and concerns of information security. Institutional developments and the overabundance of state strategies for developing cyber defences demonstrates that "...cybersecurity *is* successfully securitised..." (Hansen & Nissenbaum, 2009:1157). However, again, cyberjihad is not specifically addressed; rather it is incorporated under the framework of legal tools used to address cybercrime or is inappropriately assimilated with issues of cyber-terrorism. Integrating cyberjihad into issues of cybercrime is problematic in that framing an issue as such de-escalates the threat; as characteristically incidences of 'crime' are addressed by the police and do not suggest the need for extraordinary measures or military involvement. The distinction exists in that it is the difference between a national security concern or a problem for law enforcement (Cavelty, 2007:84).

Lastly, practices in Internet governance reveal how securitisation of the Internet can be (and already has been) realised. In Internet governance it is revealed that the Internet is not completely free and unfettered as it is limited by code and physical nodes of interface that make interaction predictable and forces finite characteristics on the network. The Internet is governed not only by the normative consensus afforded to the Internet service providers and

operators (without whom the network would not function), but also by public and private actors such as states and corporations who “...understand how leveraging and exploiting key nodes within the physical structure of the Internet can give them strategic political, social and economic advantages...” (Kingsmith, 2013:6). As demonstrated by the Freedom House findings, the imposition of filtering and surveillance mechanisms online is widespread and common practice (Kelly *et al.*, 2015). States and private companies regularly engage in filtering and surveillance practices in the interest of security, yet these practices are not revealed in the public domain and are carried out in secrecy. The enforcement of Internet security has been realised in non-democratic states such as China, where securitisation of access to the Internet is “...legitimised through references to national-cultural as well as regime security...” (Hansen & Nissenbaum, 2009:1157). These actions are not limited to non-democratic or authoritarian regimes as they take place in democratic states as well. Yet they do not constitute securitisations, in that a securitisation is not “...fulfilled only by breaking rules (which can take many forms) nor solely by existential threats (which can lead to nothing) but by cases of existential threats that legitimize the breaking of rules...” (Buzan *et al.*, 1998:25).

It is clear from review of these existing securitisations that the development of a security discourse pertaining to the prevention of the exploitation of the Internet by terrorists has already been created in part. The legal framework, policies and practices (particularly content-filtering) required for a securitising move are readily available. What remains is the need to demonstrate why cyberjihad should be perceived as a threat in its own right, rather than have it subsume a pre-existing narrative that cannot appropriately address the complexities or challenges it entails. For a securitising move to take place, cyberjihad must first be constructed as an existential threat to a referent object (Buzan *et al.*, 1998:36). Preventing terrorists from exploiting the Internet would suggest that the referent object in the securitisation is the Internet itself. This easily ties in with dominant cybersecurity discourses that assert that the Internet is a critical infrastructure essential to the survival of the state. However, review of the cyberjihadist strategies reveal that it is not the Internet that is under threat but rather the traditional object of the state and more specifically its constituents.

To elucidate, the concern presented by terrorists on the Internet does not stem from the threat of cyber-terrorism wherein computers are used to attack networks or systems, with the intention of carrying out a politically motivated violent attack against people or property. Not

only do cyberjihadists lack the technical capacity to carry out such an attack, but also there is currently no evidence that cyber-terrorist techniques have been used for serious destructive activity. Contrastingly, cyberjihad has been “...used for many activities that directly support war...” and insurgent attacks (McNeal, 2007:793). The Internet has provided the perfect operational tool for enabling the goals of many terrorist organisations with cyberjihadist strategies such as propaganda dissemination, recruitment and communication of ideologies; being carried out on a daily basis online. “Terrorist use of the Internet is common, even though cyber-terrorism is rare...”; with the former posing serious consequences to international security (Lachow, 2009:437).

If the referent is taken to be the global population, framing cyberjihad as an existential threat is straightforward as the activities carried out on the Internet on a daily basis have directly supported the ongoing global jihad. The consequences of which are plainly obvious in the deaths of thousands of people around the world (Yourish *et al.*, 2016), and the threat posed to national security by increased radicalisation to extremist narratives and its bearing on the possibility of future lone-wolf attacks (Vidino & Hughes, 2015). As demonstrated by the theory on macrosecuritisations; system level securitisations have already constructed all of humankind as the security referent “...most notably in terms of shared fears of nuclear annihilation...” and with recent decades the growing threat of terrorism (Buzan *et al.*, 1998:36). Whilst terrorism has already been successfully framed as an existential threat it is necessary to develop a discourse that specifically highlights the threats posed by terrorist exploitation of the Internet, which will ultimately aid in tackling cyberjihad.

Public messages from IS leaders reveal that the group is preparing its followers for the eventual collapse of the Caliphate. Yet even as IS core structures have come under attack in Syria and Iraq the group has continued to make appeals to its sympathisers for support in the global jihad. The Internet has allowed the group to expand and shift some of its “...command, media and wealth structure to different countries...”, which suggests that it is increasingly likely that IS will evolve from a quasi-state to a diffuse network of cells (Warrick & Mekhennet, 2016). The threat to the international community remains as shifting organisational structures and deterritorialisation of IS will reduce the efficacy of solely militaristic measures and IS movements and intentions will become more difficult to decipher. Dialling back the rhetoric on cyber-terrorism and developing a specific security discourse on preventing terrorist exploitation of the Internet is necessary for establishing

effective counter-measures to cyberjihad. Positioning the Internet as a strategic asset in the cyberjihad will serve to demarcate it as an issue mandating extraordinary measures. The securitising move exists in that the Internet must be made secure against terrorist exploitation and cyberjihad so as to protect international peace and security.

Acceptance of the Securitising Move by a Relevant Audience:

The second stage of the securitisation process pertains to the probability that an audience beyond those who are advancing the securitisation will accept the discourse surrounding a securitising move. As outlined in the chapter on theory, one of the factors that serve to influence the success of a securitising move is the credibility of the securitising actor. To reiterate, the securitising actors in Securitisation Theory are those who "...securitise issues by declaring something – a referent object – existentially threatened..." (Buzan *et al.* 1998:36). Although in theory any unit or individual can instigate a securitising move, the field is biased in that some actors are imbued with social capital that affords them greater credibility in the securitising field. Generally states are regarded as the securitising actor, but as preventing terrorist exploitation of the Internet and the global jihad mandate transnational cooperation and the existing security framework for countering terrorism depicts a macrosecuritisation; the UN is deemed to be the actor most likely to succeed in convincing an audience of a securitising move.

Realising effective countermeasures against cyberjihad requires an integrated response among national criminal justice systems and supersedes borders, hence the UN is regarded as having a pivotal role to play in that it is uniquely positioned in the global system to build consensus among Member States of how best to tackle the use of the Internet for terrorist purposes (UNODC, 2012:15). Because the UN fulfils a crucial responsibility in facilitating the discussion and the sharing of good practices on the issue; the organisation serves as the only actor capable of both; raising the profile of terrorist exploitation of the Internet to a global threat; and able to abet the identification of effective measures to be taken, particularly with regards to the implementation of Security Council Resolution 2178 (Painter, 2015). By virtue of its position of power and credibility in the international system, the UN (its Security Council organ in particular) is largely accepted as a voice of security, thus this study perceives it to be the ideal vehicle for mobilising a securitising move. By virtue of the UN's power to define security and proffer solutions derived from technical research and knowledge from task forces such as the CTITF, it is the actor most likely to be perceived as legitimate in

the eyes of a given audience. Another constraining factor that serves to influence whether a securitising move is accepted or not is the legitimacy of the claim.

Although censorship online sits at odds with liberal-democratic principles, it is certainly occurring. But it is worth noting that in many cases, censorship through Internet filtering governance is wholly justifiable. “Child pornography, human trafficking webpages, identify theft sites, xenophobic and genocidal forums, these are desecuritized norms that the majority of network subscribers would no doubt debate and advocate to be restricted...” (Kingsmith, 2013:11). Excluding its effects on investigations and surveillance, it is difficult to envisage how a case that is against securing the Internet from terrorist exploitation would be made. Since the 9/11 attacks the issue of terrorism in the global system has been a highly sedimented issue. The devastating attacks shocked the international community, invoking the ‘Global War on Terror’ and essentially a climate of constant low-level threat. The construction of the cyberjihad threat can thus draw upon a deeply sedimented context in that historically, culturally, rhetorically, institutionally and significantly discursively (Williams, 2003:514); terrorism is an issue that has a substantial bearing on the international society.

Furthermore, IS’s social media and propaganda campaign has been phenomenally effective in terms of scope and impact. Regularly carried out lone-wolf attacks, professionally choreographed videos and an endless stream of jihadi online material has served to create an environment of constant terror as IS has achieved a “...blurring effect between the real and virtual worlds, producing an artificially high degree of intimacy with the battlefield...” (Ranstorp, 2007:46). Whilst cyberjihad has allowed IS to disseminate propaganda at an unprecedented rate, cyberjihadist content online has also functioned as ‘visual facts’ that can be incorporated into security discourses by providing evidence that justifies the claims of the legitimacy of the threat (Friis, 2015:727). This context and the social praxis that accompany it thus provide favourable felicity and facilitating conditions for a securitising move to be accepted. The ‘extreme’ urgency of the situation is easily demonstrated; moreover (in terms of morality) it is unlikely that a given audience will object to the need to counter cyberjihad.

The founding fathers of Securitisation Theory do not identify the audience as a distinct unit in security analysis. Doing so lacks utility in that the same security discourse can be evoked to target different audiences. Only the referent, the securitising actor and functional actors are demarcated. Functional actors in Securitisation Theory are those “...actors who affect the

dynamics of a sector...”; they are neither the referent or the securitising actor but they significantly influence “...decisions in the field of security...” (Buzan *et al.*, 1998:36). If a securitising move is made to prevent terrorists from exploiting the Internet, this study identifies the UN as the securitising actor and the global population as the referent at the system level. The private sector is demarcated as the functional actor in that the infrastructure and operation of the Internet is dependant on it; and cooperation from private stakeholders and companies is essential to content-based countermeasures. This would suggest that states are the audience in that need to be convinced of the need for greater international co-operation and more effective measures. Although state recognition of the threat of terrorist exploitation is assured, international co-operation is not certain and democratic countries have had limited success in public-private partnerships. Policy-makers must be persuaded that placing restrictions on the Internet serves in the interest of security and the greater good; even if doing so lies in contradiction of civil liberties and free-market values of non-intervention.

Extraordinary Measures:

The final step in the Securitisation process is the uptake of extraordinary measures and restrictive responses aimed at increasing security. In realising this final step, Securitisation Theory does not “...push the demand so high as to say that an emergency measure has to be adopted...”, rather it states that the existential threat must have been successfully argued so as to garner sufficient resonance “...for a platform to be made from which it is possible to legitimize emergency measures...”, or other efforts that could not be realised had the discourse not been framed in terms of existential threats (Buzan *et al.*, 1998:25). The imperative to act immediately allows an issue that has been successfully securitised to be taken out of the realm of ordinary politics. In the case of terrorist exploitation of the Internet acceptance of the need for extraordinary measures could provide the conditions requisite; to overcome challenges presented by consideration of civil liberties and human rights; to facilitate transnational cooperation; to potentially coerce the private sector should they not cooperate voluntarily; and to mobilise greater resources to develop effective countermeasures. The section of this chapter that follows will develop upon this vein of thought by looking at the potential benefits and shortcomings of Internet securitisation to combat terrorist exploitation of the Internet in terms of the case of IS cyberjihad.

Shortcomings and Benefits of Securitisation in Countering Cyberjihad:

The benefits of securitisation as strategy for countering cyberjihad can be assessed by reviewing the possible ways it can aid and abet existing countermeasures; by reducing challenges to them. The three challenges to effective countermeasures for preventing terrorist exploitation of the Internet identified in this study are; issues of co-operation and co-ordination; concerns of human rights and liberal principles; and establishing strategic value and causality. This section begins by demonstrating how securitisation could possibly be used to overcome these challenges.

The issue of coordination and cooperation in establishing countermeasures has long since hindered attempts to secure the Internet. Review of the challenges faced in developing effective countermeasures to prevent Internet exploitation by terrorists, reveals significant weaknesses in the international system that stem from disparities in the laws and practices among individual states; which serve to limit investigations and prosecution attempts. “The Internet and other aspects of the information infrastructure are inherently transnational...” as is the threat posed by cyberjihad; hence a sufficient response necessitates transnational cooperation (Sofaer & Goodman, 2001:2). Both the threat of terrorism and the need to address cybersecurity threats such as the growth in cybercrime have led state actors to pursue bilateral and multilateral cooperation initiatives for prosecution and extradition in the interest of security capacity-building. In terms of cybersecurity, substantial efforts have been made to foster international cooperation in preventing the criminal misuse of ICTs (UN, 2001), and towards creating “...a global culture of cybersecurity...” (UN, 2004). The same is true of counter-terrorist efforts as illustrated by the UN’s global counter-strategy.

Although diplomatic efforts on these issues have certainly aided cooperation in preventing terrorist exploitation of the Internet, current transnational efforts are not sufficient and are losing the battle in cyberspace. State reluctance to share information and compromise on policies has limited coordination. “[T]he cyber domain broadly defined cannot be devoid of the inevitable contentions that arise when competing interests consolidate around different principles and priorities and then collide when actors with different intents and capabilities seek to pursue their objectives...” (Choucri, 2012:125). IS’s global campaign of terror has ensured that the group has succeeded in turning itself into an enemy of ostensibly every state in the world. However, the legal regimes and instruments for identifying, investigating and tracking terrorist related content online remain limited (Davis, 2006:128). “While no fewer

than six UN bodies and multiple regional and national forums have sought to build a consensus on the future of Internet governance, there has been little progress thus far...” (Knake, 2010:vii). Failure to collaborate on issues of Internet Governance and cybersecurity translate into impediments for preventing cyberjihad in that it links in with issues of Internet Filtering Governance and Structural Management Governance. Although state consensus on the issue is the same, no international agreement explicitly addressing the threat of terrorist exploitation of the Internet exists; which means there is substantial room for state actors to further develop international cooperation. The case for Internet securitisation so as to counter the global jihad will aid in the cooperation effort as states threatened by the groups advance will be incentivised to align their interests (Cronin, 2015:97).

The challenge of preventing cyberjihad requires a holistic range of responses that includes both voluntary and legally mandated cooperation. Securitisation at the level of the UN Security Council will aide in this matter. “Council [R]esolutions adopted under Chapter VII of the Charter of the United Nations are binding on all Member States...”(UNODC, 2012:15). The UN Security Council is able to apply legally binding obligations on member states or at the very least, provide ‘soft law’ which is imbued with substantial political importance in terms of creating sources for policy commitments or emerging norms in international law. The UN General Assembly has also demonstrated how it can be a useful source of soft law to address the cyberjihadist threat, as it has passed numerous resolutions on the issues of cybersecurity and terrorism. Should diplomatic efforts fail; in this manner securitisation can enforce transnational cooperation and coordination through existing international legal frameworks and instruments.

The other concern highlighted by challenges to cooperation and coordination is the issue of private-public collaboration. The development and operation of the Internet is largely attributed to private-sector expertise. As such states are considered latecomers to the cyber-domain and have generally boasted limited powers over cyberspace. This laissez faire legal environment is attributed with having exponentially driven technological innovation and commercial growth of the Internet (Davis, 2006:127), which serves as the primary motivation for private-sector stakeholders to reject state intervention.⁵⁹ What’s more, democratic states often boast free-market principles that are opposed to intervening in the private sector. In the

⁵⁹ This ties in with the global culture of cyber-libertarianism (Barlow, 1996).

absence of a centralised authority responsible for regulating the Internet, private stakeholders have continued to play a vital role in “...controlling the availability of terrorism-related content disseminated via the Internet...” (UNODC, 2013:123). This role is not limited to content, as the private sector is also positioned to assist in disrupting terrorist communications and access online, as well as contribute to monitoring and surveillance efforts that could help identify extremist activity that may promote radicalisation.

What is crucial here however is that the private sector is self-regulating and Internet service providers (ISPs) worldwide are not compelled to monitor cyberjihadist content or control access to their servers “...until they are made aware of egregious contents on a particular site...” (Davis, 2006:134). Lack of effective governance mechanisms online combined with the knowledge that ISPs are not mandated to regulate content and access to their servers, has provided a relatively lawless environment for cyberjihadists to carry out their operations. Extremists have sought to “...exploit the online space created by limitations on government power and the private sector’s reluctance to police cyberspace...” (Fidler, 2015:4). Lack of public-private cooperation is thus a serious impediment to effective countermeasures against cyberjihad. Securitisation is useful in that by singling out IS as a global pariah and identifying the Internet as a strategic asset that is crucial to the operation and survival of the global jihad, it is possible to identify specific conditions under which state actors can be convinced to forgo free-market principles and compel the private sector to co-operate.

Blanket attempts to secure the Internet have been unsuccessful as demonstrated by the limited success of public-private collaborations. The benefits of securitising the Internet are evident in that it allows for the extraordinary measures requisite to justify state intervention in the private sector. Concomitantly, this reflects a downside of securitisation in that intervention could serve to impact innovation and growth. However, these effects can be mitigated by isolating IS as a virtual *persona non grata*. Because the private sector is more likely to promote security interests “...when its is needed to meet customer expectations...or in attempts to meet standards of due care to avoid negligence...” (Sofaer & Goodman, 2001:21), imposing a virtual embargo on IS as a security measure would provide conditions to convince the private sector to cooperate voluntarily. Modelling this concept on the UN’s sanction regimes for targeting terrorism, securitisation allows the Internet to be framed as an asset. The UN must create public sanction lists of individuals or groups who conduct

cyberjihadist activities and “...must establish penalties for providers and hosts who negligently provide services to blacklisted users lists...” (Davis, 2006:182).

The second challenge posed to effective countermeasures to cyberjihad is derived from consideration of Human rights and civil liberties. In theory, the extraordinary measures permitted to combat an existential threat subsequent to a successful securitising will provide the conditions necessary for these considerations to be overlooked. However, ensuring Human rights and the rule of law is one of the four pillars informing the UN Global Counter-Terrorism Strategy. If the UN is taken as the securitizing actor in a move to prevent terrorists from exploiting the Internet, it is unlikely that Human rights and civil liberties will be excluded from considerations in counter-terrorist efforts. It is important to note here that the preservation of Human rights and the exacting of effective countermeasures are not in fact mutually exclusive. On the contrary, in underscoring the importance of Human rights and the rule of law; UN Security Council Resolution 2178 notes that “...that failure to comply with these and other international obligations, including under the Charter of the United Nations, is one of the factors contributing to increased radicalization and fosters a sense of impunity...” (UN, 2014).

This highlights a major detrimental effect of Internet securitisation in that vaguely formulated counter-terrorism legislation that does not comply with principles of legality and violations of rights to due process and fair trial may substantially infringe on Human rights considerations. Following a discussion by the Human Rights Council, the UN Human Rights Office of the High Commissioner (UNHROHC) asserted that although countering terrorism is imperative, countermeasures that limit freedom of expression and peacefully assembly must be “...proportionate and serve a legitimate goal...” and conducted under “...strict oversight...” (UNHROHC, 2015). The downside of Internet securitisation in this regard stems from concern that states around the world have often sought to exploit counter-terrorist strategies as an excuse to evoke punitive measures targeted against otherwise legitimate activities, such as journalism or criticism of governments. Apprehension on this issue is legitimate, as actions taken by the Shanghai Cooperation Organisation (SCO) serve to justify concerns⁶⁰. In 2015

⁶⁰ The SCO is an Eurasian international organisation composed of membership by China, Russia, Tajikistan, Kazakhstan, Kyrgyzstan and Uzbekistan for the purposes of military, political and economic cooperation. In 2009 member states to the SCO entered an Agreement on ‘Cooperation in the field of Information Security’ (SCO, 2008).

the member states of the SCO submitted a letter to UN General Assembly, which outlined the proposal for an international code of conduct for information security. The proposal asserted that; "...policy authority for Internet-related public issues is the sovereign right of states...", and sought to enforce the need to "...tie people's real names and identities to online activity..." (Kingsmith, 2013:11). The proposal was rejected in that this level of content regulation was perceived to threaten fundamental human rights.

The application of extraordinary measures denotes shifting an issue out of the realm of the public and ordinary political discourse. However current Internet filtering practices demonstrate that both states and the private sector have pursued filtering and surveillance practices that exhibit a systematic lack of accountability and transparency. "Although discussions of this issue often frame government intervention as an infringement on free speech, in reality, social media companies currently regulate speech on their platforms without oversight or disclosures of how suspensions are applied..." (Berger & Morgan, 2015:3). Lack of state intervention has meant that content filtering practices online have been left to the discretion of private companies, opening the legitimacy of these actions to criticism (Fidler, 2015:3). A feature of this study that proves to be exceptionally interesting stems from the potential for Internet securitisation to enhance human rights and civil liberties.

The contemporary global political economy reflects the substantial growth in power of multinational corporations, who control extensive human and material resources; allowing them to exert greater political influences than the majority of states. In an effort to counter these influences, which are often not benign, states are "...increasingly assigned the responsibility by many security analysts to defend human rights...and to promote social welfare by checking the power of multinational corporations..." (Kolodziej, 2005:16). This concept is easily transposed to the case of IS and cyberjihad in that the security incentives may force reluctant states to assume a greater role in content regulation practices, which could foster more effective private-public collaborations. However, for securitisation to be beneficial it is essential that states articulate the specific conditions under which they will request companies to implement content-based measures (Fidler, 2015:4).

The final challenge to effective countermeasures highlights uncertainty regarding the strategic value and causal relation of content-based and strategic communication measures. In the battle of ideas, IS activity in the cyber-domain has revealed that state actors are proving

unsuccessful in preventing the spread of extremist ideologies. Yet it is not simply the exposure to jihadist narratives online that has led to increased radicalisation. Young Muslims are growing up in an environment of ostracisation as they are spurned for their faith and religious beliefs in increasingly Islamophobic Western societies. It is isolation that leads individuals to withdraw from mainstream society, which serves as a necessary condition for the breeding of extremist behaviours. For many of these young individuals, solace is found in IS narratives. The strategic value of content-based measures is brought into question, conversely securitisation would seem to have little bearing on preventing radicalisation.

Whilst the strategic value of content-based measures can be debated, it is not possible to refute the value of strategic communication efforts both on- and off- line. “Cyber Islamic [e]nvironments have the potential to transform aspects of religious understanding and expression within Muslim contexts,...access to the [I]nternet has become a significant element of propagation and identity for Muslim individuals and organisations...” (Bunt, 2003:4). Internet securitisation could potentially have a direct impact on realizing more effective countermeasures in that framing cyberjihad as an existential threat could allow for the allocation of greater resources to tackle terrorist exploitation of the Internet. The online campaign against IS will require a substantial economic commitment in order to promote national plans and capacity-building amongst state for content-based measures. The benefits are even more pronounced in efforts that aim to promote more effective strategic communication countermeasures, specifically with regards to developing alternative and counter narratives. “Although Muslim organizations in the Middle East, Pakistan, Indonesia, and Europe have had some success countering violent extremism...these groups desperately need financial assistance to continue their work...” (Husain, 2013:1). Securitisation serves to catapult an issue to the top of the security agenda, thus the allocation of additional resources falls under the mandate of extraordinary measures which could serve to address the funding gap.

Conclusion:

This chapter boasts a three-part structure; first it develops a case study; followed by the application of Securitisation Theory to the research; and finally, an attempt to demonstrate the benefits and shortcomings of securitising the Internet. The chapter began by providing background knowledge of the development of IS and its use of the Internet in cyberjihadist strategies. Demarcation of cyberjihadists strategies served to demonstrate the different ways

terrorists have sought to exploit the Internet as an advanced operational tool. Cyberjihadist strategies outlined in this study include; propaganda; recruitment and radicalisation; communication, organisation and strategic planning; operational training; and fundraising. Thereafter, the study went on to highlight the different strategies that have been used to prevent terrorists from exploiting the Internet, with all efforts falling under the categories of being either content-based or strategic communication measures. This was followed by an outline of the challenges posed to these efforts. Once the case was sufficiently contextualised, the study then proceeded to evoke Securitisation Theory to demonstrate how Internet securitisation can be realised. After demonstrating that justification of extraordinary measures is possible, this study attempted to explore how Internet securitisation could benefit countermeasures to preventing cyberjihad; or indeed, highlight the potential shortcomings thereof.

Resituating the chapter in terms of the research problem reveals that private companies such as Twitter and YouTube, amongst others, have a pivotal role to play in ensuring effective application of countermeasures to preventing terrorist exploitation of the Internet. Considerations of human rights illustrates that state actors and the private sector have already undermined these concerns in that censorship online is carried out with relative impunity. The different sections of this chapter were structured in such a way as to directly address the research questions. This is elaborated upon in the final chapter of the study that follows. In the concluding chapter, the study attempts summarise all findings and to answer the research questions and research problem identified in the introduction. The study concludes by outlining potential areas for future research.

CHAPTER 5: Conclusion

This study has applied the theoretical assumptions of the Copenhagen School's Securitisation Theory to the case of IS integration of cyberjihad strategies in an effort to explore the utility of securitisation in developing more effective measures to counter terrorist exploitation of the Internet. Pervading security discourses have illustrated that policy-makers have displayed a tendency to fixate on concerns of cyber-terrorism, yet terrorists have instead sought to operationalize the Internet rather than threaten the global network. Despite substantial evidence of IS success in integrating cyberjihad into its operational strategies, no international policies or agreements that aim to specifically address this threat exist. Rather, the issue of terrorist exploitation of the Internet has been subsumed under the mandate and discourse of narratives pertaining to cybersecurity, information security and terrorism. This study suggests that framing the Internet as a critical asset to the global jihad and creating a discourse that specifically addresses the issue of the integration of the Internet into terrorist operations will allow for more effective countermeasures to be executed. In this, the concluding chapter of this study, all research and findings are reiterated. The chapter begins by summarising the study. Thereafter, the chapter will draw upon the findings and assertions developed throughout the study in an effort to explicitly address the research questions.

Summary of the Study:

Chapter 1 of this study put forth a general introduction to the research field by developing a background understanding of how issues of the Internet and international security fall under the mandate of IR. After outlining IS's rise to prominence, the chapter segued into the problem statement; linking concerns of international security to challenges presented by terrorist exploitation of the Internet. Thereafter, primary and secondary research questions were identified before briefly outlining the primary tenets of Securitisation Theory. The chapter went on to elucidate upon the research design and methodology of the study and concluded by providing a summary of its chapters.

Chapter 2 sought to further expound upon the understanding developed in the introduction as the terminology, operational details, and security challenges pertaining to the Internet depict a highly esoteric body of literature, thus mandates exposition. Internet Governance modalities were taken as a starting point to familiarise the study with the various facets of the Internet and to facilitate subsequent research. Demarcation of modalities led the study to identify five

types of Internet Governance, recognised as; Standardization and Protocol Governance; Intellectual Property Governance; Internet Security Governance; and Internet Filtering Governance. Differentiation between these different typologies highlights the complexities of the Internet by identifying numerous actors, protocols and policies involved in governance. The chapter then went on to describe prominent discourses surrounding debates regarding the future of the Internet's governance architecture. This served to draw attention to the role of states with regards to matters of the Internet. Discourse of Internet Governance was then linked to concerns of the international security context by focusing on issues of cybersecurity and information security. Due to variegation amongst state policies and strategies; major developments in the fields of information security and cybersecurity conducted under the UN were used to indicate the overall international security context.

Chapter 3 demonstrates the study's efforts to ground the research in a theory of International Relations. Securitisation Theory was selected as the guiding theoretical framework for this study. By first locating its theoretical underpinnings within the broader discipline of Security Studies, this chapter sought to demonstrate the utility of Securitisation Theory by emphasising the limits of major IR theories' explanatory power. The study asserts that Securitisation Theory is useful in that it can account for the multifariousness of actors and complexities of issues surrounding security considerations of the Internet. The Chapter does this by first describing the development of Security Studies, the epistemological debates it encompasses and its mainstream theoretical approaches. Thereafter it proceeds to provide a comprehensive account of Securitisation Theory before demonstrating its value as an analytical framework in the contemporary security context.

Chapter 4 attempted to integrate the body of research conducted in the earlier chapters and develop the case of IS and cyberjihad so that the study could solve the primary and secondary questions identified in Chapter 1. This Chapter began by elucidating upon the background of Islamic State and its application of cyberjihadist strategies that were identified as; propaganda creation and dissemination; recruitment and radicalization; strategic operations; operational training; and fundraising. The chapter then went on to delineate the different measures adopted by the international community to prevent terrorist exploitation of the Internet and the challenges they face. Review of the different measures led to the development of the content-based measures and strategic communication measures typology. Once more, the UN was adopted as a lens to narrow the scope of the study and ensure

consistency with preceding chapters. Challenges to preventing terrorist exploitation of the Internet, were identified as; issues of cooperation and co-ordination; concerns of human rights and liberal principles; and establishing strategic value and causality. Thereafter, application of theory was evoked to explore how securitizing the Internet could be achieved. Augmenting understandings developed throughout the study and extrapolation and inference based on existing countermeasures, policies and frameworks were then employed in an attempt to investigate the potential shortcomings and benefits of Internet securitisation as a means to undermine IS operations that employ cyberjihad strategies.

Solving the Research Questions:

Primary Research Question: What utility can Internet securitisation boast in an effort to mitigate the perceived threat of Islamic State (IS) cyberjihadism?

This study recognises the benefits of emergency measures in overcoming the challenges that serve to undermine the effectiveness of countermeasures that aim to prevent terrorist exploitation of the Internet. On the issue of cooperation and coordination, Internet securitisation is seen as useful in that it can facilitate the conditions necessary to foster cooperation amongst states, as well as amongst the public and private sector. A successful macrosecuritisation will serve to jettison the issue of terrorist exploitation to the highest level of the global security agenda; hence in theory it should provide the requisite motivating conditions. If states or the private sector do not willingly collaborate, legally binding instruments and soft law can be evoked to coerce actors into cooperating. On the challenge of preserving Human Rights and civil liberties, this study suggests that Internet securitisation need not compromise these values. If the UN pushes the securitisation, it is highly unlikely that measures will neglect these considerations as preservation of Human rights and rule of law is indoctrinated into all UN counter-terrorist efforts. In addition, review of current Internet filtering practices demonstrates that both state and private sector actors have evoked content-based measures with relative impunity.

If content-based measures are left to the discretion of the private sector they are to be considered non-politicised. Securitisation could shift them along the spectrum and by mandating state intervention, could be used to ensure greater accountability and transparency. The challenge of states exploiting Internet securitisation as an excuse to evoke punitive measures against legitimate activities remains; as illustrated by the actions of states belonging

to the SCO. At best Internet securitisation can attempt to mitigate these detrimental effects by ensuring legislation informing countermeasures complies with principles of legality and are not vaguely formulated. On the challenge of strategic value and causality, the benefits of securitisation can't be ascertained. However, the additional resources afforded by extraordinary measures will certainly serve to aid and abet current countermeasures. Not only could greater funding allow countermeasures to be executed more successfully, but the commitment of greater research resources could allow for further investigation into the development of effective countermeasures. In terms of strategic communication measures, the benefits of additional resources are most pronounced, as research suggests these efforts are strained by lack of funding.

Secondary Research Questions:

1. How have cyberjihadists sought to exploit the Internet? This study has demarcated five overarching strategies in which cyberjihadists have succeeded in exploiting the Internet. These strategies have been identified as; propaganda creation and dissemination; recruitment and radicalization; strategic operations; operational training; and fundraising.
2. What measures have been taken to counter cyberjihad and to what degree have these measures proven successful? This study has categorized the countermeasures adopted by international organizations and states to prevent terrorist exploitation of the Internet into two types of methods; namely, all measures fall under the umbrella terms of being either content-based or geared towards strategic communication. Content-based measures point to repressive and punitive efforts that aim to block/filter/remove/censor terrorist accounts or extremist content online. The second category of countermeasures outlines strategic communication methods to counter cyberjihadist narratives and propaganda. 'Soft measures' point to the need for a strategic balancing against extremist narratives by means of public information campaigns, alternative narratives, counter-narratives and media functions. The success of these measures has been limited, as numerous challenges to their effectiveness exist. These challenges are identified as; issues of co-operation and co-ordination; concerns for human rights and liberal principles; and difficulties in establishing strategic value and causality.

3. What are the disadvantages and benefits of securitisation of the Internet in terms of the international security context? This study recognises that at the intersection of the Internet and international security considerations, concerns of cybersecurity and information security arise. Security discourses surrounding cybersecurity and information security demonstrate existing securitizations. Securitisation of the Internet in this regard is thus viewed as redundant, in that its position as a critical ICT infrastructure means that issues pertaining to the Internet and international security are already sufficiently addressed by discourses of cybersecurity and information security. A major shortcoming of securitising the Internet points to concerns regarding the dangerous precedent it may set for censorship online. Several state actors have already sought to assert their sovereignty and authority in the cyber domain by adopting repressive Internet Filtering governance practices. Not only does this raise normative concerns about possible infringements on Human Rights and freedoms, it may serve to undermine future technological innovation and development of the Internet as fragmentation and balkanisation of the network could serve to constrict information flows, create access disparities and adversely affect the architecture and resilience of the Internet.

Areas for Future Research:

In Chapters 1 and 2, this study demonstrates that the success and preponderance of the Internet as a global resource has served to elicit new threats to state security and a shift in traditional understandings of power relations. This is evident in that the decentralised and ascendant structure of its framework proves complex and poses difficulties to the application of governance norms. In addition, the even landscape of the Internet has meant that states are now progressively exposed to competition from non-state actors. Global networking and interdependency have effectively served to empower non-state actors. A potential area for future research exists in that a study could attempt to determine how changes wrought on the international system by the Internet could serve to threaten or undermine traditional notions of state sovereignty.

Another potential area for future research is identified in Chapter 3, which engages with the theoretical assertions of Securitisation Theory. Proponents of Securitisation Theory firmly locate its principles and arguments in Constructivism, hence it subsumes a post-positivist logic. By rejecting positivism, Securitisation Theory dismisses the need for theory to

demonstrate causality. However, because Securitisation Theory provides a conceptual framework that can be replicated and securitisation itself must be enacted as a process, variables in a study can be temporally and analytically separated. This serves to meet the conditions for falsifiability. Of course, Securitisation Theory is not truly falsifiable in that concepts in Social Sciences can only be approximated, however an argument can be made that Securitisation Theory comes closer to demonstrating causality than the positivist theories that strive to do so. An area for future research is apparent in that there is potential for developing upon the theoretical arguments of Securitisation Theory by engaging with epistemological and ontological debates.

Finally, the research encompassed by this body of work has been conducted as a single case study that specifically focuses on IS and its integration of cyberjihadist strategies. Areas for future research are evident in Chapter 4 as a study could apply a similar framework to investigate other terrorist organisations such as Boko Haram or Al-Shabaab and determine whether they have successfully integrated cyberjihad into their operational strategies. Research need not be limited to terrorist exploitation of the Internet. Other research possibilities stem from the potential to apply a similar framework to other cyber-threats such as cybercrime or hacktivism.

BIBLIOGRAPHY:

- Acharya, A. 1997. “The periphery as the core: the Third World and security studies”, in Krause, K. & Williams, M. C. (eds.). *Critical Security Studies: Concepts and Cases*. Minneapolis: University of Minnesota Press. 299-328.
- Act No. 144. 2000. *Basic Act on the Formation of an Advanced Information and Telecommunications Network Society* [Online]. Available: <http://www.cas.go.jp/jp/seisaku/hourei/data/BAFAITNS.pdf> [2016, September 26].
- Al Jazeera. 2014. ‘*Syrian troops beheaded*’ in *Raqqa* [Online]. Available: <http://www.aljazeera.com/news/middleeast/2014/07/reports-syrian-troops-beheaded-raqqa-20147268024618783.html> [2016, October 4].
- ARIN. 2012. *World Conference on International Telecommunications* [Online]. Available: <https://www.arin.net/participate/governance/wcit.html> [2014, August 16]
- Arquilla, J. & Ronfelt, D. (eds). 2001. *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica, CA: RAND Corporation.
- Ashok, I. 2016. *Isis members share 'how to hack' tutorials encouraging supporters to target western intelligence* [Online]. Available: <http://www.ibtimes.co.uk/isis-members-share-how-hack-tutorials-encouraging-supporters-target-western-intelligence-1577097> [2016, October 5].
- Austin, J. L. 1971. *How to do Things with Words*. London: Oxford University Press.
- Avis, W.B. 2016. *The role of online/social media in countering violent extremism in East Africa*. GSDRC Helpdesk Research Report 1380. Birmingham, UK: GSDRC, University of Birmingham.
- Axelrod, R. 1984, *The Evolution of Cooperation*. New York: Basic Books.
- Baldwin, D. A. 1997. The concept of security. *Review of International Studies*, 23(5):5-26.
- Balzacq, T. 2011. “A theory of securitization – Origins, core assumptions and variants”, in Balzacq, T. (ed.). *Securitization Theory: How Security Problems emerge and dissolve*. Abingdon, Oxon: Routledge. 1-30
- Barakso, M., Sabet, D. M. & Schaffner, B. F. 2014. *Understanding Political Science Research Methods: The Challenge of Inference*. New York: Routledge.
- Barlow, J. P. 1996. *A Declaration of the Independence of Cyberspace* [Online]. Available: <https://projects.eff.org/~barlow/Declaration-Final.html> [2014, August 16].

- Barrett, R., Berger, J., Ghosh, L., Schoenfeld, D., el-Shawesh, M., Skinner, P.M., Sim, S. & Soufan, A. 2015. *Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq*. New York: The Soufan Group.
- BBC News. 2014. *What is Jihadism?* [Online]. Available: <http://www.bbc.com/news/world-middle-east-30411519> [2016, July 16].
- Bell, D. 1976. *The Coming of the Post-Industrial Society: A Venture in Social Forecasting*. New York: Basic Books.
- Berger, J. M. & Morgan, J. 2015. *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter*. Center for Middle East Policy – Analysis Paper. Washington, D.C.: Brookings.
- Booth, K. 1991. Security and Emancipation. *Review of International Studies*, 17(4):313-326.
- Bowcott, O. 2011. *Internet freedom 'is a matter for the UN'* [Online]. Available: <http://mg.co.za/article/2011-06-18-internet-freedom-is-a-matter-for-un> [2016, September 30].
- Bradner, S. 1999. The Internet Engineering Task Force, in DiBona, C. & Ockman, S. (eds.). *Open Sources: Voices from the Open Source Revolution*, California: O'Reilly Media, Inc. 47-52.
- Brenner, S.W. 2005. Why the Law Enforcement Model is a Problematic Strategy for Dealing with Terrorist Activity Online. *Proceedings of the Annual Meeting – American Society of International Law*. 99:108-112.
- Bunt, G. R. 2003. *Islam in the digital age: E-Jihad, Online Fatwas and Cyber Islamic Environments*. London: Pluto Press.
- Burnham, P., Lutz, K. G., Grant, W. & Layton-Henry, Z. 2008. *Research Methods in Politics 2nd Ed*. New York: Palgrave Macmillian.
- Buzan, B. 1983. *People, States & Fear – The National Security Problem in International Relations*. Sussex: Wheatsheaf Books Ltd.
- Buzan, B. 1997. Rethinking Security after the Cold War. *Co-Operation and Conflict*, 32(1):5-28.
- Buzan, B. & Hansen, L. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.
- Buzan, B. & Wæver, O. 2009. Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory. *Review of International Studies*, 35(2):253-276.

- Buzan, B., Wæver, O. & de Wilde, J. 1998. *Security: A New Framework for Analysis*. Colorado: Lynne Rienner Publishers.
- Bygrave, L. & Bing, J. 2009. *Internet Governance: Infrastructure and Institutions*. Oxford: Oxford Press.
- Byres, E. 2013. The air gap: SCADA's enduring security myth. *Communications of the ACM*, 56(8):29-31.
- Carmack, C. 2005. *How BitTorrent Works* [Online]. Available: <http://computer.howstuffworks.com/bittorrent1.htm> [2016, September 23].
- Carman, A. 2015. *Filtered extremism: how ISIS supporters use Instagram* [Online]. Available: <http://www.theverge.com/2015/12/9/9879308/isis-instagram-islamic-state-social-media> [2016, October 5].
- Cavelty, M. D. & Mauer, V. 2010. Introduction, in Caveltly, M. D. & Mauer, V. (eds.). *The Routledge Handbook of Security Studies*. Oxon: Routledge. 1-6.
- Cavelty, M. D. 2007. *Cyber-security and threat politics: US efforts to secure the information age*. Taylor & Francis e-Library.
- Choucri, N. & Goldsmith, D. 2012. Lost in cyberspace: Harnessing the Internet, international relations and global security. *Bulletin of the Atomic Scientists*, 68(2):70-77.
- Choucri, N. 2012. *Cyberpolitics in International Relations*, Cambridge, MA: MIT Press.
- Clarke, R.A. & Knake, R. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Harper Collins.
- CoE. 2016. *Chart of signatures and ratifications of Treaty 185 – Convention on Cybercrime* [Online]. Available: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures> [2016, October 1].
- Coll, S. & Glasser, S. B. 2005. *Terrorists Turn to the Web as a Base of Operations* [Online]. Available: <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html> [2016, July 16].
- Comey, J.B. 2015. *Counterterrorism, Counterintelligence, and the Challenges of Going Dark - Statement Before the Senate Select Committee on Intelligence* [Online]. Available: <https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark> [2016, October 5].
- Crane, E., Cheer, L., Lee, S. & Piotrowski, D. 2014. *Terror boss praises convicted terrorist Khaled Sharrouf as 'good, loveable kid' ...while his 7-year-old holds a severed head* [Online]. Available: <http://www.dailymail.co.uk/news/article-2721230/Thats-boy->

- Australian-jihadists-seven-year-old-son-poses-decapitated-head-Syrian-solider.html [2016, October 4].
- Cronin, A. K. 2015. ISIS is not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat. *Foreign Affairs*, 94(2):87-98.
- CTITF Working Group Compendium. 2011. *Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects*. New York: UN.
- Dahlgren, P. 2005. The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation. *Political Communication*, 22(2):147-162.
- Davis, B.R. 2006. Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance. *CommLaw Conspectus: Journal of Communications Law and Technology Policy (1993-2015)*, 15(1):119-186.
- De Beer, J. & Clemmer, C. D. 2009. Global trends in online copyright enforcement: a non-neutral role for network intermediaries? *Jurimetrics*, 49:375–409.
- de Borchgrave, A., Cillufo, F. J. Cardash, S. L. & Ledgerwood, M.M. 2000. *Cyber Threats and Information Security Meeting the 21st Century Challenge*. Washington, D. C.: Center for Strategic and International Studies (CSIS).
- Declaration of Principles Building the Information Society: a global challenge in the new Millennium*. 2003. [Online]. Available: <http://www.itu.int/wsis/docs/geneva/official/dop.html> [2014, August 24].
- Deibert, R. & Rohozinski, R. 2008. Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet, in Deibert, R., Palfrey, J. Rohozinski, R. & Zittrain, J. (eds.). *Access Denied: The Practice and Policy of Global Internet Filtering*. Massachusetts: MIT Press. 123-149.
- Deibert, R. J. & Rohozinski, R. 2010. Risking security: policies and paradoxes of cyberspace security. *International Political Sociology* 4(1): 15–32.
- Deibert, R. J. 2003. Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium Journal of International Studies*, 32(3):501-530.
- Deibert, R. J., Palfrey, J., Rohozinski, R. & Zittrain, J. (eds.). 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. Massachusetts: MIT Press.
- Deibert, R. J., Palfrey, J., Rohozinski, R. & Zittrain, J. (eds.). 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Massachusetts: MIT Press.
- Deibert, R. J., Palfrey, J., Rohozinski, R. & Zittrain, J. (eds.). 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Massachusetts: MIT Press.

- DeNardis, L. 2009. *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: MIT Press.
- Denning, D. 2001. Activism, Hacktivism, and Cyberterrorism, in Arquilla, J. & Ronfeldt, D. F. (eds.). *Networks and Netwars: The Future of Terror, Crime and Militancy*. Santa Monica: Rand Corporation. 239-288
- Department of Defense. 2010 (As amended through 15 February 2016). *Joint Publication I-02: Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: The Joint Staff.
- Ellis, R., Fantz, A., Karimi, F. & McLaughlin, E. C. 2016. *Orlando Shooting: 49 killed, shooter pledged ISIS allegiance* [Online]. Available: <http://edition.cnn.com/2016/06/12/us/orlando-nightclub-shooting/> [2016, July 16].
- Eriksson, J. & Giacomello, G. 2007. Introduction: Closing the gap between international relations theory and studies of digital-age security, in Eriksson, J. & Giacomello, G. (eds.). *International Relations and Security in the Digital Age*. Abingdon, England: Routledge. 1-28.
- Esposito, J.L. (ed.). 2003. *The Oxford Dictionary of Islam*. New York: Oxford University Press.
- Faris, R. & Villeneuve, N. 2008. Measuring global Internet filtering, in Deibert, R., Palfrey, J., Rohozinski, R. & Zittrai, J. (eds.). *Access Denied: The practice and policy of global Internet filtering*. Massachusetts: MIT Press. 5-28.
- Farrell, M. 2016. *Quietly, symbolically the US control of the internet was just ended* [Online]. Available: <https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana> [2016, September 24].
- Fidler, D. P. 2015. *Countering Islamic State Exploitation of the Internet – Cyber Brief*. New York: Council on Foreign Relations.
- Final Acts: World Conference on International Telecommunications*. 2012. Dubai: International Telecommunications Union.
- Friis, S.M. 2015. ‘Beyond anything we have ever seen’: beheading videos and the visibility of violence in the war against ISIS. *International Affairs*, 91(4):725-746.
- Gauntlett, D. (ed.). 2000. *Web. Studies: Rewiring media studies for the digital age*. London: Arnold.
- Gilpin, R. G. 1996. No one loves a political realist. *Security Studies*, 5(3):3-26.
- Gladstone, R. 2015. *Twitter Says It Suspended 10, 000 ISIS-Linked Accounts in One Day* [Online]. Available: <http://www.nytimes.com/2015/04/10/world/middleeast/twitter->

- says-it-suspended-10000-isis-linked-accounts-in-one-day.html?_r=0 [2016, October, 9].
- Goldsmith, J. & Wu, T. 2006. *Who Controls the Internet? Illusions of a Borderless World*. New York, NY: Oxford University Press.
- Graham-Harrison, E. 2015. *Could ISIS's 'cyber caliphate' unleash a deadly attack on key targets?* [Online]. Available: <https://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race> [2016, July 16].
- Gross, G. ICANN Leaders Push for Broad-based Internet Governance [Online]. Available: http://www.cio.com/article/743534/ICANN_Leaders_Push_for_Broad_based_Internet_Governance [2014, August 24]
- Hansen, L. & Nissenbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4):1155-1175.
- Heickerö, R. 2014. Cyber Terrorism: Electronic Jihad. *Strategic Analysis*, 38(4):554-565.
- Hinnen, T.M. 2004. The Cyber-front in the War on Terrorism: Curbing Terrorist Use of the Internet. *The Columba Science and Technology Review*, 5(5):1-42.
- Hofmann, J. 2005. Internet Governance: A Relative Idea in Flux, in Bandamutha, R. K. J. (ed.). *Internet Governance: An Introduction*. India: Icfai University Press. 74-108.
- Holden, M. 2010. *Factbox: How UK's anti-terrorism internet unit works* [Online]. Available: <http://www.reuters.com/article/us-security-internet-factbox-idUSTRE6932AY20101004> [2016, October 9].
- Hughes, C. W. & Lai, Y. M. (eds.). 2011. *Security Studies: A Reader*. Abingdon, Oxon: Routledge.
- Huntington, S. P. 1997. *The Clash of Civilizations and the Remaking of World Order*. New Delhi: Penguin Books India
- Husain, E. 2013. *Policy Innovation Memorandum No. 37*. New York: Council on Foreign Relations.
- 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.
- ICT Data and Statistics Division. 2015. *ICT Facts and Figures – The world in 2015*. Geneva: International Telecommunication Union.
- IHS. 2016. *Islamic State Caliphate Shrinks a Further 12 Percent in 2016, IHS Says* [Online]. Available: <http://press.ihs.com/press-release/aerospace-defense-security/islamic-state-caliphate-shrinks-further-12-percent-2016-ihs> [2016, October 7].

- ISOC. 2013. Internet Society Questionnaire on Multistakeholder Governance [Online]. Available: <http://www.internetsociety.org/sites/default/files/bp-msfinalreport-20132010-en.pdf> [2014, August 24].
- IT Strategy Headquarters. 2000. *Special Action Plan on Countermeasures to Cyber-Terrorism of Critical Infrastructure (Provisional Translation)* [Online]. Available: http://japan.kantei.go.jp/it/security/2001/cyber_terror.html [2016, September 30].
- IT Strategy Headquarters. 2001. *e-Japan Strategy* [Online]. Available: http://japan.kantei.go.jp/it/network/0122full_e.html [2016, September 30].
- ITU. 2016 a. *WSIS Forum 2016* [Online]. Available: <https://www.itu.int/net4/wsis/forum/2016/> [2016, September 23].
- ITU. 2016 b. *National Strategies* [Online]. Available: <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx> [2016, September 30].
- ITU. 2016 c. *National Strategies Repository* [Online]. Available: <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx> [2016, October 1].
- Jarvis, L., Macdonald, S. & Whiting, A. 2015. Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage. *Perspectives on Terrorism*, 9(1). Available: <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/402/html> [2016, June 29].
- John, T. 2015. *Timeline: The Rise of ISIS* [Online]. Available: <http://time.com/4030714/isis-timeline-islamic-state/> [2016, October, 7].
- Kalathil, S. & Boas, T. C. 2003. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. New York: Carnegie Endowment for International Peace.
- Kallberg, J. & Thuraisingham, B. 2013. From Cyber Terrorism to State Actors' Covert Cyber Operations, in Akhgar, B. & Yates, S. (eds.). *Strategic Intelligence Management – National Security Imperatives and Information Communication Technologies*. Oxford: Butterworth – Heinemann. 229-233.
- Kelly, S., Earp, M., Reed, L., Shahbaz, A. & Truong, M. 2015. *Freedom on the Net 2015*. :Freedom House.
- Kelly, S., Truong, M., Earp, M., Reed, L., Shahbaz, A. & Greco-Stoner, A. (eds.). 2012. *Freedom On the Net 2013: A Global Assessment of Internet and Digital Media*, Freedom House.
- Kenney, M. 2015. Cyber-Terrorism in a Post-Stuxnet World. *Orbis*, 59(1):111-128.

- Keohane, R. O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.
- Keohane, R. O. 2002. *Power and Governance in a Partially Globalized World*. London: Routledge.
- Kingsmith, A. T. 2013. Virtual Roadblocks: The Securitisation of the Information Superhighway. *Bridges: Conversations in Global Politics and Public Policy*, 2(1):1-14.
- Klein, H. 2004. Understanding WSIS: An Institutional Analysis of the UN World Summit on the Information Society. *Information Technologies and International Development*, 1(3-4):3-13.
- Kleinwachter, W. 2008. Multi-Stakeholder Internet Governance: the Role of Governments, in Benedek, W., Bauer, V. & Kettemann, M. C. (eds.). *Internet Governance and the Information Society: Global Perspectives and European Dimensions*. Netherlands: Eleven International Publishing. 9-29.
- Knake, R.K. 2010. *Internet Governance in an Age of Cyber Insecurity*. Council Special Report No. 56. New York: Council on Foreign Relations.
- Kolodziej, E. A. 2005. *Security and International Relations*. Cambridge: Cambridge University Press.
- Kuerbis, B. 2011. *Securing critical internet resources: Influencing internet governance through social networks and delegation*. New York: School Information Science and Technology - Dissertations. Paper 68.
- Lachow, I. 2009. Cyber Terrorism: Menace or Myth, in Kramer, F. D., Starr, S. H. & Wentz, L. K. (eds.). *Cyberpower and National Security*. Washington, DC: National Defence University Press. 437-464.
- Lessig, L. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.
- Lewis, J.D. 2014. *The Islamic State: A Counter-Strategy for a Counter-State*. Middle East Security Report 21. Washington, DC: Institute for the Study of War.
- Liang, C. S. 2015. *Cyber Jihad: Understanding and Countering Islamic State Propaganda*. Policy Paper. Geneva: Geneva Centre for Security Policy.
- Logan, R. 2016. *ISIS conducts online bomb-making tutorials over Skype to recruit youths* [Online]. Available: <http://www.mirror.co.uk/news/world-news/isis-conducts-online-bomb-making-7292245> [2016, October 5].
- Lu, H. & Liang, B. 2010. Internet development, censorship, and cyber crimes in China. *Journal of Contemporary Criminal Justice*, 26(1):103-120.

- Maher, S. 2007. Road to Jihad. *Index on Censorship*, 36(4):144-147.
- Malcolm, J. 2008. *Multi-Stakeholder Governance and the Internet Governance Forum*. Perth: Terminus Press.
- Mathiason, J. 2008. *Internet Governance: The New Frontier of Global Institutions*. New York: Routledge Global Institutions.
- McDonald, M. 2008. "Constructivism", in Williams, P. D. (ed). *Security Studies: An Introduction*. Oxon: Routledge. 59-72.
- McNeal, G. S. 2007. Cyber Embargo: Countering the Internet Jihad. *Case Western Reserve Journal of International Law*, 39(3):789-826.
- Moravcsik, A. 2001. *Liberal International Relations Theory: A Social Scientific Assessment*. Cambridge: Harvard University Press.
- Morgan, S. 2016. *Cyber Crime Costs Projected To Reach \$2 Trillion by 2019* [Online]. Available: <http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#413764003bb0> [2016, July 16].
- Morgenthau, H. J. 1966. "The purpose of political science", in Charlesworth, J.C. (ed.). *A Design for Political Science: Scope, Objectives, and Methods*. Philadelphia: American Academy of Political and Social Science. 63-79.
- Mueller, M. L. & van Eeten, M. J. G. 2012. Where is the governance in Internet governance? *New Media Society*, 15(5):720-736.
- Mueller, M. L. 1999. ICANN and Internet Regulation. *Communications of the ACM*, 42(6):41-43.
- Mueller, M. L. 2010. *Networks and States: The Global Politics of Internet Governance*. Massachusetts: MIT Press.
- Mueller, M. L., Mathiason, J. & Klein, H. 2007. The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance*, 13(2):237-254.
- Mueller, M., Schmidt, A. & Kuerbis, B. 2013. Internet Security and Networked Governance in International Relations. *International Studies Review*, 15(1):86-104.
- National Academy of Sciences. 1991. *Computers at Risk: Safe Computing in the Information Age*. Computer Science and Telecommunications Board. Washington, D.C.: National Academy Press.
- Negroponte, J. D., Palmisano, S. J. & Segal, A. 2013. *Defending an Open, Global, Secure and Resilient Internet*. Independent Task Force Report No. 70. New York: Council on Foreign Relations.

- Negroponte, J. D., Palmisano, S. J. & Segal, A. 2013. *Defending an Open, Global, Secure and Resilient Internet*. Independent Task Force Report No. 70. New York: Council on Foreign Relations.
- Nicks, D. 2016. *Why ISIS is Going Broke* [Online]. Available: <http://time.com/money/4251494/why-isis-is-going-broke/> [2016, October 7].
- Painter, C. 2015. *Remarks at a Special Meeting of the UN Counter-Terrorism Committee on Preventing Terrorists from Exploiting the Internet and Social Media to Recruit Terrorists and Incite Terrorist Acts, while Respecting Human Rights and Fundamental Freedoms* – Coordinator for Cyber Issues, U.S. Department of State [Online]. Available: <http://usun.state.gov/remarks/7062> [2016, October 14].
- Paris, R. 2011. “Human Security”, in Hughes, C. W. & Lai, Y. M. (eds.). *Security Studies: A Reader*. Abingdon, Oxon: Routledge. 71-79.
- Parliament of Australia. 2001. *Bills Digest No. 58 2001-02 Cybercrime Bill 2001* [Online]. Available: http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048 [2016, September 26].
- Passeri, P. 2016a. *March 2016 Cyber Attacks Statistics* [Online]. Available: <http://www.hackmageddon.com/2016/04/21/march-2016-cyber-attacks-statistics/> [2016, July 14].
- Passeri, P. 2016b. *April 2016 Cyber Attacks Statistics* [Online]. Available: <http://www.hackmageddon.com/2016/06/01/april-2016-cyber-attacks-statistics/> [2016, July 14].
- Peoples, C. & Vaughan-Williams, N. 2010. *Critical Security Studies: An introduction*. Oxon: Routledge.
- Ranstorp, M. 2007. The virtual sanctuary of al-Qaeda and terrorism in an age of globalization, in Eriksson, J. & Giacomello, G. (eds.). *International Relations and Security in the Digital Age*. New York: Routledge. 31-56.
- Rose, G. 1998. Neoclassical realism and theories of foreign policy. *World Politics*, 51(1):144-172.
- Rousseau, D. L. & Walker, T. C. 2010. “Liberalism”, in Cavelty, M. D. & Mauer, V. (eds.). *The Routledge Handbook of Security Studies*. Oxon: Routledge. 21-33.
- Russett, B. & Oneal, J. 2001. *Triangulating Peace: Democracy, Interdependence, and International Organizations*. New York: Norton.

- Schultz, T. 2008. Carving up the Internet: Jurisdiction, Legal Orders and the Private/Public International Law Interface. *The European Journal of International Law*, 19(4):799-839.
- SCO. 2008. *AGREEMENT between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security – Unofficial Translation* [Online] Available: <https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf> [2016, October 19].
- Segal, A. 2014. The Future of Internet Governance, in *The 2014 Council of Councils Annual Conference Panelist Papers*. Washington, DC: Council of Councils.
- Singh, J. P. 2013. Information Technologies, Meta-power and Transformations in Global Politics. *International Studies Review*, 15(1):5-29.
- Sofaer, A. D. & Goodman, S. E. 2001. *The Transnational Dimension of Cybercrime and Terrorism*. Stanford: Hoover Institution Press.
- Somerville, H. 2015. *Cyber security investing grows, resilient to market turmoil* [Online]. Available: <http://www.reuters.com/article/cybersecurity-funding-idUSL1N11O2VH20150922> [2016, July 12].
- The Economist. 2013. *What is the difference between Sunni and Shia Muslims?* [Online]. Available: <http://www.economist.com/blogs/economist-explains/2013/05/economist-explains-19> [2016, October 16].
- The Economist. 2016. *We the Networks* [Online]. Available: <http://www.economist.com/news/international/21693922-organisation-runs-internet-address-book-about-declare-independence-we> [2016, September 23].
- The White House – Office of the Press Secretary. 2016. *FACT SHEET: Cybersecurity National Action Plan* [Online]. Available: <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan> [2016, September 26]
- Tickner, J. A. 1992. *Gender in International Relations: Feminist Perspectives on Achieving Global Security*. New York: Columbia University Press.
- Tinnes, J. 2015. Although the (Dis)-Believers Dislike it: a Backgrounder on IS Hostage Videos – August - December 2014. *Perspectives on Terrorism*, 9(1).
- Twitter. 2016. *Using hashtags on Twitter* [Online]. Available: <https://support.twitter.com/articles/49309> [2016, October 5].
- Ullman, R. H. 1983. Redefining Security. *International Security*, 8(1):129-153.

- UN Human Rights Council Resolution on: The promotion, protection and enjoyment of human rights on the Internet*. 2012. [Online]. Available: <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement> [2014, August 25].
- UN-GGE. 2005. *A/60/202* [Online]. Available: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement> [2016, September 29].
- UN-GGE. 2010. *A/65/201* [Online]. Available: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement> [2016, September 29].
- UN-GGE. 2013. *A/68/98** [Online]. Available: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement> [2016, September 29].
- UN-GGE. 2015. *A/70/174* [Online]. Available: <https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf> [2016, September 29].
- UN. 1999. *A/RES/53/70* [Online]. Available: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 [2016, September 26].
- UN. 2001. *A/RES/55/63* [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [2016, September 26].
- UN. 2002. *A/RES/56/121* [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf [2016, September 26].
- UN. 2003. *A/RES/57/239* [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf [2016, September 26].
- UN. 2004. *A/RES/58/199* [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf [2016, September 26].
- UN. 2005. *S/RES/1624* [Online]. Available: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/52/PDF/N0551052.pdf?OpenElement> [2016, October 8].
- UN. 2006. *A/RES/60/288* [Online]. Available: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288 [2016, October 7].

- UN. 2010. *A/RES/64/211* [Online]. Available: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211 [2016, September 26].
- UN. 2014. *S/RES/2178* [Online]. Available: http://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf [2016, October 8].
- UN. 2015. *A/RES/70/237* [Online]. Available: <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf> [2016, September 26].
- UNDOC. 2012. *Use of the Internet for Terrorist Purposes*. Vienna, Vienna International Ctr.
- UNHROHC. 2015. *Human Rights Council holds panel discussion on the effects of terrorism on the enjoyment by all persons of human rights* [Online]. Available: <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16173&LangID=E> [2016, October 18].
- UNODA. 2015. *Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security* [Online]. Available: <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf> [2016, September 26].
- UNODC. 2012. *The use of the Internet for terrorist purposes*. Vienna: UN.
- US Congress. 2015. *Division N – Cybersecurity Act of 2015* [Online]. Available: <https://epic.org/privacy/cybersecurity/Cybersecurity-Act-of-2015.pdf> [2016, September 30].
- US Department of the Treasury. 2014. *Treasury Designates Three Key Supporters of Terrorists in Syria and Iraq* [Online]. Available: <https://www.treasury.gov/press-center/press-releases/Pages/jl2605.aspx> [2016, October 5].
- US DoD. 2015. *The DoD Cyber Strategy* [Online]. Available: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [2016, September 30].
- Van Evera, S. 1999. *Causes of War: Structures of Power and the Roots of International Conflict*. New York: Cornell University Press.
- van Ginkel, B. 2015. *Responding to Cyber Jihad: Towards an Effective Counter Narrative*. Research Paper. Netherlands: International Centre for Counter-Terrorism – The Hague (ICCT).

- Vidino, L. & Hughes, S. 2015. *ISIS in America – From Retweets to Raqqa*. Washington, DC: The George Washington University – Program on Extremism.
- Villeneuve, N. 2007. Evasion tactics: global online censorship is growing, but so are the means to challenge it and protect privacy. *Index on Censorship*, 4:71–85.
- von Behr, I., Reding, A., Edwards, C., Gibbon, L. 2013. *Radicalisation in the digital era – The use of the Internet in 15 cases of terrorism and extremism*. Brussels: RAND Europe.
- Wæver, O. 1995. “Securitization and Desecuritization”, in Lipschutz, R. (ed.). *On Security*. New York: Columbia University Press. 46-86.
- Walt, S. M. 1991. The Renaissance of Security Studies. *International Studies Quarterly*, 35(2):211-239.
- Waltz, K. N. 1979. *Theory of International Politics*. Reading, Massachusetts: Addison-Wesley.
- Warrick, J. & Mekhennet, S. 2016. *Inside ISIS: Quietly preparing for the loss of the ‘caliphate’* [Online]. Available: https://www.washingtonpost.com/world/national-security/inside-isis-quietly-preparing-for-the-loss-of-the-caliphate/2016/07/12/9a1a8a02-454b-11e6-8856-f26de2537a9d_story.html [2016, October 13].
- Waters, G. Ball, D. & Dudgeon, I. 2008. *Australia and Cyber-Warfare*. Australia: ANU E Press.
- Weimann, G. 2004a. *Cyberterrorism: How Real Is the Threat?*. Special Report 119. Washington, DC: United States Institute of Peace.
- Weimann, G. 2004b. *How Modern Terrorism Uses the Internet*. Special Report 116. Washington, DC: United States Institute of Peace.
- Westby, J. R. 2004. *International Guide to Cyber Security*. Chicago, IL: American Bar Association.
- WGIG. 2005. *Report of the working group on Internet governance* [Online]. Available: <http://www.wgig.org/docs/WGIGREPORT.pdf> [2014, August 24].
- Williams, M. C. 2003. Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly*, 47(4):511-531.
- Wohlforth, W. C. 2010. “Realism and security studies”, in Cavelti, M. D. & Mauer, V. (eds.). *The Routledge Handbook of Security Studies*. Oxon: Routledge. 9-20.
- Wolfers, A. 1952. “National Security” as an Ambiguous Symbol. *Political Science Quarterly*, 67(4):481-502.

Yourish, K., Watkins, D., Giratikanon, T. & Lee, J. C. 2016. *How Many People Have Been Killed By ISIS Attacks Around the World* [Online]. Available: http://www.nytimes.com/interactive/2016/03/25/world/map-isis-attacks-around-the-world.html?_r=0 [2016, July 15].

Zittrain, J. 2008. *The Future of the Internet: And How to Stop It*. London: Penguin Books.