

# **Information warfare as future South African national security threat**

**Rianne van Vuuren**

Dissertation presented for the degree of  
Doctor of Philosophy (PhD) in Futures Studies  
at Stellenbosch University



**Supervisor: Professor A. Roux**

**December 2016**

## **Declaration**

Hereby I, Rianne van Vuuren, declare that this study project is my own original work and that all sources have been accurately reported and acknowledged, and that this document has not previously in its entirety or in part been submitted at any university in order to obtain an academic qualification.

R van Vuuren

December 2016

## Acknowledgements

“The paths to the future are made, not found, and the process of making them changes both us and our final destination.”

Anonymous CEO (Heidrick & Struggles, 2015:5).

The truth of this quote is confirmed by my pathway to scenarios indicating the plausible manifestation of information warfare in the 2030s. My introduction to future studies took place in 1988 when I attended an introductory course presented by Prof Hentie Boshoff from Potchefstroom University. This was during dark times in South Africa’s history when most domestic security analysts predicted a serious escalation of violence in the country as well as a continued long-term political and military stalemate with no hope of polarised forces ever reaching a political compromise.

The output of a Delphi study came as a real surprise to our syndicate group. A future scenario, describing a South Africa where a negotiated, equitable, charterist but free-market orientated political settlement is reached was identified as the most probable scenario. This was during a time even before rumours of negotiations between the government and the African National Congress (ANC) became known. The subsequent development of South Africa’s history vindicated the finding of that exercise, a fact that made a deep impression on me regarding the value of future studies methodologies.

Subsequently, academic interest steered me to strategic security issues and specifically South Africa’s nuclear weapon related decisions which highlighted the issue of how security decisions impact on the future. In the South African case incremental decision-making resulted in the primary decision-maker in South Africa owning the “Sword of Armageddon” without any clear reason or utility for this capacity. This increased my interest in the future of security decision making.

Since the early 1990s the new possibilities for conflict represented by technological developments and especially the digital revolution interested me intensely. After some discussions with local and international experts, I came to the conclusion that pursuing this interest in a structured way would be best served by conducting a PhD study using the theoretical and methodological foundations of international relations, business studies and futures studies.

I acknowledge Professor André Roux and Dr Jan Naude for their support and encouragement during my work on this thesis. Finally, without the consistent support of Lizelle, Renaldo and Estefan this thesis could not have been completed.

May the people of South Africa continue to fearlessly resist the forces of polarisation.

## Abstract

The objective of this study was to use the emerging discipline of futures studies through the application of social science methodologies to generate foresight about the plausible manifestation of information warfare in the 2030s as an upcoming national security threat. Interdisciplinary theories from futures studies and international relations in conjunction with methodologies from business and futures studies (environmental scanning, causal layered analysis, a Delphi study and a scenario exercise) were used.

Information warfare is an emerging threat which is on its way to develop into a significant global challenge. The definition proposed for information warfare encompasses three manifestations, namely netwar, psychological operations and cyber warfare. The differentiation between the three manifestations is elucidated by a cognitive-technology continuum. Critical realism, which regards all knowledge as conjectural, served as basis for the philosophical approach in this study. According to critical realism there are both an external world independent of human consciousness and, at the same time, a dimension that includes humanity's socially determined knowledge about reality. Transformation, networking and the impact of technological innovation in all the environments investigated were highlighted as central to the manifestation of information warfare in the present as well as in the future. These drivers influenced not only the entities involved in power relations in society, but also enhanced the potential influence and power of small and marginalised entities in society. New forms of network-related actions were identified as of particular use for information warfare in the future. A model to address information warfare as an upcoming national security threat was developed.

The two most significant driving forces were an increase in integration and polarisation that will contribute to systemic stresses, and information communication technology (ICT) embedding itself as a crucial part of society. This resulted in four plausible scenarios. The "Shango Rejuvenated" scenario foresees rapid technological advances, boosted by high levels of social integration stimulated by swift advancement in communication technologies. Information warfare is a preferred tool for power projection and consolidation but takes place in the context of relatively advanced cognitive and technological capacities. The "Gaunab Rising" scenario anticipates low levels of social cohesion combined with high levels of technological participation resulting in a potentially volatile society providing opportunities for authoritarian elites to expand control. Information warfare remains rife and is expanding on all societal levels. The "Inkanyamba Reduced" scenario foresees that the combination of low social cohesion and low levels of technological participation will magnify dissent, resulting in high levels of conflict and competition for resources. The technological part of information warfare in the form of cyberwar is limited, but the cognitive aspects in the form of netwar and psychological operations remain high. In the "Tsunigoab Revived" scenario high levels of social integration with low levels of technological participation ensure relative stability but also limit the potential value that technology could add to society. The

intensity of information warfare is lower but information warfare continues to be an instrument for power enhancement in society. Polarisation poses a significant future risk in terms of leveraging information warfare as a national security threat.

Key words: Causal Layered Analysis, Cyber warfare, Delphi Study, Environmental Scanning, Futures Model, Futures Studies, Information Warfare, Netwar, Psychological Operations, Scenario Study, 2030

## Table of contents

<b>Declaration</b>	<b>ii</b>
<b>Acknowledgements</b>	<b>iii</b>
<b>Abstract</b>	<b>iv</b>
<b>List of tables</b>	<b>xiii</b>
<b>List of figures</b>	<b>xvi</b>
<b>List of acronyms and abbreviations</b>	<b>xvii</b>
<b>CHAPTER 1: INTRODUCTION</b>	
1.1 GENERAL INTRODUCTION	1
1.2 INFORMATION AS GLOBAL INSTRUMENT FOR POWER	1
1.3 RESEARCH FOCUS	3
1.3.1 Problem statement	3
1.3.2 Aim of the study	4
1.3.3 Thesis statement	4
1.4 PHILOSOPHICAL APPROACH	4
1.5 RESEARCH METHODOLOGY	9
1.5.1 Qualitative text analysis	10
1.5.2 Methodology outline	11
1.5.3 Phase 1: Definition of concepts	12
1.5.4 Phase 2: Environmental scanning	13
1.5.5 Phase 3: Development of a futures model inclusive of CLA	14
1.5.6 Phase 4: Delphi study	16
1.5.7 Phase 5: Scenario analysis	17
1.5.8 Phase 6: Formulate propositions	17
1.6 LITERATURE SURVEY	17
1.6.1 Theoretical literature	18
1.6.2 Information warfare and national security literature	19
1.6.3 Methodological literature	20
1.7 ETHICAL REQUIREMENTS	21
1.8 STRUCTURE OF THE STUDY	22

**CHAPTER 2: INFORMATION AS STRATEGIC POWER INSTRUMENT: THEORETICAL APPROACH**

2.1	INTRODUCTION	25
2.2	CRITICAL REALISM AS OVERARCHING THEORY	26
2.3	INTERNATIONAL RELATIONS THEORY	29
2.3.1	The realist tradition	32
2.3.1.1	The central role of power	32
2.3.1.2	Stability through the balance of power	33
2.3.1.3	Balance of power in the Information Age	34
2.3.1.4	Criticism of realism	35
2.3.1.5	Prospects for the realism worldview in the future	36
2.3.2	The rationalist tradition	37
2.3.2.1	The central role of international cooperation	37
2.3.2.2	The role of rules, international organisations and international law	39
2.3.2.3	Criticism of rationalism	40
2.3.2.4	Critical realism in international relations theory	41
2.3.2.5	Critical security studies	43
2.3.3	Postmodernism in international relations	44
2.3.3.1	The information society in international relations	43
2.3.3.2	Criticism of postmodernism	45
2.3.3.3	Retention in the Information Age	46
2.3.3.4	The rise of signs, symbols and simulacra	46
2.3.3.5	International relations theory and information warfare	47
2.4	CONCLUSION	48

**CHAPTER 3: FUTURES STUDIES AS AN INSTRUMENT FOR FORESIGHT**

3.1	INTRODUCTION	50
3.2	TIME PERCEPTION CHALLENGES TO FUTURES STUDIES	51
3.3	THE RATIONALE FOR FUTURES STUDIES AND THE ROLE OF THE FUTURIST	52
3.4	FORESIGHT AS AN OUTCOME OF FUTURES STUDIES	54
3.5	SYSTEMS APPROACH	56
3.5.1	Futures maps	60
3.5.2	Layered systems approaches as analysis tools	61
3.5.3	Causal layered analysis	62
3.6	CONCLUSION	65

**CHAPTER 4: DEFINING INFORMATION WARFARE AND NATIONAL SECURITY**

4.1	INTRODUCTION	67
4.2	DEFINING DATA, INFORMATION, INTELLIGENCE, KNOWLEDGE AND WARFARE	68

4.3	HISTORIC OVERVIEW OF INFORMATION AND NATIONAL WILL IN A NATIONAL SECURITY CONTEXT	70
4.4	DEFINING INFORMATION WARFARE	72
4.4.1	Challenges in finding a definition	72
4.4.2	Broad definitions	73
4.4.3	Definitions limited to the ICT component	75
4.4.4	Military definitions	75
4.4.5	Synopsis of information warfare definitions	76
4.4.6	The relationship between information warfare and power	76
4.4.7	Definition of information warfare	77
4.4.8	Netwar, psychological operations and cyber warfare defined	79
4.5	THE FUNDAMENTALS OF INFORMATION WARFARE	81
4.6	DEFINING NATIONAL SECURITY	82
4.6.1	Context for finding a definition for national security	82
4.6.2	Definition of national security	86
4.7	CONCLUSION	86

## **CHAPTER 5: ENVIRONMENTAL ANALYSIS OF INFORMATION WARFARE AS A NATIONAL SECURITY THREAT**

5.1	INTRODUCTION	88
5.2	ENVIRONMENTAL SCANNING CONCEPTUALISED	89
5.3	ENVIRONMENTAL SCANNING IN THE INFORMATION AGE	92
5.3.1	Technological environment	93
5.3.2	War / conflict environment	99
5.3.3	Political environment	104
5.3.4	Social environment	107
5.3.5	Economic environment	108
5.3.6	The enhancement of the power of networks, innovation and transformation	111
5.4	INFORMATION WARFARE TARGETS	113
5.5	THE MANIFESTATION OF INFORMATION WAR	116
5.5.1	Overview of information warfare manifestation from 1990 to 2015	117
5.6	THE FUTURE OF INFORMATION WARFARE	124
5.7	CONCLUSION	125

## **CHAPTER 6: IDENTIFYING DRIVING FORCES FOR INFORMATION WARFARE FUTURES**

6.1	INTRODUCTION	127
6.2	CODING OF THE ENVIRONMENTAL SCAN OUTPUT	128
6.3	FROM GROUNDED THEORY TO A FUTURES MODEL	135
6.3.1	The use of a model	136

6.4	AN INFORMATION WARFARE ENVIRONMENT FUTURES STUDIES MODEL	136
6.5	CLA ASSESSMENT OF THE ENVIRONMENTAL SCAN	139
6.5.1	CLA assessment of the technology environment	140
6.5.2	CLA assessment of the war/conflict environment	142
6.5.3	CLA assessment of the political environment	143
6.5.4	CLA assessment of the social environment	144
6.5.5	CLA assessment of the economic environment	145
6.6	INTEGRATION OF CLA ASSESSMENT WITH MODEL IDENTIFIED TRENDS	147
6.7	CONCLUSION	149

## **CHAPTER 7: VERIFYING AND PRIORITISING DRIVING FORCES FOR INFORMATION WARFARE FUTURES THROUGH THE DELPHI METHOD**

7.1	INTRODUCTION	151
7.2	VALIDATION AND PRIORITISATION OF DRIVING FORCES	152
7.3	BACKGROUND TO THE DELPHI METHOD	153
7.4	THE DELPHI STUDY PROCESS	154
7.5	FRAMEWORK OF THE DELPHI STUDY	155
7.5.1	Purpose of the study	156
7.5.2	Number of rounds	156
7.5.3	Participants and panel size	156
7.5.4	Choosing the participants	157
7.5.5	Mode	158
7.5.6	Anonymity	158
7.5.7	Media	158
7.5.8	Concurrency	159
7.5.9	Evaluation criteria	159
7.6	PILOT DELPHI STUDY	161
7.6.1	Aim of the pilot study	160
7.6.2	Focus of the pilot study	162
7.6.3	Participants in the pilot study	162
7.6.4	Structuring of the questionnaire	163
7.6.5	Evaluation of Delphi study pilot Round 1	165
7.6.6	Evaluation of Delphi study pilot Round 2	180
7.7	SECOND DELPHI STUDY	191
7.7.1	Aim of the Second Delphi study	191
7.7.2	Focus of the Second Delphi study	192

7.7.3	Participants in the Second Delphi study	192
7.7.4	Questionnaire	193
7.7.5	Evaluation of the second Delphi study pilot Round 1	194
7.7.6	Evaluation of the second Delphi study pilot Round 2	203
7.8	FINAL MAIN DRIVING FORCES	214
7.9	CONCLUSION	215

## **CHAPTER 8: 2030 SCENARIOS FOR INFORMATION WARFARE AS NATIONAL SECURITY THREAT**

8.1	INTRODUCTION	216
8.2	BACKGROUND TO THE DEVELOPMENT OF SCENARIOS	217
8.3	USE OF SCENARIOS IN SOUTH AFRICA	219
8.4	DEFINING SCENARIOS	220
8.5	FOUR TYPES OF FUTURES	221
8.6	APPROACHES TO SCENARIOS	222
8.7	IDENTIFYING DIFFERENT PURPOSES FOR SCENARIOS	223
8.7.1	Purpose of scenario method in this study	224
8.8	SCENARIOS AS MENTAL MODELS	224
8.9	KEY ASPECTS OF SCENARIOS	227
8.9.1	Boundary setting	227
8.9.2	Managing uncertainties	227
8.10	STRENGTHS AND WEAKNESSES OF SCENARIO METHODOLOGY	228
8.11	THE PROCESS OF DEVELOPING SCENARIOS	230
8.11.1	Establish the aim of scenario creation	231
8.11.2	Define the key concepts	231
8.11.3	Analyse and evaluate the environment	231
8.11.4	Evaluate the driving forces	231
8.11.5	Identify two key drivers	232
8.11.6	Produce a basic scenario matrix	236
8.11.7	Provide a rationale for the scenario names	238
8.11.8	Produce the scenarios	239
8.12	SCENARIO 1: "SHANGO REJUVENATED"	239
8.12.1	Information warfare and national security manifestation	239
8.12.2	Technology manifestation	241

8.12.3	Economic manifestation	241
8.12.4	Political manifestation	242
8.12.5	Social manifestation	243
8.12.6	CLA evaluation of scenario “Shango Rejuvenated”	242
8.13	SCENARIO 2: “GAUNAB RISING”	244
8.13.1	Information warfare and national security manifestation	245
8.13.2	Technology manifestation	246
8.13.3	Economic manifestation	246
8.13.4	Political manifestation	247
8.13.5	Social manifestation	248
8.13.6	CLA evaluation of scenario “Gaubab Rising”	248
8.14	SCENARIO 3: “INKANYAMBA REDUCED”	250
8.14.1	Information warfare and national security manifestation	250
8.14.2	Technology manifestation	250
8.14.3	Economic manifestation	251
8.14.4	Political manifestation	251
8.14.5	Social manifestation	252
8.14.6	CLA evaluation of scenario “Inkanyamba Reduced”	252
8.15	SCENARIO 4: “TSUNIGOAB REVIVED”	254
8.15.1	Information warfare and national security manifestation	254
8.15.2	Technology manifestation	254
8.15.3	Economic manifestation	255
8.15.4	Political manifestation	255
8.15.5	Social manifestation	255
8.15.6	CLA evaluation of scenario “Tsunigoab Revived”	256
8.16	CONCLUSION	257
<b>CHAPTER 9: EVALUATION</b>		
9.1	SUMMARY	258
9.1.1	Sub-problem outcomes	258
9.2	PROPOSITIONS	265
9.3	RESEARCH CONTRIBUTIONS	268
9.4	CONCLUSION	269
<b>LIST OF SOURCES</b>		271
<b>APPENDICES</b>		

APPENDIX A: THEMATIC QUALITATIVE TEXT CODING OF THE ENVIRONMENTAL SCAN OUTPUT	311
APPENDIX B: DELPHI ADMINISTRATION: ROUND 1 QUESTIONNAIRE	316
APPENDIX C: DELPHI ADMINISTRATION: LETTER FOR FIRST ROUND DELPHI	318
APPENDIX D: DELPHI ADMINISTRATION: ROUND 2 QUESTIONNAIRE	319
APPENDIX E: DELPHI ADMINISTRATION: LETTER FOR SECOND ROUND DELPHI	329
APPENDIX F: PILOT DELPHI STUDY: ROUND 1 RESULTS	330
APPENDIX G: PILOT DELPHI STUDY: ROUND 2 RESULTS	331
APPENDIX H: SECOND DELPHI STUDY: ROUND 1 RESULTS	332
APPENDIX I: SECOND DELPHI STUDY: ROUND 2 RESULTS	333

## List of tables

Table 2.1	Critical realism's ontological map	26
Table 4.1	Manifestation of information warfare	78
Table 5.1	Three technological revolutions	94
Table 5.2	Consequences of agents of globalisation	97
Table 5.3	Evolution of warfare	104
Table 6.1	CLA assessment of the technology environment	140
Table 6.2	CLA assessment of the war/conflict environment	142
Table 6.3	CLA assessment of the political environment	143
Table 6.4	CLA assessment of the social environment	145
Table 6.5	CLA assessment of the economic environment	146
Table 6.6	Identification and evaluation of driving forces	147
Table 7.1	The Delphi design choices	159
Table 7.2	Evaluation of Driving Force 1 (first-round pilot Delphi)	166
Table 7.3	Dimensions of the category "Shifting Power"	167
Table 7.4	Evaluation of Driving Force 2 (first-round pilot Delphi)	167
Table 7.5	Dimensions of the category "Networked Security"	169
Table 7.6	Evaluation of Driving Force 3 (first-round pilot Delphi)	169
Table 7.7	Dimensions of the category "Clashing Centripetal and Centrifugal Forces"	170
Table 7.8	Driving Force 4 (first-round pilot Delphi)	170
Table 7.9	Dimensions of the category "Alternative Power Projection Instrument"	171
Table 7.10	Driving Force 5 (first-round pilot Delphi)	171
Table 7.11	Dimensions of the category "Symbolic"	172
Table 7.12	Driving Force 6 (first-round pilot Delphi)	172
Table 7.13	Dimensions of the category "Hyper-Speed"	173
Table 7.14	Driving Force 7 (first round pilot Delphi)	173
Table 7.15	Dimensions of the category "Rise of the Non-State Actor"	174
Table 7.16	Driving Force 8 (first-round pilot Delphi)	175
Table 7.17	Dimensions of the category "Global Inequality"	176
Table 7.18	Driving Force 9 (first-round pilot Delphi)	176
Table 7.19	Dimensions of the category "Embedding of ICT"	177
Table 7.20	Driving Force 10 (first round pilot Delphi)	177
Table 7.21	Dimensions of the category "Rise of Social Media"	178
Table 7.22	Driving Force 11 (first-round pilot Delphi)	178
Table 7.23	Dimensions of the category "Threshold Low"	179
Table 7.24	Additional driving forces as suggested by the pilot Delphi panel members	179
Table 7.25	Evaluation of Driving Force 1 (second-round Delphi pilot)	181

Table 7.26	Evaluation of Driving Force 2 (second-round Delphi pilot)	182
Table 7.27	Evaluation of Driving Force 3 (second-round Delphi pilot)	183
Table 7.28	Evaluation of Driving Force 4 (second-round Delphi pilot)	184
Table 7.29	Evaluation of Driving Force 5 (second-round Delphi pilot)	185
Table 7.30	Evaluation of Driving Force 6 (second-round Delphi pilot)	186
Table 7.31	Evaluation of Driving Force 7 (second-round Delphi pilot)	187
Table 7.32	Evaluation of Driving Force 8 (second-round Delphi pilot)	188
Table 7.33	Evaluation of Driving Force 9 (second-round Delphi pilot)	187
Table 7.34	Evaluation of Driving Force 10 (second-round Delphi pilot)	188
Table 7.35	Evaluation of Driving Force 11 (second-round Delphi pilot)	189
Table 7.36	Additional comments by the pilot Delphi panel members for Round 2	190
Table 7.37	List of participants in the second Delphi study	192
Table 7.38	Evaluation of Driving Force 1 (first-round Second Delphi)	194
Table 7.39	Evaluation of Driving Force 2 (first-round second Delphi)	195
Table 7.40	Evaluation of Driving Force 3 (first-round second Delphi)	195
Table 7.41	Evaluation of Driving Force 4 (first-round second Delphi)	196
Table 7.42	Evaluation of Driving Force 5 (first-round second Delphi)	197
Table 7.43	Evaluation of Driving Force 6 (first-round second Delphi)	198
Table 7.44	Evaluation of Driving Force 7 (first-round second Delphi)	199
Table 7.45	Evaluation of Driving Force 8 (first-round second Delphi)	199
Table 7.46	Evaluation of Driving Force 9 (first-round second Delphi)	200
Table 7.47	Evaluation of Driving Force 10 (first-round second Delphi)	201
Table 7.48	Additional driving forces as suggested by the Delphi panel members	202
Table 7.49	Evaluation of Driving Force 1 (second-round second Delphi)	203
Table 7.50	Evaluation of Driving Force 2 (second-round second Delphi)	205
Table 7.51	Evaluation of Driving Force 3 (second-round second Delphi)	206
Table 7.52	Evaluation of Driving Force 4 (second-round second Delphi)	207
Table 7.53	Evaluation of Driving Force 5 (second-round second Delphi)	208
Table 7.54	Evaluation of Driving Force 6 (second-round second Delphi)	209
Table 7.55	Evaluation of Driving Force 7 (second-round second Delphi)	209
Table 7.56	Evaluation of Driving Force 8 (second-round second Delphi)	210
Table 7.57	Evaluation of Driving Force 9 (second-round second Delphi)	211
Table 7.58	Evaluation of Driving Force 10 (second-round second Delphi)	212
Table 7.59	Additional comments by the second Delphi panel members for Round 2	213
Table 7.60	Final driving forces	214
Table 8.1	Influence matrix for driving forces	233
Table 8.2	Legend and outcome of the influence matrix for driving forces	233
Table 8.3	Legend and outcome of the impact/uncertainty matrix for driving forces	235

Table 8.4	Final two driving forces for information warfare scenarios	236
Table 8.5	CLA assessment of the scenario “Shango Rejuvenated”	243
Table 8.6	CLA assessment of the scenario “Gaunab Rising”	248
Table 8.7	CLA assessment of the scenario “Inkanyamba Reduced”	252
Table 8.8	CLA assessment of the scenario “Tsunigoab Revived”	256

## List of figures

Figure 1.1	Thematic qualitative text analysis process	11
Figure 1.2	Visualisation of the research outline	22
Figure 2.1	International relations framework influencing information warfare	47
Figure 3.1	A simplified model of a system in the context of a society	58
Figure 3.2	Futures map	61
Figure 3.3	Layered systems explanation of reality	62
Figure 3.4	Causal layered analysis (CLA)	63
Figure 4.1	Data, knowledge, information and intelligence continuum	68
Figure 4.2	Von Clausewitz's national security trinity and national will	71
Figure 4.3	Components of information warfare	79
Figure 5.1	The TWEPS macro-environmental hexagon	90
Figure 5.2	The RMA system-of-system argument	102
Figure 5.3	Rhizome network	112
Figure 5.4	The pillars of an information society	113
Figure 5.5	Warden's five targeting rings	115
Figure 6.1	Qualitative text analysis of the three environmental categories	131
Figure 6.2	Subcategories for Innovation, Networks and Transformation	131
Figure 6.3	Future studies model applicable to information warfare futures	137
Figure 6.4	Trend planning horizon roadmap	138
Figure 6.5	Driving forces for information warfare futures	149
Figure 8.1	Different purposes and different focuses for scenarios	223
Figure 8.2	Scenario matrix	225
Figure 8.3	Illustrative impact/uncertainty matrix	235
Figure 8.4	Information warfare 2030s scenario matrix	237

## List of acronyms and abbreviations

4GW	Fourth-generation warfare
ADB	Asian Development Bank
AI	Artificial Intelligence
AIB	Asian Infrastructure Investment Bank
ASIO	Australian Security Intelligence Organisation
AYM	Alliance of Youth Movements
ANC	African National Congress
AU	African Union
BSI	Germany's Federal Office for Information Security
C2W	Command-and-Control Warfare
CAT	Coding Analysis Toolkit
COG	Centre of Gravity
CENTCOM	United States of America's Military Central Command
CIA	Central Intelligence Agency
CLA	Causal Layered Analysis
COG	Centre of Gravity
DDOS	Distributed Denial of Service
EZLN	<i>Ejército Zapatista de Liberación Nacional</i>
EW	Electronic Warfare
IBW	Intelligence-Based Warfare
ICT	Information communication technology
IDF	Israeli Defence Forces
IEW	Information Economic Warfare
IFOR	Implementation Force
IFR	Institute for Futures Research
IO	Information Operations
IoT	Internet of Things
IS	Islamic State
IT	Information technology
ITU	International Telecommunications Union
IMF	International Monetary Fund
IW	Information warfare
IQR	Interquartile range
LDCs	Least Developed Countries
NATO	North Atlantic Treaty Organisation
NDP	National Development Plan

NIS	National Intelligence Service
NGO	Non-Governmental Organisation
OODA	Observe – Orient – Decide – Act
PGM	Precision-guided munitions
PSYOPS	Psychological Operations
QDAP	Qualitative Data Analysis Program
RAND	Research and Development (Corporation)
REC	Regional Economic Community
RMA	Revolution in Military Affairs
S <sup>3</sup>	Speed, Scope and Significance
SSC	State Security Council
STEEP	Social, Technological, Economic, Environmental and Political (sectors)
SU	Stellenbosch University
USAID	United States Agency for International Development
USB	University of Stellenbosch Business School
USB-DESC	Departmental Ethics Screening Committee of the University of Stellenbosch Business School
USA	United States of America
TPP	Trans-Pacific Partnership
TWEPS	Technological, War/Conflict, Economic, Political and Social (macro-environmental hexagon)
WEF	World Economic Forum
WFS	World Future Society
WMD	Weapons of Mass Destruction
WTO	World Trade Organization
WWW	World Wide Web

## CHAPTER 1

### INTRODUCTION

#### 1.1 GENERAL INTRODUCTION

The Information Age is bringing to the fore a new generation of national security threats and challenges, intermingled with the threats of the past. The most significant security-related events during the Industrial Age was the atomic devastation of Hiroshima and Nagasaki. Since then efforts to manage and control the overwhelming power of nuclear weapons have been at least successful in preventing the use of these weapons again in a conflict situation.

Since the Information Age is only in its infancy, the question remains as to what would be the upcoming national security threats that governments will face in the future. Successful management of these threats builds upon the capability of government leaders to adjust to a fast-changing global security environment.

While security threats associated with the earlier agricultural and Industrial Ages remain relevant, the identification of emerging threats to national security in the Information Age remains a challenge. Unfortunately, the lead time that decision makers once benefited from to analyse and respond to these challenges is diminishing. Conventional long-range planning models, with their reliance on historical data and inward focus, do not empower decision makers to foresee changes to the environment and assess their impact on national security (Teece, 2010:174). In this regard the study of a phenomenon currently referred to as “information warfare” does hold some promise, especially if the exponential global growth of networking, boosted by rapidly developing information communication technology (ICT) and rapid societal transformation, is taken into account.

#### 1.2 INFORMATION AS GLOBAL INSTRUMENT FOR POWER

Generally, the term information warfare is still associated with high-technology weapons and broadcast images of drones destroying military targets with apparently assured accuracy and computer hackers taking down a country’s power grid by gaining control of the power supplier’s mainframe computer. Unfortunately, this armchair view of the sometimes confusing capabilities made possible by high technology and information technology has created a simplistic and sanitised vision of information warfare in which, to paraphrase Toffler (1990), the mindless fist is replaced by the congealed mind. The media’s early focus on guided missiles and intelligent warfare systems, the tangible element of the so-called digital battle space, masked the potentially deeper societal implications of virtual warfare strategies and global power projection (Cronin & Crawford, 1999:257). Of specific interest for further study is the additional intangible role that information and communication play in terms of success in this new unfolding conflict environment.

It is suspected that this aspect might become a major determinant of potential future political and economic supremacy.

Information is increasingly linked to power. How a government uses that power progressively controls how effectively a country may be influencing world politics and national security. In the past, the elements of power included mainly military, economic and diplomatic factors. However, in the 21st century, information is rapidly assuming a key position in foreign and security policy. It can potentially fulfil many roles, such as being a force multiplier, a tool for influencing decision-making and/or an instrument for manipulation. Information has evolved into a significant power projection instrument for the state. However, as much as it presents an offensive power projection capability to the state, it also poses a potential momentous threat to the state (Armistead, 2004:231).

The constantly changing national security environment is linked to the shifting basis of state power. As the foundation of global civilisation evolved from agriculture to industry and then to the information sector, the power structures within states also changed. At its core, the transformation to an information-based society represents a shift from manufacturing to knowledge, where the creation, application and dissemination of knowledge, rather than the production of manufactured goods or agricultural products, is becoming the central defining activity of modern society and governance (Mazarr, 1997:25). This shift has a direct impact on how national security is being viewed by some governments. At the same time, there has been an increase in the number of countries studying innovative ways to endeavour to gain an advantage by changing the way in which conflict is managed and power is projected. The information society brings new and revolutionary technologies and means, which demand change in the way state security is managed (Lin, 2000). This has a broad impact on modern society, changing risk and threat analysis in most human endeavours.

Regardless of shifting global power structures, a coherent national security strategy is an important instrument for any state. All states, even those with limited resources, have a broad range of tools at their disposal to advance their interests. These tools, whether diplomatic, economic, informational or military, provide the means by which they seek to achieve their security objectives. A national security strategy provides a rational framework for specifying interests in a comprehensive and methodological way (Africa Centre for Strategic Studies, 2005:1). While many governments have developed strategic security frameworks as national security strategies, this remains largely limited to the developed world countries. Even in the case of countries addressing information-related threats the focus remains largely limited to cyber security. However, the threat from the information environment is broader than the cyber dimension. The pervasiveness of information in modern society makes it a key factor in the construction of a global information society (Chadwick, 2006:209).

Already in the 1990s the potential threat posed by information warfare was identified as a significant national security threat in the future (Waltz, 1998:13). A significant question to be asked is whether the information dimensions, especially in terms of their comprehensive implication for national security, are adequately addressed by a regional power such as South Africa. While a significant amount of work has been done on efforts to define information warfare and related concepts, this is taking place mainly in the developed world. In general, information warfare has not been regarded in a comprehensive manner as a significant part of the national security threat perception in the developing world. Larger developing countries such as China and India are exceptions. This leads to the problem statement for this study.

### **1.3 RESEARCH FOCUS**

#### **1.3.1 Problem statement**

What plausible scenarios can be identified that focus on the manifestation of information warfare as a national security threat confronting South Africa during the 2030s? A multi-disciplinary approach, supported by futurist methodologies, has the capacity to create knowledge provide insight regarding this problem statement. Plausible scenarios on how information warfare will manifest as a national security threat in South Africa during the 2030s are identified. Deriving from the results of this study, propositions are also identified that are applicable to the probable information warfare threat against South Africa in the 2030s.

In this study, the 2030s are set as the timeframe for the development of scenarios because of various reasons. As this study was conducted during the period from 2008 to 2015, the 2030s provides a time horizon of minimum 15 years, which is short enough to fit comfortably in the lifespan of individuals involved and interested in the question of how information warfare might influence society, but long enough to feel confident that significant changes in this regard could occur over this time period. At the same time, South Africa's National Development Plan (NDP) 2030, drafted in August 2012 by the National Planning Commission, contains a series of proposals to eliminate poverty and reduce inequality by 2030. A wide range of challenges have been identified which would hinder the achievement of sustainable development in South Africa. Although information warfare is not specifically identified as a challenge, the external drivers identified, namely international and domestic political developments, globalisation, Africa's development and technology change, all are closely interrelated with the expected rise of information warfare as a significant national security threat (National Planning Commission, 2011:7-9). Molitor (1977:5) stated that anticipating specific public-policy relevant developments looking ten years ahead is possible with a very high degree of accuracy. However, the aim of the study is not predicting the future.

### **1.3.2 Aim of the study**

This study is not aimed at proving a hypothesis. In this study an emerging discipline (futures studies) is used through the application of social science methodologies to generate knowledge and foresight about a major future concern. Interdisciplinary theory from futures studies and especially international relations in conjunction with methodologies from mainly the domains of business studies and future studies (environmental scanning, causal layered analysis, Delphi study and a scenario exercise) are used to develop plausible futures regarding the potential threat information warfare will pose to South Africa by the 2030s. Specific propositions are identified applicable to the decision makers in government who will by the 2030s be confronted by both international and domestic information warfare – related national security threats. Propositions relevant to creating a preferable future scenario in terms of information warfare as a national security threat are also identified.

It is not endeavoured to lay claim to an exact conclusion or statement of truth in this study. Rather the study is positioned to deliver on what it was designed to achieve, namely an exploratory study. The research topic is fluid and difficult to contain within a national or organisational context, as it is a globally dispersed and layered problem. The security threats are therefore multi-layered, emerging in disruptive ways and not limited to traditional national security paradigms.

Consequently these futures are developed based on an analysis of a definition of information warfare and relevant concepts, the identification of a broad theoretical framework, and an environmental analysis of dynamics creating change and impacting on the concepts information warfare and national security. Central to the study is an analysis of the changing nature of power in the Information Age and its changing role in terms of national security in the future.

### **1.3.3 Thesis statement**

The thesis statement was formulated as follows:

The South African government will by the 2030s need to make significant adjustments to its national security threat assessment and national security policy management to effectively cope with the challenges that information warfare will pose to national security at that stage.

## **1.4 PHILOSOPHICAL APPROACH**

This study use critical realism as epistemological approach, which is implemented through a qualitative research design. The philosophical approach for this study was sourced from different social science fields, mainly from futures studies and international relations theory, but also from other relevant social sciences such as sociology and political science.

Scientific observations and theories are always concept-dependent but not concept-determined. Science should be regarded as a practical social activity, which is carried out under similar conditions to other forms of social practice. This means that questions on method are primarily practical questions, which must always be considered in relation to the character of the object of investigation and the purpose of the investigation (Danermark, Ekström, Jakobsen & Karlsson, 2005:39). Thus scientists blend approaches in different ways and to differing degrees for different problems. In addition, nearly all scientific approaches have something positive to offer, as long as their application is not carried to an extreme (Jaccard & Jacoby, 2010:259).

Critical realism forms the foundation of assumptions about the nature of reality and knowledge, and provides:

- The philosophical assumptions about what constitutes social reality (*ontology*);
- A description of what is accepted as valid evidence of that reality (*epistemology*);
- The means by which that context is investigated (*methodology*); and
- The means by which evidence is gathered (*methods*).

According to critical realism the central problem of science is that knowledge of reality is always filtered through language and concepts that are relative and changeable in time and space. This has resulted in doubts about any possibilities of acquiring valid knowledge of reality, and sometimes even doubts about the objective existence of reality. However, in opposition to cognitive relativist and idealist positions, critical realism postulates that there is a reality independent of our knowledge of it, and that science, like all other practices, offers an opportunity to obtain more or less truthful knowledge of this reality. At the same time, contrary to “naive objectivism” and empiricism, it is also stated that reality cannot be studied by neutral empirical observations alone (Danermark, Ekström, Jakobsen & Karlsson, 2005:39).

Any possibility of “objectivity” in social science is refuted by critical realism (Whitham, 2014:12). Bhaskar (2008:46-49) identified reality as consisting of three domains: firstly, our experiences of events in the world; secondly, the events as such (of which we only experience a fraction); and, thirdly, the deep dimension where one finds the generative mechanisms producing the events in the world. Further, it is the business of science to establish the connections between these three domains. Thus critical realists accept the sceptical belief that humanity cannot have certain knowledge, if we define knowledge as justified true belief. However, neither can humanity abandon efforts to know and understand. Knowledge is redefined as “conjectural knowledge”, allowing for the possibility of the fallibility of their conjectures (Bell, 2007:210).

Critical realism provides insight regarding the shift of emphasis from experience and events to mechanisms. To obtain such knowledge about underlying causal mechanisms influencing the role of information and information warfare on the global terrain, it is necessary to provide an overview

of specific international relations and related theories. However, the capacity of existing international relations theory to adequately explain future security related issues and conflicts remains limited, necessitating gleaning insights from associated theoretical sources. This is in particular the case because of the growing significance of the information revolution and the impact of globalisation on community, enterprise, national and international security (Burchill & Linklater, 2005:23).

Combining different theories may lead to epistemological difficulties, but critical realism attempts to provide a framework within which a synthesis of more than one position is possible (Smith, 2013:12). Niiniluoto (2002:21) stated that critical realism turns out to be compatible with a surprising variety of philosophical positions. Although the theories used in this study come from different but related fields, at the end an integrated approach to the problems of information warfare as a current and future national security threat remains the central aim. The meta-theoretical framework in this study is provided by critical realism. The meta-theoretical framework provides space for the investigation of broader philosophical approaches from which useful theoretical insights can be obtained.

Wight (1991) identified the main international political traditions as the realist, rationalist and revolutionist traditions. Each of these traditions embodies a wide variety of doctrines about international relations, among which there sometimes exists only a loose connection. These traditions, however, incorporate a set of distinctive questions and assumptions about the basic units and forces in international relations (Keohane, 1989:2). The first condition is that no political superior is acknowledged and a multiplicity of independent sovereign states accepts the use of military force and warfare ultimately as a method to regulate relationships. This is the basis of the realist worldview regarding international relations. The second condition identified is that diplomacy and commerce form the basis of international and institutionalised interaction between sovereign states. Rationalists tend to emphasise and concentrate on the element of international interaction, which focuses on the role of measures to create and enhance order in the anarchic world as well as investigate the concept of an international society. Thirdly, the concept of a society of states, or family of nations, brings with it certain moral and psychological as well as possibly even legal obligations. Revolutionists tend to concentrate on the concept of a society of states or an international society but they can be defined more precisely as those who believe passionately in the moral unity of a society of states.

The challenges posed by the Information Age have produced some theoretical shortcomings to adequately address the growth of information as an instrument of power. The changing nature of national security and the role of information in this context highlight shortcomings related to the advancement of the role of information in the modern world, which transcends the boundaries of realist, rationalist and revolutionist worldviews. Theoretical work done in terms of critical realism

within international relations theory and theory focusing on the power of symbolism done by Baudrillard (1983) is of value in this regard.

In addition to the understanding gained from international relations theory, the theoretical insights obtained from the emerging discipline of futures studies provide assistance for judgements in terms of the assumptions and methodology followed in this study. Bell (2005:73) defined the main purposes of futures studies as “to discover or invent, examine and evaluate, and propose possible, probable and preferable futures”. Futures thinking is thus based on three interrelated inquiries into the future with the objective to determine the truth about the future (Spies, 2015). These inquiries are: (1) measuring the future to obtain knowledge about the future; (2) imagining the non-existing future; and (3) purposefully designing or making the future. Measuring, imagining and making sustainable alternative futures should be the preferable outcome of holistic futures thinking and requires active interventions to realise. This study is primarily focused on the measuring and imagining dimensions.

Since time immemorial, thinking about the future has been an ingrained part of human civilisation. As humanity desires some insight into the future it consequently endeavours to form adequate “images of future realities (futura)” (De Jouvenel, 1967:40). Futures studies is multi-disciplinary in its research approach and trans-disciplinary in its intellectual tradition with efforts since the late 1990s to have a knowledge base defined (Inayatullah & Wildman, 1996:725). Despite its historical roots, futures studies remains a relatively recent academic discipline and intellectual tool.

The future is not specified or prearranged. A multitude of futures remains possible, but only one can manifest in the end. Futures studies promotes inquiry into how current activities (or lack thereof) will become the reality of the future. This includes endeavours to analyse the causes, sources and patterns of stability and change with the intention of creating foresight and even different futures. Despite technological progress being an integral part of our society today, civilisation is seemingly racing itself into a “pathologically short attention span”, according to one author, a trend which, he claims, is “... boosted by the acceleration of technology, the short horizon perspective of market driven economics, the next election perspective of democracies, and the distractions of personal multitasking” (Brand, 1999:2).

Futures studies takes the longer view. It is largely focused on understanding social realities or “constructs” which build the future. For futures studies the development of sustainable future-oriented visions which can motivate individuals and bodies is also essential (Slaughter, 1999:305). Futures studies thus provides the means to investigate the practical attainment of more preferred futures. Social reality in all its complexity can be described as consisting of structures (how things are interconnected), processes (how things are being done), ordering (how things are kept together), context (influence of the environment) and outcomes (why things are done) (Gharajedaghi, 2006:29).

In general, a futures-orientated philosophical approach also subscribes to the worldview of critical realism in which it concurs with the notion that the absolute truth of knowledge is untenable. When focusing on science it includes a concern about the logical structure and coherence of statements, and also a special concern about the utility in manipulating the world to achieve human goals, as, for example, in the conscious process of using known cause-and-effect relationships to create desired ends (Bell, 2007:207).

Science rests on the supposition that although many aspects of reality may always remain beyond the human facility to discern and understand, how the world really is, plays a decisive role in the achievements of science. Truth can be known within the limits of human senses and intellect. Even though truth "... is not absolute and is fallible, conjectural, conditional, corrigible, tentative, qualitatively judgemental, and presuppositional; warranted assertability is possible; some assertions are true and some are false, and we can frequently justify our beliefs, empirically or logically, about which is which" (Bell, 2007:207-208). Another crucial futurist relevant theoretical perspective includes the use of systems approaches to analyse the varied relationships of the many aspects of the social world, thus operating against piecemeal analyses of the social world. The systems approach tends to regard all aspects of socio-cultural systems in process terms, especially as networks of information and communication (Ritzer & Goodman, 2004:314-315). The horizontal dimension of systems, especially the layered view of systems, proves to be constructive in enhancing understanding.

Our knowledge of the future is notoriously meagre compared with our knowledge of the past (Swinburne, 1966:166). Concepts like prediction, forecasting and foresight are generally used to refer to knowledge of the future. It remains important to distinguish between these concepts in order to understand the boundaries and limitations of futures studies.

The nature of society as an open system makes it impossible to make predictions as can be done in natural science. But, based on an analysis of causal mechanisms, it is possible to make well-informed arguments about the potential consequences of mechanisms working in different settings (Danermark, Ekström, Jakobsen & Karlsson, 2005:2). The aim of forecasting is based on the implicit desire to make the world more stable and to influence or even control the future. The assumption behind forecasting is that with more information, particularly more timely information, decision-makers can make wiser decisions. Having more information at hand is especially important presently since the rate of technological change has significantly increased (Inayatullah, 2005b).

The term foresight, which takes forecasting further, is the capacity to think ahead and consider, model, create, and respond to future eventualities. Foresight is the process of developing a range of views on possible ways the future could develop, and understanding these sufficiently well to be

able to decide what decisions can be taken today in order to create the best possible tomorrow (Horton, 1999:6).

Slaughter (1995:1) stressed that foresight is not the ability to predict the future; instead, it is a human attribute that allows humankind to weigh up pros and cons, to evaluate different courses of action, and to invest possible futures on every level with enough reality and meaning to use them as decision-making aids. The simplest possible definition of foresight is: “opening to the future with every means at our disposal, developing views of future options, and then choosing between them”. The significance of foresight is further strengthened by its additional dimensions such as acting with provident care as well as the innate human ability to develop foresight to ensure long term survival (Suddendorf, Addis, & Corballis, 2009:1322).

Foresight thus can act to promote knowledgeability in humans, and as such it operates as a “higher order” language. Truly understanding the present is part of such a knowledgeability. Acknowledging that many of the prior actions of foresight have served the interests of those in power is also part of such a knowledgeability. This includes the understanding that language and technology should not be regarded as neutral, and endeavouring to view the present outside the confines of a short-term approach. Instead of seeking stability, understanding surprise, limits, disturbance, consciousness and transformation is likewise part of such a knowledgeability (Hayward, 2005).

A multitude of methods can be used to produce the knowledgeability that underlies insight. This is done through the application of a research design following a phased use of social study methods.

## **1.5 RESEARCH METHODOLOGY**

Qualitative research methodologies have been followed in this study. In this regard the study drew extensively on descriptive research, qualitative text analysis, and the use of business science and futures studies methodologies. The research process was conducted by following six qualitative research phases, namely the definition of concepts, an environmental scan, the development of a futures model inclusive of causal layered analysis (CLA) for information warfare (by way of grounded theory), a Delphi study, and a scenario exercise. Lastly, propositions are provided on the plausible manifestation of information warfare in the 2030s. Qualitative inquiry is aimed at improving the description and explanation of complex, real-world phenomena pertinent to information warfare, while futures methodology assists in providing insight into the plausible future manifestation of information warfare as an upcoming national security threat. The study was conducted in the period 2009 to 2015.

### 1.5.1 Qualitative text analysis

In some senses, data is always qualitative since it refers to essences of people, objects and situations (Miles & Huberman, 1994:9). In this study, the focus is on data in the form of words; thus language in the form of extended text. The words are based on documents, analysed text, Delphi questionnaires and observation. The data collection activities were carried out by the researcher in Pretoria and Beijing. Some data is not immediately accessible for analysis, but requires some processing (Miles & Huberman, 1994:9). Data analysis requires astute observation, questioning, a relentless search for answers and active recall. It is a process of piecing together data, of making the invisible obvious, of distinguishing significance from insignificance, of linking seemingly unrelated facts logically, of fitting categories with one another, and of attributing consequence to antecedents (Morse, 1994:25).

Processing and analysis in this study are done with qualitative text analysis. Kuckartz (2014:33) stated that qualitative text analysis is a form of analysis in which an understanding and interpretation of the text play a far greater role than in classical content analysis, which is more limited to the so-called manifest content. In contrast to some computer-assisted statistical analyses, which sometimes use automatic dictionary coding and which ignore ambiguities, qualitative content analysis presents an interpretive form of analysis in which the coding is completed on the basis of interpretation, classification and analysis. Moreover, text analysis and coding are not done exclusively by computer, so they are linked to human understanding and interpretation (Kuckartz, 2014:33-34). Kuckartz (2015) confirmed that the best results are obtained by using qualitative text analysis on documentary source material.

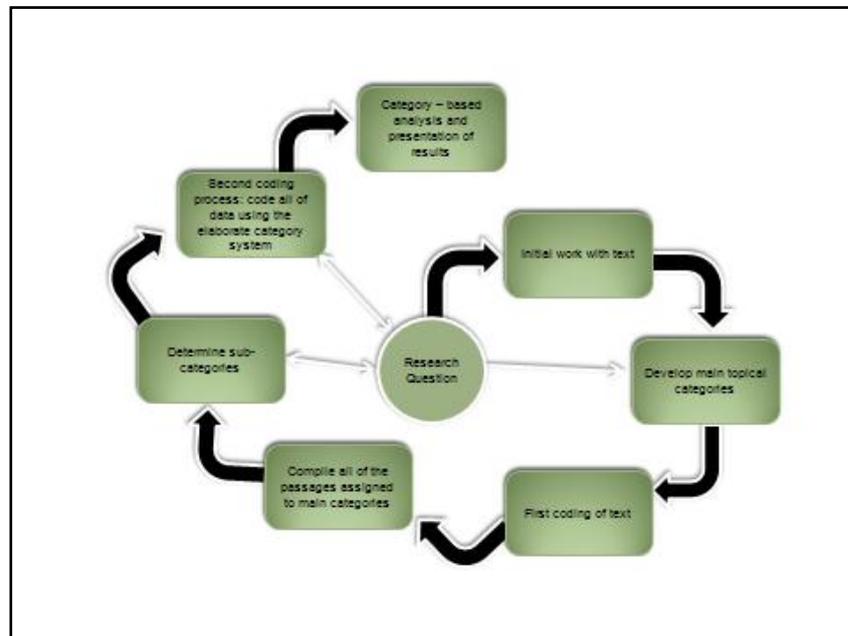
Open coding is used as the qualitative text analysis of choice. Open coding is defined as "... the analytic process through which concepts are identified and their properties and dimensions discovered in data" (Strauss & Corbin, 1998:101). Thus, open coding is the process during which the researcher starts to investigate, compare, conceptualise and categorise data. It "opens" the analysis by processing the data carefully and by developing preliminary concepts and their dimensions (Kuckartz, 2014:23).

Generally, during open coding, data is broken down into discrete elements, intimately examined, and compared for differences and similarities. Events, happenings, substance and actions/interactions that are found to be conceptually similar in nature or related in meaning are grouped under more abstract concepts termed "categories". Closely examining data for both differences and similarities allows for fine discrimination and differentiation among categories (Strauss & Corbin, 1998:102).

As the research focuses on theme-related issues associated with the current and future manifestation of information warfare, thematic qualitative text analysis is focused on the text itself, notably based on the text in its entirety. Even after categories have been assigned, the text itself,

i.e. the wording of the statements, is relevant and also plays an important role in the preparation and presentation of results (Kuckartz, 2014:66).

The basic process of thematic analysis focuses on seven steps, as illustrated below (see Figure 1.1 for a brief explanation of the process).



**Figure 1.1: Thematic qualitative text analysis process**

Source: Kuckartz, 2014:70.

Step 1 of the analysis process focuses on the initial text, highlighting text passages. During Step 2 the main thematic categories are developed. Step 3 centres on the first coding by utilising the main categories. During Step 4 and Step 5 all of the text passages that belong to the same main category are compiled, and sub-categories are created based on the data. During Step 6 the second coding process is executed, coding all the data using the complete category system. Finally, during Step 7 a category-based analysis takes place in which the relationships between the sub-categories and categories are highlighted (Kuckartz, 2014:71-84). During the coding exercise, coding software called Coding Analysis Toolkit (CAT), developed by the University of Pittsburgh, is used to assist in the qualitative text analysis process.

### 1.5.2 Methodology outline

The outline for the mentioned six qualitative research phases is explained above:

- i) Define key concepts including the definition of information warfare for which no general acceptable definition exist.

- ii) Conduct an environmental scan focused on the Technological, War/Conflict, Economic, Political and Social (TWEPS) macro-environmental hexagon.
- iii) Use grounded theory to create an information warfare futures model, in which CLA is also applied to the output of the environmental scan in order to identify the driving forces applicable to information warfare as a national security threat.
- iv) Prioritise and validate driving forces critical to the future manifestation of information warfare as a national security threat in the 2030s by way of Delphi studies.
- v) Develop four scenarios on the plausible manifestation of information warfare in the 2030s.
- vi) Formulate propositions on the plausible manifestation of information warfare in the 2030s.

### **1.5.3 Phase 1: Definition of concepts**

In this study two central concepts need clear definitions, namely information warfare and national security.

Although the information revolution and growing global integration are ensuring that information warfare<sup>1</sup> is destined to become one of the most significant national security challenges in the future, diverse and sometimes even contradictory definitions have complicated the debate about this phenomenon (Van Vuuren, 2009:177).

In this study the term information warfare is used in its contemporary and futurist contexts, but it is also acknowledged that the phenomenon has strong historical links. While some aspects related to information warfare are as old as humankind, many aspects as to how it is being applied in our contemporary information driven world are new (Jones, Kovacich & Luzwick, 2002:5). In order to facilitate a broader discussion on information warfare, an initial working definition of information warfare is proposed. Provisionally, information warfare refers to actions influencing the information networks of the state and society in general for power projection aims. However, despite the common use of the term the lack of consensus on its meaning in both academia and the mass media necessitates finding a more exact definition to assist in understanding this concept in its current and futurist contexts.

In this study information warfare is understood in the context of two broad categories. One category refers to the more intangible sphere of perceptions, deception, decisions, influencing and

---

<sup>1</sup> As on 12 August 2015 a Google Boolean search for the term "information warfare" indicated references to 470 000 documents.

knowledge, and the second refers to the more tangible sphere of digital networks, critical infrastructure protection and computer software and hardware. These two categories cannot be completely separated from one another. However, the study will focus more strongly on the contemporary manifestation, as well as the anticipated manifestation by the 2030s.

National security has been seriously debated since the end of the Cold War in particular, with some scholars and policy-makers calling for the expansion of its scope. This expansion of scope remains significant for this study but, in general, the theoretical aspects regarding national security as representing real and potential threats against the state are investigated. Additionally, the Information Age has a significant influence on national security with the contemporary challenge of how to meet national security needs in this new and ever-changing technology environment (Goldman, 2004:11). This is especially significant as the control and use of information and knowledge are increasingly central driving forces dominating human activity and progress.

#### **1.5.4 Phase 2: Environmental scanning**

After clarity is established regarding the key phenomena of information warfare and national security, the question remains as to what appropriate methodologies exist to evaluate the current milieu within which information warfare manifests with the capacity to also provide some level of insight into how a plausible future might manifest. For this purpose the appropriate futurist or business research methodology identified is an environmental scan.

Environmental scanning has proved its value to explain the current environment as well as its use as a futures methodological tool to investigate uncertainties about the future in a systematic fashion (Heinonen, 2008:53). Furthermore, it has the capacity to function on a higher level of knowledge creation rather than a lower level of information creation (Naude, 2016:14). Therefore, scanning the horizon is always prudent to identify new developments that can challenge past assumptions while it also provides new perspectives to future threats or opportunities (Gordon & Glenn, 2003:3). Information is gathered from the macro-environment with the aim to develop a better understanding of those factors and forces that may have a bearing on the way possible, probable and preferable futures take shape (Roux, 2007:1). This futures-orientated nature of environmental scanning is of particular value because an important effect of scanning is to increase and enhance communication and critical thought about future-oriented issues in general (Choo, 1999). The environmental scan is mainly focused on issues that directly influence information warfare as a national security threat.

The planned multi-disciplinary environmental scanning consists of a literature review, qualitative text analysis aimed at coding and focused on the current manifestation of information warfare, and the identification of the driving forces and trends influencing the future manifestation. Environmental scanning is the acquisition and use of information about events, trends, driving forces and relationships that form part of the external environment of any given phenomena.

Knowledge of this would assist in identifying the future development of the phenomenon (Choo, 2001).

At its broadest level, namely the macro environment, the focus is normally on the Social, Technological, Economic, Environmental and Political (STEEP) sectors (Kurian & Molitor, 1996:814). After critically evaluating the applicability of the STEEP sector for this study, the environmental sector is replaced by the war and conflict environment, thus creating a Technological, War/Conflict, Economic, Political and Social (TWEPS) macro-environmental hexagon.

The outcome of the environmental scan needs to be evaluated in order to identify the most significant driving forces which will influence the future manifestation of information warfare. The outcome of the environmental scan, however, is one-dimensional and does not necessarily take into account the full dynamics and complexity present in the macro environment. For this purpose a futures model opening the opportunity to enhance the depth of evaluation is useful.

### **1.5.5 Phase 3: Development of futures model inclusive of CLA**

The environmental scan lays the basis for the identification of the crucial driving forces that will be central to the manifestation of information warfare in the future. A futures model developed from the qualitative coding of the environmental scan serves as a roadmap to assist in identifying the driving forces influencing the future manifestation of information warfare as an upcoming national security threat. Such a model provides a tool for visualisation and understanding to add value to the analysis of the environmental scan output. However, additionally multi-level analysis as a methodology for the analysis of information with complex patterns of variability is needed. This is especially important with the underlying assumption being that information shows a hierarchy that cannot be neglected in such an analysis (Russo, 2009:64).

The grounded theory method is a systematic methodology in the social sciences involving the discovery of theory through the analysis of data (Martin & Turner, 1986:141). Grounded theory was proposed as a methodology with the aim of creating theory by way of systematically gathering and analysing data. The theory is a product of continuous interplay between analysis and data collection, and evolves during the research process itself. It furthermore requires the recognition that facts should be viewed as both theory laden and value laden, and that enquiry is always context bound (Goulding, 2002:42). In traditional social science, the researcher enters a research situation with an *a priori* theory, and the purpose of data collection is to “confirm” or “refute” that theory, hence the phrase confirmatory approach to science. In grounded theory, data is not used to test an *a priori* theory; rather, data is used to evolve a theory. Typically, the data is collected by means of qualitative methods (Jaccard & Jacoby, 2010:256). Knowledge is regarded as actively created with meanings of existence only relevant to an experiential world. Essentially, this

methodology is mostly applied with the aim to generate theory to provide a fresh slant on existing knowledge or where little is currently known (Baszanger, 1998:354).

In this study the aim of using grounded theory is not to create a theory but to assist in formulating a model that could be of value to focus the outcome of the environmental scan regarding the future of information warfare. The specific aim of the model will be to provide a framework to evaluate driving forces stemming from the TWEPS macro-environment hexagon. In order to provide magnitude to the insights and macro-driving forces within the model, causal layered analysis (CLA) is used within the model. CLA is a futures methodology which has the potential to bring depth to a research endeavour (Bussey, 2014:45). It is used as a mapping strategy to identify the main driving forces identified by way of an environmental scan (Inayatullah, 2014b). CLA is especially useful for generating new images of the future, given its focus on imagery and metaphor (Voros, 2006:51).

Using CLA evaluation takes place on four levels, namely the litany, social causes, discourse/worldview, and myth/metaphor levels. The litany level refers to the highly visible but largely unquestioned data and headlines which attract attention. The social cause level focuses on systemic approaches and situations underlying the visible litany level. The worldview level refers to the different ways of knowing. The last level refers to the myths, metaphors and narratives which are central to all views, actions and situations under scrutiny (Inayatullah, 2014a). The challenge is to conduct research that moves up and down these layers of analysis and is thus inclusive of different ways of knowing (Inayatullah, 2000).

Although CLA is a futures methodology it is less concerned with predicting a particular future than opening up the present and past to create alternative futures (Inayatullah, 2005a:50). As a methodology, CLA seeks to integrate empiricist, interpretive, critical and action learning modes of knowing (loosely, science, social science, philosophy and mythology). It is also useful for developing more effective, deeper, inclusive and longer term policy (Inayatullah, 2000). However, in this study the CLA aim is more restricted as it assists in integrating the driving forces produced by the environmental scan and later provides depth to the developed scenarios.

All of these methodological approaches provide the output for identifying the driving forces applicable to information warfare as a national security threat. These driving forces are developed within the TWEPS macro-environmental hexagon. Each driving force is described in terms of how and why it will affect information warfare as a national security threat. These driving forces are formulated to be both predictable and unpredictable. Identifying these driving forces is attempted from a range of disciplines with the aim to gain a holistic or systemic view based on these different insights.

### 1.5.6 Phase 4: Delphi study

The value of the information warfare futures model or CLA-derived insights is enhanced when it is scrutinised, integrated and validated by a panel of local and global experts knowledgeable about the environments identified as relevant to the future of information warfare. Given the lack of statistical data and concrete information on the future orientation of driving forces, expert opinion is used to assist in validating and prioritising these driving forces. A structured group method, namely the Delphi technique, is especially appropriate to be utilised in this regard (Keeney, Hasson, & McKenna, 2011:1).

The Delphi methodology was originally developed as a systematic, interactive forecasting method which relies on a panel of experts. This is useful in assisting to identify the main driving forces vital to the manifestation of information warfare as a national security threat in the 2030s. Through the Delphi technique, independent insights and forecasts are obtained from an expert panel over two or more rounds, with summaries of the anonymous inputs (and reasons for them) provided after each round (Armstrong, 2001:776). In using the Delphi method, it is possible to manage the exchange of information between anonymous panellists over a number of rounds (iterations), taking the average of the estimates on the final round as the group judgment (Rowe & Wright, 2001:125).

This method benefits from being a democratic and structured approach that harnesses the collective wisdom of participants (Powell, 2003:381). The Delphi study does not call for expert panels to be representative samples for statistical purposes. Representativeness is assessed on the qualities of the expert panel rather than its numbers (Powell, 2003:378). According to research conducted by Rowe and Wright (2001:125), Delphi groups are substantially more accurate than individual experts and traditional groups, and somewhat more accurate than statistical groups (which are made up of non-interacting individuals whose judgements are aggregated).

A Delphi study is thus conducted as the most suitable method for arriving at expert consensus on the most appropriate driving forces influencing the manifestation of information warfare as a national security threat by the 2030s. Delphi study users suggest that experts should be chosen for their work in the appropriate area and credibility with the target audience (Powell, 2003:379). The Delphi study focuses on experts from all the domains covered in the environmental scan, namely social, technological, economic, political and war/conflict (TWEPS) environments. However, the core study is the pilot study focusing on the South African security environment (encompassing individuals knowledgeable and experienced on the TWEPS macro environments). In order to compare the South African outcome with more general expert opinion, a domestic and global expert Delphi study is also performed.

The outcome of the Delphi study is a validated and prioritised list of driving forces relevant to the manifestation of information warfare as a national security threat in South Africa by the 2030s. This serves as substantial input for the development of scenarios on this issue.

### **1.5.7 Phase 5: Scenario analysis**

Next, a scenario-building exercise is conducted creating plausible information warfare scenarios with the aim of developing strategic insights into the manifestation of information warfare as a national security threat by the 2030s. Scenario analysis provides a method of developing alternative futures based on diverse combinations of assumptions, facts and driving forces. Scenarios are not about predicting, but rather about perceiving futures in the present (Schwartz, 1991:38). Scenarios present excellent mental frameworks for exploring new ideas and thinking. Part of this analysis entails identifying the two driving forces on two axes, assessing each force on an uncertain/(relatively) predictable and important/unimportant scale (University of Arizona, 2006). Four scenarios are developed, presenting a series of differing views of the environment within which information warfare will manifest as a national security threat by the 2030s.

Inayatullah (2005d:156) explained the full spectrum of scenario outcomes as being possible (irrespective of laws of the universe), plausible (more realistic, structural considerations), probable (given historical trends and quantitative data) and preferred (what participants desire, the vision of the organisation). The purpose in this study is to create plausible scenarios within which the manifestation of how information warfare could develop as a national security threat in South Africa by the 2030s could be evaluated.

### **1.5.8 Phase 6: Formulate propositions**

Once the scenarios are compiled, they provide the necessary insight and knowledge to formulate specific propositions applicable to interested parties who will by the 2030s be confronted by both international and domestic information warfare related national security threats. This provides insights into appropriate strategies, and new initiatives for strategic action to address information warfare as a national security threat.

## **1.6 LITERATURE SURVEY**

Sources of information included both primary and secondary sources. The study is focused on the qualitative social research as evidenced by the literature survey below. The literature used is found mainly in books and journals, in diverse fields of management and business studies, futures studies, international relations, strategic studies and sociology.

### 1.6.1 Theoretical literature

The first category is theoretical literature on the broader worldview in which information warfare manifests as a national security threat. In this context, there is significant literature relevant to critical realism, international relations and futures studies. Critical realism forms the foundation of the assumptions on the nature of reality and knowledge. Critical realism is built on the work of philosophy of science scholar Bhaskar in *A Realist Theory of Science* (2008).

Morgenthau's *Politics Among Nations: The Struggle for Power and Peace* (1973), Waltz's *The Balance of Power in International Politics* (1987), Nye's *Soft Power* (1990b), Wight's *International Theory: The Three Traditions* (1991), McGrew's *Conceptualizing Global Politics* (1992), Bull's *Order and Anarchy in International Society* (1992), Wight and Joseph's *Scientific Realism and International Relations* (2010) and Nye's *The Future of Power* (2011) are examples of major works on international relations. It is, however, obvious from analysing international relations literature that the capacity of existing international relations theory to adequately explain future security-related issues and conflicts remains limited, necessitating a broader approach to identifying international relations theories useful for this study. Therefore, theoretical work undertaken by postmodernist Baudrillard (1983) provides valuable insights into the power of symbolism and information in the Information Age.

The second category is the futures study literature, which provides the futurist context in which information warfare as a future national security threat can be viewed. Bell's seminal work on futures studies – *An Overview of Futures Studies* (2005) and both volumes of *Foundations of Futures Studies: Human Science for a New Era* (2007) – provide a comprehensive overview of future studies.

The rationale for futures studies and the role of the futurist are extensively described by futurist thinkers such as Brand (1999), Slaughter (2005), Inayatullah (2008a) and Spies (2015). Foresight remains a vital futures tool for opening the future with every means, developing views of future options, and then choosing between them (Slaughter, 1995:1). In *Thinking about the Future: Guidelines for Strategic Foresight*, Bishop and Hines (2013) provide an overview of the widely scattered professional knowledge and capability on strategic foresight in a way that provides useful insight into its application for futures studies. Foresight also highlights the need for creativity which requires divergent thinking (Van der Laan & Yap, 2016:70). Additional futures theoretical insights useful for the study of information futures includes the systems approach as proposed by Easton (1965), Waltz (1979) and Senge (1990); the futures map as formulated by Malaska and Virtanen (2009); and the CLA approach developed by Inayatullah (2000) and enhanced by Voros (2006). The collection of studies regarding the last mentioned method in *CLA 2.0: Transformative Research in Theory and Practice* edited by Inayatullah and Milojević (2015) shows that CLA can

also be used to reconstruct the future by creating worldviews and narrative solutions to the complex problems humanity faces.

### **1.6.2 Information warfare and national security literature**

The third category of literature focuses on information warfare and national security. Information warfare futures have not been the primary focus of any other scholarly study. Information warfare in terms of its modern meaning is also a fairly recent concept with the 1991 Gulf War refocusing the importance of information superiority especially in the realm of high-technology weapons in a modern conflict. This war was regarded as the first information war (Campen, 1992:vii). The origins of concepts and practices relevant to information in conflict, however, go back much earlier and can be identified in the seminal works *Art of War* by Tzu (translated 1963) and *On War* by Von Clausewitz (translated 1989). Where the legacy works focus on the role of information and knowledge in the successful conduct of war, the modern concept of information warfare remains closely linked to the exponential growth of digital and ICT capabilities and their role in enhancing political power projection.

Since 1991 extensive literature on information warfare theory and practice, much of which is in the public domain, followed (De Landa, 1991; Libicki, 1995; Schwartau, 1996; Waltz, 1998; Denning, 1999; Arquilla & Ronfeldt, 2001; Ventre, 2009 & 2011; Singer & Friedman, 2014 and Green, 2015). While the literature does provide a comprehensive description of information warfare manifestations, no consensus exists on defining information warfare. However, the fundamental common elements and characteristics of information warfare have been identified (Vlahos, 1998; Arquilla & Ronfeldt, 2001; Bishara, 2001; McLendon, 2008 and Schneier, 2008). Some scholars such as Grey (2007) argued conflicts in the history of humankind have been defined by the use of asymmetries that exploit an opponent's weaknesses, thus leading to complex situations involving regular/irregular and conventional/unconventional tactics. Similarly, the rise of information warfare has according to him not fundamentally changed the nature of warfare, but expanded its use in a new dimension.

Official and international publications served as important components for the collection, research and analysis processes. While information warfare and related concepts are fairly recent developments, the nature of this theme is largely internet friendly with many of the studies and official publications available on the World Wide Web (WWW) and the rest of the internet. A major challenge in evaluating these materials was the significant United States of America (USA) bias in available material on information warfare. Since the mid-1990s writers from Europe, Australia, Israel and to a lesser extent China and India have also been focusing on relevant themes. A developing world perspective on this issue is, however, nearly completely absent. This issue has been a high priority focus in China but only a fraction of material in Mandarin has been translated. Even here the main interest is again from a Taiwanese and USA perspective. The researcher

critically evaluated relevant published and unpublished works, studies, policy documents, journals and electronic resources on information warfare issues.

Coupled with challenges brought about by globalisation and the Information Age, national security also needed to adapt to this new and ever-changing technology environment (Goldman, 2004:11). The changing nature of national security is addressed to include additional non-military issues, for example economics, the environment and human rights have increasingly forced their way onto the global security agenda (Sheehan, 2000:471). A United Nations (2004) report on *Threats, Challenges and Change* helped to fundamentally shift the focus of National Security by emphasising that states' security threats do not respect national boundaries – from invasion, war and conflict within states they extend to poverty, infectious diseases and environmental degradation. Scholars also started to focus on works about the security implication of technology (Rappert & Croft, 2007). Additionally the rise of the Copenhagen School of thought increased coexistence and competition on what national security entails as the notion that the individual and not the state should be the primary beneficiary of national security. The Copenhagen School places particular emphasis upon the social aspects of security (Mcsweeney, 1996:82).

### 1.6.3 Methodological literature

The fourth category is the literature on methodologies (environmental scanning, Delphi studies and scenario studies), qualitative text analysis methods, qualitative coding and model building by way of grounded theory used in this study. Environmental scanning is elucidated by Coates' *Issues Identification and Management: The State of the Art of Methods and Techniques* (1985), Choo's *The Art of Scanning the Environment* (1999), Molitor's *Molitor Forecasting Model: Key Dimensions for Plotting the "Patterns of Change"* and Morrison's *Environmental Scanning* (1992).

Kurian and Molitor in the *Encyclopaedia of the Future* (1996) raised the use of STEEP (Social, Technological, Economic, Environmental and Political) sectors in environmental scanning. As various futurists use different systems to uniquely classify the focus area of their studies (Haberman, 2013), for the purpose of this study the environmental sector is replaced by a conflict/war sector as this reflects to focus area of this study closer. Thereby creating the social, technological, economic, political and war/conflict (TWEPS) environments. Most literature on environmental scanning refers to its role in business contexts, but the future-orientated nature of environmental scanning is of particular value because an important effect of scanning is to increase and enhance communication and critical thought about future-oriented issues in general (Choo, 1999).

The qualitative text analysis and the qualitative coding are provided by Kuckartz in *Qualitative Text Analysis: A Guide to Methods, Practice and Using Software* (2014) and Charmaz in *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis* (2006). These publications also provide practical guidance with the qualitative coding process. Computer assistance in coding is

provided by using the Coding Analysis Toolkit (CAT) software developed by the University of Pittsburgh's Qualitative Data Analysis Program (QDAP) (University of Pittsburgh, 2015).

Assisting in the visualisation of system elements, modelling is used as a mental tool to represent reality. Here Jaccard and Jacoby's *Theory Construction and Model-Building Skills: A Practical Guide for Social Scientists* (2010) provides valuable insights. Grounded theory is utilised in this regard as presented by Martin and Turner (1986), Strauss and Corbin (1998), Goulding (2002) and Charmaz (2006). Although grounded theory is generally used to develop theory, in this study it is used to assist in developing a model for information warfare futures.

The framework for developing such a model is provided by the futures map (Kuusi, Cuhls & Steinmüller, 2015), causal layered analysis (CLA) (Voros, 2006 & Inayatullah, 2008c) and systems layered explanation of reality (Senge, Smith, Kruschwitz, Laur & Schley, 2008). Modelling is a visualisation and mental tool developed to add value to the analysis of the environmental scan output.

The Delphi method is used to scrutinise, integrate and validate the driving forces identified in the environmental scan, and processed in terms of the information warfare model. Extensive background information and practical advice are provided by Rowe and Wright (2001), Linstone and Turoff (2002), Gordon (2003), Powell (2003), Okoli and Pawlowski (2004) as well as Keeney, Hasson and McKenna, 2011:1) on the techniques and applications of the Delphi method. Literature provides sufficient insight to utilise the Delphi method with the aim to achieve the goals set.

The literature on scenario planning models and methodologies is found mainly in books and journals, chiefly in the field of management and business. The following works serve as leading examples: *The Art of the Long View: The Path to Strategic Insight for Yourself and Your Company* by Schwartz (1991), *Scenario Planning: The link between future and strategy* by Lindgren and Bandhold (2003), *Scenarios: The Art of Strategic Conversations* by Van der Heijden (2005), *Foresight: The Art and Science of Anticipating the Future* by Loveridge (2009) and *Scenario Planning in Organizations: How to Create, Use, and Assess Scenarios* by Chermack (2011).

## **1.7 ETHICAL REQUIREMENTS**

In this study, the researcher is committed to protecting the rights, privacy, dignity and well-being of the persons who took part in this research. This applied in particular to the conduct of the Delphi studies in which local and foreign experts participated.

As the Delphi studies might present some ethical challenges these were carefully managed to ensure that they remained a low-risk endeavour by abiding to the following principles:

- Possible participants were provided with the background, potential benefit and aim of the study.

- Participants were informed that participation is voluntary, and individuals were free to stop participating at any stage.
- Participants were informed that their identities would not be revealed to other members of the study or identified in the thesis; their privacy was respected and it was confirmed, where appropriate, that organisational approval had been granted for their participation.

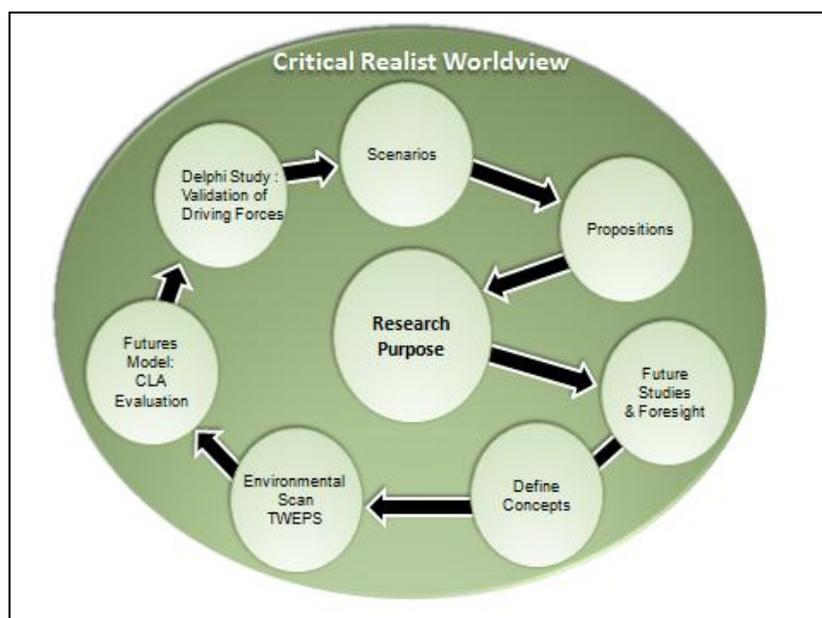
The Departmental Ethics Screening Committee of the University of Stellenbosch Business School (USB-DESC) reviewed the researcher's application for the Delphi studies, and the research as set out in the ethics application was approved on 23 June 2014.

The pilot study was conducted with a South African foreign security panel providing a cross-environmental perspective on the proposed driving forces. In January 2014, the relevant state entity responsible for South African foreign security related issues granted permission for the researcher to proceed with a Delphi study, provided that no members participating were identified and no organisational information was revealed in the study. As anonymity is one of the criteria for a Delphi study and as classified information is not the focus of this study, these provisos had no negative impact on the outcome of the pilot study. In line with the request the name of the intuition is also not revealed in this study. The pilot Delphi study was conducted from August 2014 to February 2015. A second Delphi study was conducted from February 2015 to September 2015 in which domestic and international experts participated.

## 1.8 STRUCTURE OF THE STUDY

To provide a response to the problem statement and to reach the aim of this study, sub-problems were formulated. These sub-problems have been addressed in line with the stated research outline.

This study consists of nine chapters. See Figure 1.2 for a visualisation of the research outline.



## Figure 1.2: Visualisation of the research outline

Chapter 1 is an introductory chapter which sets out the identification, demarcation and formulation of the research problem. An overview of the study aims, thesis statement, philosophical approach, methodology, a core literature survey, the ethical requirements and an outline of the structure of the study are provided.

In Chapter 2 the following sub-problems are dealt with: *What are the epistemological approaches followed in this study and how does international relations theory provide insight into information warfare as an upcoming national security threat?* The critical realist worldview is elucidated and theoretical underpinnings in terms of international relations theory are provided.

Chapter 3 deals with the second sub-problem: *What is futures studies' contribution in providing insight into the future of information warfare?* The focus is on futures studies, its rationale, systems approach, the futures map and layered analysis tools. Foresight can act to promote knowledgeability in humans, and as such it operates as a "higher order" language.

Chapter 4 deals with the third sub-problem, namely: *What do the concepts information warfare and national security represent?* Both information warfare and national security are defined and explained. A brief overview of the manifestation of information warfare is provided.

The fourth sub-problem is dealt with in Chapter 5. *How does information warfare manifest in the current environment taking into account factors influencing its future manifestation in the 2030s?* The environmental scan is focused on events, developments and manifestations related to information warfare and national security within the TWEPS macro-environmental hexagon. This multi-disciplinary environmental scanning focuses on literature with the aim to identify current manifestations, but also to recognise possible trends and driving forces flowing from this.

In Chapter 6 the fifth sub-problem is answered, namely *How can the output of the environmental scan be processed to assist in providing foresight into the future manifestation of information warfare as a future national security threat?* The output from the TWEPS macro-environment hexagon is processed using qualitative text analysis coding and grounded theory to develop a futures model. CLA is integrated into the model with the aim to assist in identifying the key driving forces underlying the future manifestation of information warfare.

The sixth sub-problem is dealt with in Chapter 7. *What are the main driving forces which will influence the shaping of the future of information warfare as a national security threat?* Expert opinion by way of a Delphi study is used to prioritise and validate the driving forces identified in the environmental scan.

The seventh sub-problem is the focus of Chapter 8. *What are the plausible scenarios in which information warfare would manifest as a national security threat for South Africa?* The four

plausible scenarios according to which information warfare could manifest by the 2030s are provided.

In Chapter 9, the conclusion, the final problem relevant to the study will be answered and the outcome of the research will be provided. *What propositions can be identified applying to the plausible information warfare threat against South Africa in the 2030s?* Propositions are identified which could provide interested parties with insights into the driving forces that would be critical in the creation of these scenarios.

## CHAPTER 2

# INFORMATION AS STRATEGIC POWER INSTRUMENT: THEORETICAL APPROACH

### 2.1 INTRODUCTION

Information in all its manifestations from data to wisdom has been central to institutional power since the dawn of humankind. The technological efficacies brought about by the digital revolution and the enhanced global networking activities have boosted the role of information in national power. Technological development catapulted information to the centre of most human endeavours, although high levels of inequality persist as manifested in the so-called digital divide. However, innovation does have the potential to address at least some aspects of inequality in the future. The digital and information revolutions have enhanced the impact of information globally, with significant implications for the phenomenon of information warfare, which is likely to pose a significant risk to global society on many levels in the future.

Since information warfare is a relatively new concept it has not been adequately addressed in social science theoretical frameworks. Focusing on the challenge that information warfare poses to national security in the future, the starting point for the theoretical framing of this phenomenon is in the appropriate social science disciplines. Such a systematic reflection will need to take note of issues such as integration versus disintegration, nationalism versus globalism, and conflict versus cooperation, which are simultaneous but divergent trends that underlie the transformation of contemporary international relations and the security environment. These sometimes divergent trends and forces influencing national security in the international system require an integrated use of theoretical insights. The aim in this chapter is to highlight the theoretical frameworks against which information warfare as a security threat can be analysed. The philosophical approach for this study is sourced from different social science disciplines, mainly from futures studies and international relations theory, but also from other relevant social sciences such as sociology and political science.

The worldview and theory within which these phenomena can be understood, explained and foresight generated need to be presented in a systematic way. Before a more precise definition of information warfare as a national security threat can be presented in Chapter 4, the macro-theoretical framework within which this study is embedded must be elucidated. Thus, this chapter is centred on the theoretical approaches followed in the study, while the theoretical and practical link with futures studies and foresight is highlighted in the next chapter.

Dougherty and Pfalzgraff (1997:15) defined theory as “systematic reflection on phenomena, designed to explain them and to show how they are related to each other in a meaningful, intelligent pattern, instead of being merely random items in an incoherent universe”. By creating the mental order, theory fulfils useful roles in endeavouring to understand and explain the world. However, there is another view of theory, namely that theories “constitute” the world on which they are focusing. According to this view, theories can never be separate from the world; thus they are an intrinsic part of it. Therefore, there can never be a “view from nowhere”, and all theories make assumptions about the world, both ontological ones (what features need understanding or explaining) and epistemological ones (what counts as understanding or explanation). All theories are located in space, time, culture and history, and there is no possibility of the separation from these (Smith, 2013:9).

## 2.2 CRITICAL REALISM AS OVERARCHING THEORY

One of the reasons for the development of critical realism is the critique of the positivist approach which has dominated many of the social sciences since the 1930s (Danermark, Ekström, Jakobsen & Karlsson, 2005:2). Positivism is a philosophy of science based on the view that information derived from logical and mathematical origins and reports of sensory experience is the only source of all authoritative knowledge (Macionis & Gerber, 2011:79). Critical realism is being associated with the British philosopher Roy Bhaskar (Judd, 2003:14). Bhaskar’s critical realism has since been expanded on and used in academic disciplines such as sociology, economics, psychology, future studies and international relations.

Bhaskar (2008:46) provided an “ontological map” which distinguishes between three ontological domains: the empirical, the actual and the real. The empirical domain consists of what is experienced, directly or indirectly. It is separated from the actual domain where events happen whether it is experienced or not. That which is observed is not the same as what happens in the world. The domain of the actual is in its turn separated from the domain of the real. In this domain there is also that which can produce events in the world, that which metaphorically can be called mechanisms. See Table 2.1 for a breakdown of critical realism’s ontological map.

**Table 2.1: Critical realism’s ontological map**

	Domain of the real	Domain of the actual	Domain of the empirical
Mechanisms	√		
Events	√	√	
Experiences	√	√	√

(Source: Bhaskar, 2008:47.)

Bhaskar (2008:46) argued that events must occur independently of the experiences in which they are apprehended. Structures and mechanisms are real and distinct from the patterns of events that they generate; at the same time events are real and distinct from the experiences in which they are held.

These three levels of reality are not naturally or normally in phase, but it is the social activity of science which makes them so. Experiences, and the facts they cause, are social products. The conjunctions of events, when held in experience, provide the grounds for causal laws. These are also social products. Underlying the implicit ontology of critical realism is that it is an implicit human endeavour in which facts and their conjunctions are seen as produced by humankind or given by nature (Bhaskar, 2008:47). The empirical domain, which in scientific contexts contains humanity's "facts" or "data", is always theory-laden. Practically all data produced arises in connection with some theory, and thus an individual does not experience the events in a direct way, which is what the empiricist research tradition claims. Individual theoretical conceptions are always mediating data (Danermark, Ekström, Jakobsen & Karlsson, 2005:5).

Consequently, even the rather common expression "the empirical world" is misleading. It represents what Bhaskar (1978:36) calls "the epistemic fallacy", because it reduces the three domains to a single one. It reduces what can be known about it. Scientific work should rather investigate and identify relationships and non-relationships between, respectively, what individuals experience, what actually happens, and the underlying mechanisms that produce the events in the world (Danermark, Ekström, Jakobsen & Karlsson, 2005:21). Although mechanisms, events and experiences are distinct, value can be obtained by moving focus between these levels in order to enhance the analytical process. This is explored further in Chapter 3, which focuses on futures studies and especially a layered analysis system approach.

Within philosophy, critical realism involves a switch from epistemology to ontology, and within ontology a switch from events to mechanisms. This is the core of critical realism, and it reflects a metatheory with consequences for scientific work. What Bhaskar (2008:13) emphasised here is the fundamental question in the philosophy of science: "What properties do societies and people possess that might make them possible objects for knowledge?" This ontological question must be the starting point for a philosophy of reality, not the epistemological question of how knowledge is possible, which in the past has mostly been the case (Danermark, Ekström, Jakobsen & Karlsson, 2005:5).

Another significant contribution by critical realism is the switch from events to mechanisms, which means switching the attention to what produces the events, not just to the events themselves. Reality is thus assumed to consist of experiences, events and mechanisms. Mechanisms sometimes generate an event. When they are experienced they become an empirical fact. If one is to attain knowledge about underlying causal mechanisms, it is necessary to focus on these

mechanisms, not only on the empirically observable events (Danermark, Ekström, Jakobsen & Karlsson, 2005:5-6). This is especially relevant from a futurist perspective as the underlying mechanisms directly influence the driving forces.

Furthermore, rather than following the pattern in some critical literature, for example on information technology as instrument of freedom versus information technology as instrument of oppression where discussion of causation is avoided entirely on the grounds that it is an essentially positivist pursuit, critical realism allows the researcher to “reclaim” causal analysis for the critical traditions (Whitham, 2014:15). Critical realism thus “assumes that causal relationships exist outside of the human mind” (Cook & Campbell, 1979:29).

The point of departure in critical realism is that the world is structured, differentiated, stratified and changing (Danermark, Ekström, Jakobsen & Karlsson, 2005:5). Bunge (2009:366-368) highlighted the following implications, namely that:

- Reality is arranged in levels;
- Something qualitatively new can emerge from a lower level (emergence); and
- There is a distinction between a real world and a conceptual one.

Critical realism also provides an answer to the serious dichotomy of realism versus anti-realism, where the fundamental question is whether there exists a world independently of human consciousness. According to critical realism there exists both an external world independently of human consciousness, and at the same time a dimension that includes our socially determined knowledge about reality (Danermark, Ekström, Jakobsen & Karlsson, 2005:5-6). Thus critical realism is “realist” because it assumes that a reality exists quite apart of human constructions of it. This is known as “ontological realism”. It is a belief “that the world of which we have knowledge exists quite apart of human constructions of it” (Skagestad, 1981:77-78).

It is also important to understand the relations between practice, meaning, concept and language. In this context the decisive differences between the objects of natural science and social science should be noted. These differences, among other things, lead to the situation that whereas experiment is seen as the main method of the natural sciences, the focus in social science practice is on conceptualisation through conceptual abstraction (Danermark, Ekström, Jakobsen & Karlsson, 2005:40).

When focusing on science, it includes a concern about the logical structure and coherence of statements and also a special concern about the utility in manipulating the world to achieve human goals as, for example, in the conscious process of using known cause-and-effect relationships to create desired ends (Bell, 2007:207). Science rests on the supposition that although many aspects of reality may always remain beyond human facility to discern and understand, how the world really is, plays a decisive role in the achievements of science. Truth can be known within the limits of

human senses and intellect. Even though truth "... is not absolute and is fallible, conjectural, conditional, corrigible, tentative, qualitatively judgmental, and presuppositional; warranted assertability is possible; some assertions are true and some are false, and we can frequently justify our beliefs, empirically or logically, about which is which" (Bell, 2007:207-208).

Although critical realism will be the overall philosophical approach, insights from various international relations theories are relevant to the manifestation of information warfare as a national security threat currently and in the future. Contributions are made from realism, rationalism, critical realism in international relations theory, critical security studies and postmodernism in this regard.

### **2.3 INTERNATIONAL RELATIONS THEORY**

Critical realism provides the insight regarding the shift of emphasis from experience and events to mechanisms. To obtain such knowledge about underlying causal mechanisms impacting the role of information and information warfare in the global terrain, it is necessary to provide an overview of relevant international relations and related theories.

The capacity of existing international relations theory to adequately explain future security related issues and conflicts remains limited, necessitating a broader approach to identify international relations theories useful for this study. This is in particular the case because of the growing importance of the information revolution and the impact of globalisation on national and international security. This trend towards a multi-disciplinary approach has manifested even within international relations theory (Burchill & Linklater, 2005:23). Combining different theories could lead to epistemological difficulties, but critical realism attempts to provide a framework within which a synthesis of more than one position is possible (Smith, 2013:12). Niiniluoto (2002:21) stated that critical realism turns out to be compatible with a surprising variety of philosophical positions.

Similar to the broader situation with theory, it is not possible to simply add up these various accounts of international relations to get one overarching theory. Theories are part of the social world; they can never be separate from it, and thus they constitute the social world in which we live. Each defines the problems to be examined differently, and may well define how we know things about those problems in different ways. Thus the social location of the observer will influence which theory is regarded as the most useful, simply because that location will predispose that observer to define some features of international relations as key and others as less relevant (Smith, 2013:11).

Classically, the study of international relations has focused on the analysis of the causes of war and the conditions of peace. Such an agenda seemed particularly pertinent in the 20th century in the aftermath of two World Wars. However, the study of the use of force continues to motivate international relations scholars even now "... as we move well into the second decade of the twenty-first century" (Smith, 2013:1). The social world is one in which individuals exist within

powerful economic, political, social, racial, gendered, moral and linguistic structures (Smith, 2013:3). Theories offer accounts of why things happened, and the fact that they offer a wide range of reasons for action reflects the fact that they have very different assumptions (Smith, 2013:3). None of this means that the traditionally dominant mainstream approaches are outdated or peripheral to an explanation of international relations.

So, although many of the mentioned theories are absolutely central to explain aspects of international relations, equally importantly, they are not sufficient to explain the complexities associated with information warfare as global and national power projection phenomena on their own. Wight (1991) identified the main international political traditions as the realist, rationalist and revolutionist traditions. Each of these traditions embodies a great variety of doctrines about international relations, among which there sometimes exists only a loose connection. These traditions, however, incorporate a set of distinctive questions and assumptions about the basic units and forces in international relations (Keohane, 1989:2). Such paradigms<sup>2</sup> or worldviews represent the main traditions of political thought, a description of the nature of international relations and a set of prescriptions about international conduct (Bull, 1987:93). These traditions represent comprehensively normative views of international relations, which are relevant to debates about security within contemporary international relations. The interaction and dialogues created between the traditions are conducive for efforts to explain the dynamics of international relations.

Wight (1991) described these traditions as related to three interrelated political conditions which comprise the main subject matter of international relations. The first condition is that no political superior is acknowledged and a multiplicity of independent sovereign states accepts the use of military force and warfare ultimately as a method to regulate relationships. This is the basis of the realist worldview regarding international relations. Realism explains and interprets world politics in terms of power (Basu, 2012:171). Realists stress power and interest rather than ideals in international relations. Realism is basically conservative, empirical, prudent, suspicious of idealistic principles, and respectful of the lessons of history. It is also more likely to produce a pessimistic rather than an optimistic view of international relations. Realists regard power as the fundamental concept in the social sciences (such as energy in physics), although they admit that power relationships are often cloaked in moral and legal terms. Realists view theories as rationalising, rather than shaping, events. They criticise the utopian approaches to international relations for preferring visionary goals to scientific analysis (Carr, 1964:40). According to the realists a state's ideological or ethical preferences are neither good nor bad but what matters is whether its self-interest is served (Kegley & Wittkopf, 1997:23).

---

<sup>2</sup> A paradigm is a mixture of beliefs, theory, preconceptions and prejudices that shapes ideas of how the international system works, generates expectations and prescribes appropriate behaviour (McCgwire, 2001:777). The term was coined by Thomas S. Kuhn (1962) and used by him in a more formal way.

The second condition identified is that diplomacy and commerce form the basis of international and institutionalised interaction between sovereign states. Rationalists tend to emphasise and concentrate on this element of international interaction. The focus is on the role of measures to create and enhance order in the anarchic world as well as the concept of an international society. Emphasising how people ought to behave in their international relationships rather than how they actually behave, rationalists usually spurn balance of power politics, national armaments and the use of force in international affairs. Instead, they stress international legal rights and obligations, the natural harmony of national interests as a regulator for the preservation of international peace, a significant reliance upon reason in human affairs, and confidence in the peace-building function of the “world court of public opinion” (Carr, 1964:40). Rationalists thus argue that an element of order is maintained in the international society despite the absence of a central authority commanding overwhelming force and a monopoly of the legitimate use of it (Bull, 1992:590).

Thirdly, the concept of a society of states, or family of nations, brings with it certain moral and psychological as well as possibly even legal obligations. Revolutionists tend to concentrate on the concept of a society of states or international society but they can be defined more precisely as those who believe passionately in the moral unity of a society of states. This view is strongly influenced by an ideological or extremist religious worldview. Revolutionists postulate a transcendental source of authority behind political structures, social interaction and government. At first revolutionists endeavour to explain the overall structure of the global system, within which behaviour takes place. In this regard the tracing of the historical evolution of systems is especially of value. In general, the revolutionists assume that mechanisms of domination exist that keep disadvantaged people as well as nations from development, and that this contributes to world-wide inequalities (Viotti & Kauppi, 1999:399-400). The revolutionist’s paradigm provides a framework for opposing this situation and foresees a deterministic solution to these problems (Van Vuuren, 2003:23). Although the influence of this paradigm has diminished since the end of the Cold War it has again become relevant since the 2014 rise of the Islamic State (IS) in Syria and Iraq and extremist activity in Africa (Roggio, 2014).

The challenges posed by the Information Age have already identified some theoretical shortcomings to accommodate the challenges posed by the growth of information as instrument of power. The changing nature of national security and the role of information in this context do highlight shortcomings related to the advancement of the role of information in the modern world, which transcends the boundaries of realist, rationalist and revolutionist paradigms. Theoretical work done in terms of critical realism within international relations theory and specifically theory focusing on the power of symbolism done by Baudrillard (1983) are of value in this regard.

### 2.3.1 The realist tradition

#### 2.3.1.1 *The central role of power*

Realists in the context of international relations theory have a high regard for the value of national security, state survival, and international order and stability. In general, they believe that there are no international obligations in the moral sense of the word (i.e. bonds of mutual duty) between independent states (Jackson & Sørensen, 2003:103).

In the mind of the realist, power plays a central role in this world view. Realists postulate that any political unit (such as a state) will act in such a way as to maximise its power, which is defined mainly in terms of the security of its territory (Edwards, 1969:69). Political power can be seen as a psychological relation between those who exercise it and those over whom it is exercised. Those who exercise power gain control by actions which have an impact on the minds of those over whom it is exercised. The impact derives from three sources, according to Hans Morgenthau (1973:28), namely "... the expectation of benefits, the fear of disadvantages, and the respect or love for men and institutions". Power may be exerted through orders, threats, the authority or charisma of a person or of an office, or a combination of any of these.

Traditionally, the power exercised by states within the international system is viewed as the aggregate of many attributes, including economic, technological, cultural, diplomatic, ideological and military factors. Two groups of factors that form the basis of power are identified by Morgenthau (1973:112-113); those that are relatively stable, and those that are subject to constant change. Some of the more stable factors underlying a state's power include geography and natural resources. Less stable factors include industrial capacity, military preparedness, national morale, the quality of foreign policy management, as well as the quality of government. The information dimension<sup>3</sup> of power can be regarded as part of the growing but also less stable factors underlying state power. Despite a growth in what is termed "soft power" in international relations, "hard power" such as military power and the capacity to use violence for the protection, enforcement or extension of authority are instruments which the vast majority of states still find impossible to totally dispose of (Howard, 1970:115). States are also confronted with the dilemma of finding a balance between security versus defence needs.

The struggle to increase power by strengthening, for example, military capabilities has negative consequences for the security of other states. Each state must look to itself to guarantee its security against (potential) threats from other states. At least in terms of security, states are locked into conflict, and the security of one or some is often obtained at the expense of the insecurity of others. This is because of what is known as the security dilemma. It is often difficult, if not

---

<sup>3</sup> The information dimension refers to the role of information in maintaining and expanding the power instruments of the state.

impossible, to distinguish between offensive and defensive military capabilities. Capabilities that make one state feel secure are regarded by other states as threatening, and vice versa (Bromley, 2004:108).

Most realists focus their analytical efforts on the behaviour of the national state because they believe that the state has remained relatively more powerful than other types of transnational entities and forces, such as international organisations, multilateral corporations or capitalist markets, non-state actors, religions and cultures. However, realists are clear that their propositions are supposed to apply to groups in general and that a dynamic of competitive, relative power can be found in the behaviour of all types of groups throughout history (Sterling-Folker, 2006:16).

### 2.3.1.2 *Stability through the balance of power*

Significant inequalities in the power between states increase possible insecurities experienced in the international political system. In this regard equilibrium between states in the form of a balance of power remains a useful means of denoting contemporary and possible future strategies for security.<sup>4</sup> Such a balance of power includes a balance of all the capacities, including physical force which states choose to use in pursuing their goals (Waltz, 1987:100).

The aim of a balance of power system is thus to create equilibrium to promote stability. The concept of “equilibrium” as a synonym for “balance” is commonly employed in many sciences, including physics, biology, economics, sociology and political science. It signifies stability within a system composed of a number of autonomous forces. Whenever the equilibrium is disturbed, either by an outside force or by a change in one or other element composing the system, the system shows a tendency to re-establish either the original or a new equilibrium (Morgenthau, 1970:167-168). Thus, a balance of power system is generally in equilibrium because usually the territorial integrity and physical survival of states are not in question (Twitchett, 1971:24).

The balance of power embodies the belief that any state’s survival is best assured by reliance on its own military strength, allied where and when necessary to the military strength of others. The main objective of the balance of power is to preserve the security of states, particularly the larger ones. It is thus focuses on preserving the state system or international stability (Berridge, 1997:166).

Stemming from stability, peace has since the advent of nuclear weapons become an objective of the balance of power. Nevertheless, nuclear weapons have merely raised the finite political price

---

4

The balance of power theory has been criticised by many theorists including realists such as Hans J. Morgenthau, describing it *inter alia* “... as a crude, unsophisticated, naively simplistic, or obsolete theory of international politics” (Dougherty & Pfalzgraff, 1997:26-28). It, however, remains a useful concept to make sense of the power relationship between states and other entities even in the Information Age.

that states are prepared to pay for peace within the balance of power; there is no evidence that they have raised this price to infinity itself. The values and passions attached to independence, not peace, remain the primary objectives of the balance of power (Berridge, 1997:167). The Information Age influenced the way in which the balance of power manifests.

### 2.3.1.3 *Balance of power in the Information Age*

Even in the Information Age the traditional measures of military force, gross national product, population, land, minerals and energy continue to dominate discussions of the balance of power. These power resources still matter and governments continue to depend on them but the information dimension of these resources as well as information in its own right are growing in significance. Information power remains difficult to categorise because it cuts across all other military, economic, social and political power resources, in some cases diminishing their strength, in others multiplying it (Nye & Owens, 1996:xviii). Nye and Owens (1996:2), in highlighting the soft power attributes of contemporary power, contended that "... soft power is passing from the capital rich to the information rich".

According to Gompert (1998:5), information technology is the *sine qua non* of both power and globalisation as it is integrating the world economy and spreading freedom, while at the same time becoming increasingly crucial to military and other forms of national power. Information technology thus accounts both for "power and the process that softens and smooths power". Technological development enhances two trends that change the role of the state, having implications for national security, increasing the role of non-state entities and increasing internationalisation. Two central conflicts reveal the nature of the ongoing redistribution of power: first, the notion that the information revolution empowers new forms of international actors, such as NGOs and activists, thus challenging the state's status as the major player in the international system, and second, the idea that the emergence of a global e-commerce market would inevitably challenge the state's economic influence as companies increasingly become global citizens and as economic boundaries no longer correspond to political ones. Both of these trends have particular implications for states' freedom of action to manoeuvre when it comes to security (Rothkopf, 1998:321-356).

Mayer-Schoenberger and Brodnig (2001:27) stated that information power shifts among and between the key stakeholders in international relations, namely governments, corporations and NGOs are occurring. It is possible to attribute these power reconfigurations to shifts of control over the underlying information infrastructures, strengthening the non-governmental sector's power position. The contrary view is also held that technological innovation strengthens and not weakens the state's power to control and secure its position in terms of potential security threats (Morozov, 2011:xvii). Some authoritarian governments actively censor content and regularly disrupt internet service, with limited direct evidence that digital activism has succeeded in opening closed regimes. However, social media and the internet in general are in fact important instruments for the purpose

of pressurising authoritative regimes to relinquish control for the betterment of the individual, society and global civilisation (Stanko, 2013:16-17). It can be expected that the role of social media will become a power flashpoint in the future.

While military power still remains dominant in the positioning of states, the impact of information related power raises potential for the future. Global inequality remains a problem and a factor inhibiting the power position of weaker states. The decreasing cost of technology, however, makes it possible to acquire asymmetric capabilities by jumping certain development phases. Technology thus ensures that the capacity for national power will change. These changes would probably be exponential. A combination of old and new capacities could also result in the growth of asymmetric power capacity, which could enhance a state's power or ensure that the power profile of states change significantly in a relatively short space of time.

Information warfare can thus be added to the realist's existing assortment of power instruments. While this dimension has been part of the traditional power instruments in the past, it can be expected that the expansion in scope, sophistication and role of information networked systems will increase significantly in the future. Chapter 5 will provide an overview of how information warfare has recently manifested globally.

#### *2.3.1.4 Criticism of realism*

The state is the centrepiece of realist thought. While the state remains a major force in international relations this situation is changing. General criticism against the views of realists is that they ignore other actors and other issues not directly related to the maintenance of state security. Non-state actors such as multinational corporations, NGOs, financial institutions and terrorists are mostly excluded, downplayed or trivialised in the realist perspective. The lack of viewing the world outside the realist's relatively narrow national security prism result in issues, such as the global socio-economic inequality and environmental concerns, not forming part of the realist's national security threat perception (Viotti & Kauppi, 1999:84-85).

The main question remains: To what extent can realism really explain the changing nature of the international environment in which globalisation and interdependence have grown sharply? The timeless quality of international relations, its repetitious nature and cycles of war and conflict, and a world in which the strong do as they will and the weak do as they must, dominate the realist image (Viotti & Kauppi, 1999:86). Although it could be argued that this realist image does reflect an element of even the contemporary global security environment, the changes brought about by the information revolution and globalisation have resulted in some change in the international environment.

The state may still be the main actor in the international security environment as the nature of the state and the patterns of relations among states are the most important determinants of the

character of international relations at any given moment. This, however, does not presume that states always need to be the central actors, nor does it presume that the nature of the state always need to be the same and that the contemporary national state is the ultimate form of political organisation (Gilpin, 1984:302). Taking current trends into account, it is also increasingly possible that this dominance of the state is changing.

#### *2.3.1.5 Prospects for the realism worldview in the future*

The end of the Cold War and the increasing impact of globalisation have already brought into question if political realism does fully reflect the realities of the security dilemma now and especially the future. Even before the end of the Cold War, military power has been overtaken by other, “softer” forms of power in world politics (Nye, 1990a). Another subtle but increasing important aspect of power in the new era is the ability of a system, or society, to sense the need for change and to adapt (Gompert 1999:65).

This is not to say that all aspects of realism will prove to be non-applicable. Will the bases of power in terms of realism – namely military might, resources, population and level of development – remain deterministic factors that will ensure only slow change in terms of state capacity and ensuring equilibrium? The changing role of non-state actors and multi-lateral role-players remains a major factor impacting on the lack of realism’s capacity to address all concerns regarding new challenges posed to national security.

Realism became more responsive to criticism in the late 20<sup>th</sup> century to remain relevant with competing thoughts, by the further refinement of realism in terms of neo-realism<sup>5</sup> and structural realism<sup>6</sup>. Despite these refinements, it can still be postulated that to explain the role of information warfare in terms of national security in the future, it will not sufficiently fulfil that role but continue to highlight the significance of the role of power in international relations. Thus, while power is not the only driving factor in security relevant behaviour, it remains a significant factor underlying conflict in the international environment.

Keohane and Nye (2000) proposed complex interdependence as a new account of international relations to run alongside realism, and set out three key differences between the two approaches. First, complex interdependence assumes that there are multiple channels of access between societies, including different branches of state apparatus as well as non-state actors as opposed to the unitary state assumption characteristic of realism. Second, complex interdependence assumes that for most international relationships, force will be of low salience as opposed to the central role that force is given in realist accounts of the world. Finally, under complex interdependence there is

---

<sup>5</sup> Neo-realists recognise that economic actors are significant in the international system and are not just details on the edge of the serious matter of power politics (Nicholson, 2002:96).

no hierarchy of issues; any issue area might be at the top of the international agenda at any particular time, whereas realism assumes that security is everywhere and always the most important issue between states (Brown, 2005:35-36). Complex interdependence stipulates that states confront multiple issues simultaneously, not serially and sequentially. The hierarchical division of high and low politics posited by realism is supplanted by "... a horizontally defined agenda with multiple, conflicting, and interconnected trade-offs" (Kolodziej, 2005:155).

In terms of complex interdependence, states and other non-state actors cannot entirely separate their own interests from those with whom they closely interact. Actors may thus be sensitive to the acts of others to the extent that they feel the effects of those acts (Nicholson, 2002:98). This connects with the second broad view of international relations namely, rationalism.

### **2.3.2 The rationalist tradition**

#### *2.3.2.1 The central role of international cooperation*

According to Brown (2005:5), physical violence and overt conflict as manifestations of power projection are nowhere near as central to international relations as the traditional description of the subject would suggest. Brown said that most countries, most of the time, live at peace with their neighbours and the world at large. Such views are important for rationalism which provides an alternative broad explanation of international relations. In contrast to the realist views, rationalists are of the opinion that order is not maintained in the global system primarily only through states and the balance of power (McGrew, 1992:20). The discussion on realism pointed to the fact that the absence of a central government on the international scene creates a power vacuum, which is used by realists to explain the vital value of sovereignty and efforts by states to secure this sovereignty. Rationalists, however, argue that an element of order is maintained in the international society despite the absence of a central authority commanding overwhelming force and a monopoly of the legitimate use of it (Bull, 1992:590). Rationalists focus on international cooperation or the potential for such cooperation as the basis of their international relations worldview.

Rationalists argue that, as is the case in domestic society, order is maintained, *inter alia*, through commonly accepted values, a recognition of a high degree of interdependence between national societies, and the existence of accepted rules and norms of behaviour, as well as the existence of accepted institutions or processes of governance. Order is thus achieved and maintained through a complex web of crisscrossing governing arrangements which bind states and societies together (McGrew, 1992:20). However, there are also traits in modern international society that fall outside the structure of rules itself, encouraging the politically competent groups and elites to agree to these rules. These include mutual deterrence, fear of unlimited conflict, force of habit or inertia, and

---

<sup>6</sup> Structural realists are basically neo-realists who state in order to understand the behaviour of the international system, it would be necessary to start with the system and move down to the individual actors rather than the other way round as traditional realist

the long-term interest of elites in preserving the system of collaboration, whatever their short-term interest in destroying it (Bull, 1992:590-591). This shift away from power politics reflects not so much an idealist faith in abstract principles as the recognition that, when power is widely distributed, competition tends to be self-defeating. As a result rationalists tend to argue that, in an increasing interdependent world, the tendency towards cooperation and integration will ultimately prove to be irresistible (Heywood, 2002:130).

For the rationalists, the central cohesive element of international relations is the concept of international society. The idea of international society forms a powerful image of world politics. Its power derives from the wide and now general acceptance that a society of states or international society does actually exist. It underpins the idea of an international community with society and community often being used interchangeably (Wight, 1966:93). For Wight (1991:30), international society "... is *prima facie*, a political and social fact, attested by the diplomatic system, diplomatic society, the acceptance of international law and writings of international lawyers, and also by a certain instinct of sociability".

The image of international society is one in which states articulate and agree upon rules, based upon their mutual recognition as sovereign states of acceptable behaviour. It depicts states as acting in concert to achieve international order and as laying down criteria for the determination of which states are to be accepted as legitimate members of international society. Those that are so regarded are then entitled to be treated according to the norms and rules of the society. It is a view of political relations between states in which states are capable of creating and maintaining order in their relations (international order) without an overriding authority standing above them (Keal, 2000:61).

From the security perspective, one of the main implications of the rationalist view is that it impacts the central concept of sovereignty, which is a fundamental concept in the realist point of view. Based upon the primacy of a conception of unrestricted national sovereignty, the international system would not long have survived unless states actually accepted and acted upon a set of well-understood though limited and conditioned restraints. These limitations on state action, acknowledged by all (or at least most) governments as the price they pay for continued viability of the global system, are only partially formalised. They rest to a large extent upon tacit agreement and the force of practice (Said, Lerche [Jr.] & Lerche [III], 1995:135). If states violate a rule, they risk a countervailing and costly reaction from other states, potentially damaging to their interests (Kolodziej, 2005:159).

Globalisation has an impact on the traditional view of sovereignty. The capacity of each state to direct the political loyalties of its citizens has been weakened by an increasing popular awareness

of the problems faced by humanity. The state cannot prevent its citizens turning to a range of sub-national and transnational agents to secure their political identities and promote their political objectives. Sovereignty is no longer an automatic protection against external interference called “humanitarian intervention”. Decision making on a range of issues, including the security field, has become internationalised, rendering national administration often much less important than transnational political cooperation (Burchill, 2005:82). International cooperation or the potential for such cooperation can increasingly impact international relations and national security. Growing interdependence because of globalisation has strengthened the role of international cooperation.

Despite these changes, there are also counter-trends which can be identified. A number of important powers are retained by the state despite globalisation, including monopoly or control of the weapons of war and their legitimate use, and the sole right to tax its citizens. Only the state can still command the political allegiances of its citizens or adjudicate in disputes between them. It is still only the state which has the exclusive authority to bind the whole community to international law (Burchill, 2005:82).

It is not that sovereignty is totally negated by the rationalist scholars. It is, however, not regarded as the core foundation of the international system as is the case with realist viewpoints. Associated with sovereignty is the concept of national interest. In realist terms it is seen as attaining security by maximising power but in rationalist terms it is viewed as “an abstraction that summarises the perceived purposes of a certain state at a certain moment in time” (Bonkovsky, 1980:157). This view is broadening the scope and importance of international interaction and influences in developing the national interest but also boosted a shift from emphasis on human rights to that of social responsibilities.

For the international system to survive, the constant adoption of new technological, political and economic trends is necessary, according to rationalist views. The assumption flowing from this perception is that as the interactive processes grow and expand, and as individuals and groups increasingly interact across international frontiers, they will be more prone to adjust their differences rather than resort to conflict which might destroy the system (Holsti, 1980:25).

#### *2.3.2.2 The role of rules, international organisations and international law*

Any kind of sustained interaction leads to the development of rules that define roles and assign rights and responsibilities to them (Sandholtz, 1999:195). The function of rules is to provide a sense of common interests in elementary goals of social life and thereby to provide guidelines in international society as to what behaviour is consistent with these goals. The status of these rules differs and includes international law and moral rules based on prudence, etiquette or custom, or established practice, or they may even be merely operational rules or “rules of the game”, worked out without formal agreement or even without verbal communication. It is not uncommon for a rule to emerge first as an operational rule, then to become established practice, then to attain the status

of a moral standard and finally to be incorporated in a legal convention on international level (Bull, 1992:593).

Rules, however, do not stand alone; they are linked in clusters, or institutions. Organisations are the subset of institutions. International organisations were developed to serve as collective problem-solving entities but also bargaining forums (Sandholtz, 1999:196). The growth in the number of these international organisations reflects the general expansion of transnational links. The development of international and transnational organisations has led to important changes in the decision-making structure of world politics. New forms of multinational politics have been established and with them new forms of collective decision-making involving states, intergovernmental organisations and a whole variety of transnational pressure groups (Held, 1989:232).

Furthermore, rights and duties are recognised in international law, which transcend the claims of nation states and which, while they may not be backed by institutions with coercive powers of enforcement, have far-reaching consequences (Held, 1989:234). In the absence of a world legislature, international law draws on a number of sources: treaties, custom, general principles (such as respect for territorial integrity), and legal scholarship accumulated by the international courts. Traditionally, rationalists have placed a strong emphasis on international law, seeing it as a means of establishing order through respect for moral principles, which makes the peaceful resolution of international conflicts possible (Heywood, 2002:154).

The problem with information warfare as a security threat is that it is largely of an intangible nature. Industrial related threats, such as nuclear weapons, are tangible and do provide the scope for international cooperation because of the physical dimensions of this threat, namely highly radioactive material for which credible containment and management processes could be negotiated. This is not the case with information warfare. While rules and norms could be developed, the application thereof will be challenging. Countries such as the Russian Federation are campaigning for the creation of a disarmament/arms control related treaty covering this issue; this has not achieved any significant support (Johnson, 2002:442). The practical verification and monitoring mandated by such a treaty would be virtually impossible because of the nature of information warfare. The expected escalation of information warfare (see Chapter 5 for an overview of how information warfare has recently manifested globally) might thus place additional strain on the rationalist approach to develop global rules in terms of the control of this phenomenon. The active role that sub-national entities are playing in terms of information warfare will further complicate any such efforts.

### *2.3.2.3 Criticism of rationalism*

Despite endeavours to incorporate some of the challenges posed by the Information Age within the rationalist view (also the realist view), it remains difficult to account for all implications. Here,

information warfare opens up significant challenges such as the role of sub-national entities which can now seriously threaten global stability supported by global media coverage and the proliferation of social media. Information warfare makes it possible to attack a country geographically distant from the aggressor. Potential security threats transcending the traditional geo-strategic paradigms are becoming quite common. These traditions do not for example sufficiently provide the theoretical context for the two battle spaces of information warfare, namely cyberspace and mind space. Taking into account the rapid technological driven change of the past few decades with the likelihood of exponential change in the future, the realist and rationalist views' limitations are even more apparent.

#### *2.3.2.4 Critical realism in international relations theory*

The application of critical realism to international relations theory is related to efforts explaining complexity and the fast-paced global political, economic, technological and social transformation. In the mid-1980s, international relations theory moved into what is known as its post-positivist phase (Wight & Joseph, 2010:1). In recent years, Kurki (2008), Wight (2006), Patomäki (2002) and Roach (2013) have all made important theoretical contributions to international relations theory in this regard.

Similar to critical realism's work at the level of philosophical critique, it challenges some of the philosophical assumptions of contemporary international relations theory and in so doing it also introduces important epistemological and ontological insights in its own right (Wight & Joseph, 2010:1). Roach (2013:172) stressed the ongoing struggle to develop a relevant critical theory of international relations that can accomplish two aims: (1) explain the shifting empirical dynamics of governance, and (2) allow the understanding of the social genesis of norms and events/crises. He further argued that critical international relations theorists have made important strides towards realising and formulating the normative and social requirements of a critical theory of international relations.

Most critical realist philosophies of international relations accept the same basic principles in terms of the discipline. Such thinking maintains (or at least does not deny) the following views (Wight & Joseph, 2010:2-3):

- There is a social reality which consists of multiple forces that condition individuals' lives.
- Some of these forces may well be unobservable but remain real nonetheless.
- These forces are structured by forms of internal and external relations, power structures and social roles.
- It is not possible to capture the nature of causal forces in the social sciences merely through empirical investigation.
- Social and political sciences are fundamentally social and political in nature and reflect, in part, the inquirer's position in social reality.
- The interaction of agents, structures, material and abstract forces is a significant question to be settled empirically and not by theoretical determination.

The agent-structure problem is a much discussed issue in the field of international relations. A significant international relations and security causal insight is generated from critical realism. According to critical realism, structures and agents have distinct properties and powers. Social structures have visible but also deeper and invisible effects on activity. While structures may depend upon human actions for their reproduction, these actions are already conditioned by the structures in a way that the actors are seldom aware of. Therefore, the model proposed here is that agents act consciously within (positioned) practices, but that the effect of this is generally the unconscious or unintended reproduction of deeper social structures that the agent is largely unaware of (Wight & Joseph, 2010:20-21). The potential of social structures influencing behaviour is especially relevant in the domain in which information warfare takes place, which is constrained by the technological environment as well as the cyber-cultural aspects that influence behaviour.

The potential of social groups to transform society is also highlighted by critical realism. These powers and liabilities derive from the structural location of these groups and the powers and potentialities conferred upon them. Usually social transformation only takes place under exceptional conditions when structural crisis occurs. Moments of structural crisis tend to throw the process of unconscious reproduction into question, and change agents become more aware of the situation confronting them and the possibilities open to them. At the same time, if some agents may become aware of their transformative capabilities, then certain other agents will attempt to resist this. The process of transformation encounters resistance from those who have an interest in maintaining the structure as it is. They will engage in an act of conservation. Thus struggles will break out over transformation and the conservation of structures. These struggles can be called hegemonic struggles where agents, through their practices, act to preserve or transform a given set of relations (Wight & Joseph, 2010:21-22). Creating conditions for trust, fostering particular values and symbols, and forging collective identities and cooperation presupposes power and may create new resources for subsequent actions. On the other hand, domination and organised violence also presuppose power as transformative capacity (Patomäki, 2002:199). The influence of grouping using social media and information warfare techniques in order to advance their interests is a growing phenomenon (Chadwick, 2006:201).

An additional contribution to the debate around agents and structures has been the manner in which it highlights the impossibility of maintaining the disciplinary boundary between domestic and international politics. In fact, the agent-structure problem makes the breaching of disciplinary boundaries seem not only honourable but necessary. When viewed from an agent-structure perspective, the distinction between domestic and international structures seems untenable and agents are seen to be located within a plurality of structural constraints and enablements, some domestic, some international. Accordingly, the interests of agents can be seen to differ according to the agents' structural milieu, and since agents face differing structural contexts they acquire

differing identities and interests. In this respect, artificial boundaries between politics and international politics represent real barriers to analytical progress (Wight, 2006:292). The information and digital revolutions have transcended borders and are increasingly influencing one another.

Suganami (1997:149) stated that causation, narration and explanation are seen to be inextricably intertwined both in relation to events in nature and with reference to historical events in the social world. Kurki (2008:10) called for broadening and deepening the conception of cause at work in dominant strands of social science, and invoked Aristotle's Four Causes<sup>7</sup> as a more useful model to investigate. Kurki (2008:27) stated that critical realism can create more complex and plausible causal relationships by drawing upon the Aristotelian concepts of "formal" causes (ideational factors in the name of which social action takes place, such as discourses and ideologies) and "material" causes (the limits to what is socially possible set by the pre-existing material conditions in which social action takes place, such as resource availability). Layered views of causes can assist to obtain deeper insights into phenomena (Inayatullah, 2004:8).

#### 2.3.2.5 *Critical security studies*

Critical realism in international relations theory also contributed to the creation of critical security studies. The central aim of critical security studies, which emerged in the mid-1990s, is to develop an imminent critique of security policy and strategy; more concretely, to show how traditional mainstream approaches suppress cultural, social, historical and humanistic elements in international security (Roach, 2013:182). Here, the focus shifts to the role of states in oppressing populations. Nonetheless, as long as dogmatism and orthodoxy continue to exist, so too will the need for critical theory to expose the traits of these oppressive discourses in international relations (Roach, 2013:183). Globalisation results in two opposing outcomes in terms of security. It can open up emancipator struggles beyond the nation state while it can also challenge the development of solidarity and political unity which is necessary for promoting deliberation and/or deliberative democracy (Pensky, 2005:9). This includes addressing issues related to cyberspace and the implications of information technology for state power.

---

<sup>7</sup> In *Physics* II 3 and *Metaphysics* V 2, Aristotle offered his general account of the four causes. This account is general in the sense that it applies to everything that requires an explanation, including human action. Here, Aristotle recognises four types of things that can be given in answer to a why question:

- The material cause: "that out of which", e.g. the bronze of a statue.
- The formal cause: "the form", "the account of what-it-is-to-be", e.g. the shape of a statue.
- The efficient cause: "the primary source of the change or rest", e.g. the artisan, the art of bronze-casting the statue, the man who gives advice, the father of the child.
- The final cause: "the end, that for the sake of which a thing is done", e.g. health is the end of walking, losing weight, purging, drugs, and surgical tools" (Stanford Encyclopaedia of Philosophy, 2006).

Cyberspace is omnipresent in today's world and it has significant implications not only for global economic activity but also for transnational social relations and international relations. Theoretical focus also started to address the "cyberization" of international relations, the growing dependence of actors in international relations on the infrastructure and instruments of networking and the internet, as well as the penetration of cyberspace into all fields of their activities. The intricacies and broad meanderings of the relationship between information technologies and global politics are still being developed with the way the spread of information technologies is shifting power and the locus of authority away from the state (Singh, 2002:2).

Critical security studies can gain from some of the insights attributed to postmodernism, especially in terms of issues related to information<sup>8</sup> and the impact of information on politics and international relations.

### **2.3.3 Postmodernism in international relations**

#### *2.3.3.1 The information society in international relations*

Much of the political interest which is discussed in terms of international relations theory revolved around issues such as power politics, international society, and the contest over the distribution of the gains from the increase in productivity that capitalist industrialisation created. The Information Age created new challenges and rules pertaining to international relations, which have not yet from a theoretical viewpoint been fully taken into account by existing theory. Therefore, while international theory still needs to be developed and adopted to fully analyse the role and impact of information on the international relations field some direction can be found in postmodernist thought.

Postmodernism, however, poses theoretical challenges to the social scientist. These challenges are more related to form than to substance. In rejecting grand narratives, postmodernists are rejecting most of what is usually regarded as social science. Contrary to the realist and rationalist worldviews and to an extent also critical realism theory, postmodernists do not offer these grand narratives but rather fragments of ideas that often seem to contradict one another (Ritzer & Goodman, 2004:609). Furthermore, postmodernists are in general unwilling to define themselves in any precise way; consequently, there are many different strands of thought (Nicholson, 2002:117-118).

Postmodernists are critical of what they call "modernity". Modernity is used to describe the rise of notions of objective science. It is especially critical of the industrial revolution and the rise of technology. Postmodernists argue that modernity has made rationality an end in itself, and far from being a progressive force, this has resulted in outcomes such as the Holocaust and nuclear

---

<sup>8</sup> Information is organised and collated into sets of data in context (Hutchinson & Warren, 2001:1).

weapons. This is in part because the drive to find technical solutions to problems has largely sidelined moral and political questions (Nicholson, 2002:118).

Postmodernism actively seeks to upset what is taken for granted and to reveal how discourse imposes meaning and hence a value structure that is both socially constructed and historically arbitrary (Sterling-Folker, 2006:158). As a tool of social and political analysis, postmodernism highlights the shift away from societies structured by industrialisation and class solidarity to increasingly fragmented and pluralistic information societies in which individuals are transformed from producers to consumers, and individualism replaces class, religious loyalties and ethnic loyalties (Heywood, 2002:65).

Within postmodernism meaning is always assigned through an oppositional arrangement in which some symbols, ideas and values are elevated and others subordinated. Truth itself then becomes a function of this discursive oppositional arrangement. Individuals take for granted certain ideas and activities as naturally good or bad when such judgements are actually products of specific knowledge-producing systems and hence specific historical circumstances (Sterling-Folker, 2006:159). Postmodernism does not seek to replace the meta-narratives by utilising alternative methodologies, and in so doing, "... it accepts inconsistency and contradiction, feeling no need to reconcile opposition or to choose between them" (Rosenau, 1990:86).

Postmodernism delivers critical insight relevant to the theoretical perspective. According to postmodernism, social science is not neutral; rather, it is historical, cultural and political, and therefore biased. There is no neutral, impartial or independent standpoint to decide between rival empirical claims. Knowledge is not at all immune from the workings of power (Smith, 1997:165-190). These insights enrich and strengthen arguments for the potential impact of information warfare as a national security threat.

### *2.3.3.2 Criticism of postmodernism*

Before explaining specific insights obtained from postmodernism, it is necessary to caution against postmodernism as its relativism, which is a basis of postmodernism, poses some danger. Extreme postmodernism can result in paralysis seeing that certainty regarding all knowledge is challenged. There is, however, a moderate postmodernist view (similar to critical realism) that is premised on the notion that our ideas and theories about the world always contain elements of both subjectivity and objectivity. The subjective element is tied to an individual's adherence to different values and concepts and the inescapable fact that each and every person views the world from his or her own personal standpoint. The objective element is tied to the fact that people can actually agree on substantial insights about what the real world is like. This is aligned with critical realism, which is the point of departure of this study. Specific postmodernist thought relevant to the role of information warfare in society includes the insights offered by Stiegler (1998) and Baudrillard

(1983), which includes the concept of retention in the Information Age and the rise of signs, symbols and simulacra.

#### 2.3.3.3 *Retention in the Information Age*

With the advent of the information society, the transfer of knowledge and culture values between generations in particular are fraught with challenges. While institutions like culture, education and national entities responsible for this transfer are dynamic, in general, they maintain a similar in approach to methods used in the past. Stiegler referred to the concept of retention within the Information Age, which will result in fundamental and even exponential change between generations.

Stiegler referred to tertiary retention, which plays an important part in the creation of generations. Tertiary retention is experiences of people, selected by their culture and then distributed by their prevailing communication technology. As long as culture controls the tertiary retention, it is transferred within a society; however, control by the global market is increasingly globalising these transfers. One of the implications of the proliferation of information related technologies is that future tertiary retention will ensure that generations are much shorter lived but also much more fluid than in the past (Rossouw, 2002).

#### 2.3.3.4 *The rise of signs, symbols and simulacra*

According to Baudrillard's analysis of contemporary society, it is no longer dominated by issues such as production, but rather by the "media, cybernetic models and steering systems, computers, information processing, entertainment and knowledge industries, and so forth" (Kellner, 1989:61). Originating from these models and systems is an absolute explosion of signs. Society has moved from being dominated by the "mode of production" to one controlled by the "code of production". The objective has shifted from exploitation and profit to domination by the signs and the systems that produce them (Ritzer & Goodman, 2004:607-608).

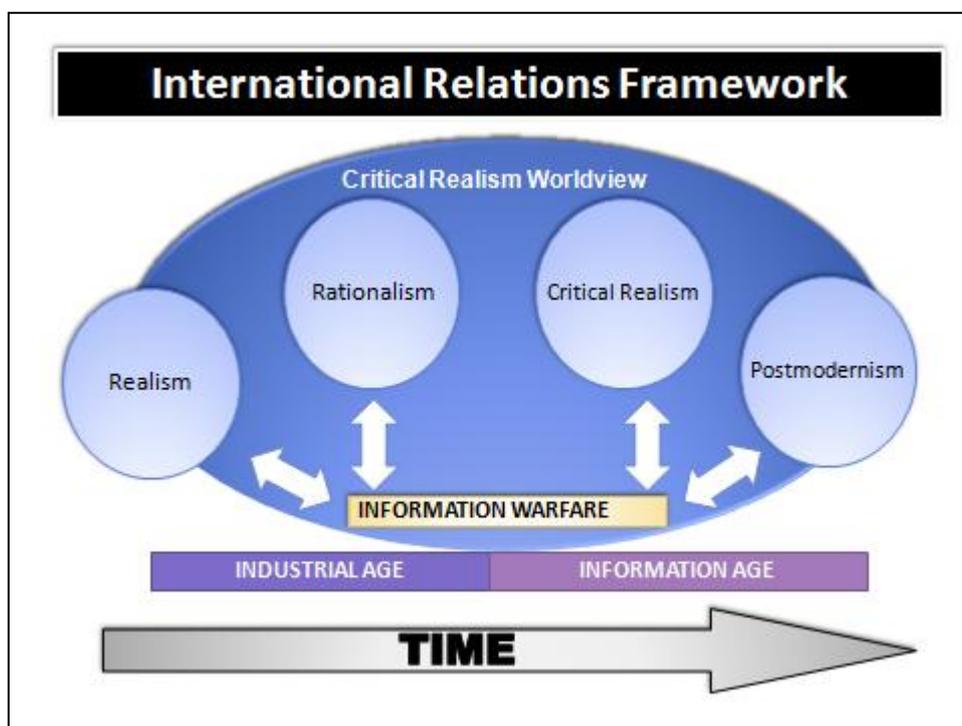
Accordingly, Baudrillard argued that since the late 20th century in "global" society the excess of signs and of meaning have caused a (quite paradoxical) effacement of reality. In general, people no longer believe in ideological worldviews such as liberal or Marxist utopias. Baudrillard argued that the world is currently easily petrified by even the smallest event. Baudrillard stated that as the "global" world operates at the level of the exchange of signs and commodities, it becomes ever blinder to symbolic acts such as terrorism. In Baudrillard's work the symbolic realm is seen as quite distinct from that of signs and signification. Signs can be exchanged like commodities; symbols, on the other hand, operate quite differently: they are exchanged, like gifts, sometimes violently, as a form of potlatch. Baudrillard, particularly in his later work, regarded "global" society as without this "symbolic" element, and therefore symbolically (if not militarily) defenceless against acts such as

the Rushdie Fatwa or even the September 11, 2001 terrorist attacks against the USA and its military establishment (Kellner, 2007).

The world is characterised by simulations, and Baudrillard (1983:4) declared that we live in “the age of simulation”. The process of simulation leads to the creation of *simulacra*, or “reproductions of objects or events” (Kellner, 1989:78). With the distinction between signs and reality imploding, it is increasingly difficult to tell the real from those things that simulate the real. For example, Baudrillard (1983:55) talked of “the dissolution of TV into life, the dissolution of life into TV”. Eventually, it is the representations of the real, or the simulations, which become predominant. Society is in the thrall of these simulations, which “form a spiralling, circular system with no beginning or end” (Kellner, 1989:83). With the advent of social media the dissolution of life into the internet has become a potential challenge for modern times. The potential for manipulation of these *simulacra* remains significant, and with the exponential development of technology coupled with social media they become a growing potential threat to society.

#### 2.3.3.5 International relations theory and information warfare

An integrated view of international relations theory’s macro relationship with information warfare is illustrated in Figure 2.1. Insights relevant to the manifestation of information warfare obtained from these different theories include: the centrality of power, the growing influential role of networking in international relations, complex and multi-layered transformation of the domestic and international society, the increased influence of non-state actors, the dynamics of future tertiary retention as well as growing significance of symbolic, information-related phenomena which are increasingly impacting on the real world.



### **Figure 2.1: International relations framework influencing information warfare**

These insights are, however, also linked to the macro historical environment. In the Industrial Age, realism was closely linked to the Cold War global political stand-offs, while rationalism focused on efforts to expand international political and economic relations within the global community (Smith, 2013:4). Information Age concerns, as described by critical realism and postmodernism, reflect increased diversity, inconsistency and contradictions in human activity. These Information Age related theories highlight some trends relevant in human activity, namely renewal, relationship shifts, modernisation, continuous modernisation, growing complexity and interconnectness. The dominance of any one theory is the result of a prior assumption about the main issues in world politics that need explaining. However, all of these theoretical insights play a role in assisting the systematic reflection on information warfare in its global context.

## **2.4 CONCLUSION**

As information warfare is a relatively new concept, it has not been fully addressed in a social science theoretical framework. In this chapter critical realism is proposed as the overarching theory framework within which international relations theory and philosophy are proposed as providing the main body of theoretical insights relevant to the manifestation of information warfare as national security threat. The futures study theoretical elements are addressed in the next chapter.

The realist worldview explains many of the national security threats related to national security during the Industrial Age. Maximising power without any consideration for the interests of other states was part of catastrophic conflicts during the 20th century. The rationalist worldview acknowledges the existence of an international society sustained by the role of growing international interdependence and integration as a reality closely interlinking states globally. Cooperation between states facing up to national security related issues is part of this worldview but at the same time the scope of national security threats expanded to include issues such as the environmental and human security.

The start of the Information Age, globalisation and the explosion in ICT development, however, also opened new dimensions in the national security perspective. Critical realism in international relations theory and postmodernism provide some insights into the significance of the manipulation of the global information sphere. This is done by creating opportunities for information warfare to exponentially grow from a still upcoming issue in terms of national security to becoming a substantial national security threat in the future.

Thus all of these worldviews add value to the understanding of the broader framework within which information warfare manifest as a national security threat. Elements of realism, rationalism and critical realism in international relations theory as well as postmodernism can be used to provide

insight into the manifestation of information warfare. While realism was the dominant worldview during the Cold War, the other views also became prominent since then.

These worldviews are not representing completely mutually exclusive perceptions about international relations and security but are highlighting diverse insights regarding the role of information warfare in international security relations. While these worldviews provide insights into the context of information warfare as national security threat, it is probably not sufficient to systematically explore its possible medium to long-term future manifestation. Futures studies as an instrument of foresight is the focus of the next chapter.

## CHAPTER 3

### FUTURES STUDIES AS AN INSTRUMENT FOR FORESIGHT

#### 3.1 INTRODUCTION

Futures studies is a relatively new emerging discipline endeavouring to develop a future consciousness as well as seeking a systematic and pattern-based understanding of the past and present with the aim to determine the likelihood of future events and trends (Princeton University, 2015). Thinking about the future has been part of the human civilisation since the earliest times. De Jouvenel (1967:40) described humankind as beings who need the future and subsequently strive to form adequate images of future realities (*future*) that inhabit the future domain.

Futures studies as a focused intellectual exercise directed at the future is, despite its historic roots, a much more recent phenomenon (Bell, 2007:6). The basis of futures studies is diverse and includes the earliest science fiction writing, strategic planning during and after the Second World War, the centrally planned development strategies of states and think tanks' initial work on future challenges. All of these diverse strands resulted in the development of futures studies as field of study. Futures studies provides a unique perspective on the social sciences. It provides an opportunity for researchers to create useful information about the future, especially in the light of constant change, instability and uncertainty (Kristof, 2006:263).

The topics and methods of futures studies include the possible, probable and preferred variations. Futures studies covers a broad field of inquest and combines the insights of a range of disciplines to provide a fresh outlook on the future. While futures study methodologies are not necessarily going to stop policy mistakes from being made, they do provide individuals and entities with the capacity to think about the future in a more structured and focused way (Van Vuuren, 2011:240).

Traditional disciplines have a *doxa* – a certain collection of classic, acknowledged texts that must be read and that explain the basics of the discipline. Futures studies in general and futures research in particular largely still lack a *doxa* and clear boundaries. Futures studies is multi-disciplinary in its research approach and trans-disciplinary in its intellectual tradition with only fairly recent efforts to have a knowledge base defined (Inayatullah & Wildman, 1996:725). These challenges call for a brief evaluation of time perceptions, the rationale of futures studies, the manifestation of the future, the role of foresight, the systems approach within the discipline, the role of futures maps and the layered approach, especially causal layered analysis (CLA).

The future is not specified or prearranged. A multitude of futures are possible but only one can manifest in the end. Futures studies promotes enquiry on how current activities (or lack thereof) will become the reality of the future. This includes endeavours to analyse the causes, sources and patterns of stability and change with the intention of creating foresight and even different futures.

### **3.2 TIME PERCEPTION CHALLENGES TO FUTURES STUDIES**

Time, like space, is an inevitable aspect of individual experience and social interaction. Everything occurs at some time and in some space. Although at quite different rates, nearly everything changes from one time to another (Bell, 2007:5). Conceptions of time and the future also exist in every known society (Bell, 2005). While the understanding of time and future differs from culture to culture, some general observations can be made about time.

The differences between the past, present and future are important, but these three views of time are also significantly interconnected. Human understanding, focus and perception in the present are affected by the history, achievements and identity of the past. This, in turn, influences planning, projects and future aims. As the flow between these connections is multidirectional, such links are even strengthened. Many decisions that are taken are influenced by both the past and future. These decisions arise partly from the historical and cultural paradigms in which the decision-makers find themselves. Consequently, the boundaries between past, present and future are, in reality, open and fluid. In practice, this indicates that the decision-maker is not necessarily trapped in a constricted present, but there are other resourceful and intellectual choices, which require easy and relatively unrestricted movement between past, present and future (Slaughter, 2005a). Thus, even without a specific futures orientation, the future inevitably plays a role in decision making.

Although futures studies established itself in the intellectual and practical milieu globally, it experiences significant perception challenges. While one would expect exponential technological progress, growing networking and globalisation to enhance the popularity and use of futures studies to develop futures-orientated strategies, the contrary is sometimes more prevalent. Futures-orientated thinking is sometimes negated by the very developments directly related to the high level of advancement globally. According to the Clock of the Long Now Project's summary: "Civilization is revving itself into a pathologically short attention span. The trend might be coming from the acceleration of technology, the short-horizon perspective of market-driven economics, the next-election perspective of democracies, or the distractions of personal multitasking" (Brand, 1999:2). Ironically, as humankind is facing more and more challenges, short-term thinking remains prevalent. Fortunately, significant work has been done theoretically as well as practically in all human endeavours focused on the future and the implications of the future.

### 3.3 THE RATIONALE FOR FUTURES STUDIES AND THE ROLE OF THE FUTURIST

Futures studies is primarily concerned with the understanding of the social constructs that shape the future and the development of viable forward-looking views to inspire and lead societies and organisations (Slaughter, 1999:305). Bell (2007:73) defined the purposes of futures studies as follows: “The purposes of futures studies are to discover or invent, examine and evaluate, and propose possible, probable and preferable futures.” Futures studies can be undertaken at different levels. This includes at a superficial level extrapolating trends, at a pragmatic level which tends to be quite empirical and focused on particular problems, or at deeper epistemological or critical levels focusing on the assumptions that frame particular worldviews (Slaughter, 1999:145). The focus in this study is ultimately on a practical level, but initially attention is directed to the broader practical and theoretical framework in which futures studies function.

The question remains as to whether futures studies provides a unique set of methodologies for knowledge creation, which could be of value for the policy-maker and individual in general in order to counter the mentioned short-term approaches. Before proceeding to the theoretical and practical application of futures studies, it is important to distinguish futures studies from the futurist element present in most social sciences. Bell (2005) identified a number of specific futures assumptions that, although some may be shared by other fields, taken together, are a distinctive part of the futures studies perspective:

- *“Time moves unidirectional and irreversibly from the past (seen in terms of a continuous momentary present) toward the future. There are a number of different arguments that support this assumption, such as: biological development (people grow older with time, never younger); the second law of thermodynamics (entropy always goes in one direction); wave motion (radio waves, for example, are never received before they are sent); the history of the universe (residual galactic radiation supports the idea that time has a beginning, sequence, duration, and direction); and traces of the past (the fossil record remains in the present as evidence of the past).*
- *Not everything that will exist has existed before or does exist now. Thus, the future may contain things that have never existed before. These may invite new thoughts, new understandings, new developments and new reactions.*
- *The future is not totally predetermined. This assumption explicitly recognises the fact that the future does not already exist. The future is thus still ‘open’.*
- *Futures thinking is essential for human action. Reaction might be possible without futures thinking, but not action, because to act requires anticipation. Thus, images of the future (goals, objectives, intentions, hopes, fears, aspirations) are part of the causes of present action.*
- *To some extent, future outcomes can be influenced by individual and collective action, and by the choices people make.*
- *Global interdependence invites a holistic perspective and a multidisciplinary approach. Futurists view the world as so interrelated that no system or unit can be viewed as*

*totally isolated. Rather, futurists argue that every unit that is the focus of futures research should be considered to be an open system.”*

Expanding on these assumptions, Slaughter (2005) identified four key rationales for a futures approach:

- *Some decisions have long-term consequences.*

When following a futures consciousness approach it has significant implications for decision-making. Each decision made implies a potential change in direction with potential noteworthy future consequences. Some decisions are trivial and turn out to be insignificant in the context of larger events, while others are strongly conditioning the present and the future.

- *Future alternatives imply present choices.*

As humans become conscious of diverse future alternatives, it is possible to gain access to new preferences in the present. Should an unacceptable futures scenario be detected appropriate action can be taken to avoid this. Similarly, if a preferable future scenario is identified, action can be set in motion with the view towards creating it. The possibility of future alternatives implies present choices, because it takes time to focus effort on and mobilise the resources involved to achieve a particular outcome or avoid undesirable consequences.

- *Forward thinking is a preferable alternative to crisis management.*

While it is not possible to predict the future state of affairs of social systems, it is possible to take a strategic view, to explore alternatives and options, to anticipate eventualities, and to prepare for contingencies. Forward thinking is a structural alternative, especially for societies in transition. This remains preferable to crisis management as the latter is wasteful and expensive.

- *Further transformations are certain to occur.*

The potential changes over the next 100 years are probably as significant, if not more significant, than those which have occurred over the last 1 000 years. This is especially the case with assessments of the role of technology in future development. Technological change is no longer merely linear but increasingly exponential (Kurzweil, 2006:12). However, it must be made clear that the future is a mental construct. On a basic level it derives from the way humans interpret the past and the present. The future also drives action. Humanity's individual and collective actions are not reacting in a one-on-one fashion to incoming signals. Instead, available cognitive systems intermediate, and the mental constructs that are called “futures” play an important part in this process (Van der Heijden, 2004:208).

In understanding the assumptions and rationale of futures studies, the role of the futurist needs to be defined. Thuraisingham (2005) defined the futurist's role as strategic, namely one of contributing to and adjusting the belief systems, worldviews and paradigms of our society.

Bell (2007:238) took this further by stating: "Futurists focus on the transformation of hindsight into foresight. On the one hand, they speculate, think laterally, intuit, reason counterfactually as well as factually, cogitate linearly and dialectically, entertain outrageous – and even despised – notions, and creatively invent in order to unveil possible and probable futures. On the other hand, they specify past and present data using a multitude of standard and special methods, collecting, analysing, and interpreting evidence in order to make posits about possible and probable futures and to construct surrogate knowledge as reliably and validly as they can. Their candidates for surrogate knowledge of the future are based on patterns of reasoning and marshalling evidence, and they can become justified belief if they remain unrefuted after being subjected to serious efforts to falsify them."

Expanding on why the futurist should be performing these tasks, Bell (2005) identified the maintenance or improvement of the welfare of humankind and the life-sustaining capacities of the earth itself as a major purpose of the futurist. Futurists do this by systematically exploring alternative futures. Engaging in prospective thinking is an important part of this task to create new, alternative images of the future – visionary explorations of the possible, systematic investigation of the probable and moral evaluation of the preferable. Some futurists strive for more than institutional change by focusing on consciousness change (Inayatullah, 2008b).

Futures thinking is based on three interrelated inquiries into the future with the objective to determine the truth about the future (Spies, 2015). These inquiries are: (1) measuring the future to obtain knowledge about the future; (2) imagining the non-existing future; and (3) purposefully designing or making the future. Measuring, imagining and making sustainable alternative futures should be the preferable outcome of holistic futures thinking, and requires active interventions to realise. This study is primarily focused on the measuring and imagining dimensions.

### **3.4 FORESIGHT AS AN OUTCOME OF FUTURES STUDIES**

Despite many futurists agreeing on the rationale, role and aims of futures studies, approaches to futures studies differ significantly.<sup>9</sup> The approach to futures studies in this study is trans-disciplinary and action-orientated. The attainment of foresight remains a core principle.

When focusing on knowledge of the future, more than one term can be used. Since the meanings of these terms do differ, it remains important to distinguish between the concepts of prediction, forecasting and foresight in order to understand the boundaries and limitations of futures studies.

Humans have an instinctive competence for speculation, prediction, foresight, modelling and deciding between alternatives as humanity is not trapped in a deterministic world (Slaughter, 1994:1078). With astrology and prophecy being given less credence in the modern world, forecasting has become the preferred technique of planners, economists and social scientists (Inayatullah, 2005b). A forecast is a prediction or estimate of an actual value in a future time period (Armstrong, 2001:783). Stated differently, a forecast is a declaration of what is expected to happen in the future, especially in relation to a particular event or situation (Saffo, 2007). Forecast, prediction and prognosis are typically used interchangeably (Armstrong, 2001:783).

The aim of forecasting is based on an implicit desire to make the world more stable and to influence or even control the future. The assumption behind forecasting is that with more information, particularly more timely information, decision-makers can make wiser decisions. Having more information at hand is especially important presently since the rate of technological change has dramatically increased (Inayatullah, 2005b). Forecasting is thus a significant tool for use in planning. However, planning and forecasting are not necessarily intertwined. Planning is concerned with what the world should look like, while forecasting is about what it will look like (Armstrong, 2001:2). Planners can use forecasting methods to predict the outcomes for alternative plans. If the forecasted outcomes are not satisfactory, they can revise plans, then obtain new forecasts, repeating the process until forecasted outcomes are satisfactory (Armstrong, 2001:2-3).

The term foresight, which is generally used in futures studies, takes forecasting further. Foresight is the capacity to think ahead and consider, model, create, and respond to future eventualities. It encompasses the process of developing a range of views on possible ways the future could develop, and understanding these sufficiently well to be able to decide what decisions can be taken today in order to create the best possible tomorrow (Horton, 1999:6). Slaughter (1995:1) stated that foresight is not the skill to predict the future: "It is a human attribute that allows us to weigh up pros and cons, to evaluate different courses of action and to invest in possible futures on every level with enough reality and meaning to use them as decision making aids ...The simplest possible definition [of foresight] is: opening to the future with every means at our disposal, developing views of future options, and then choosing between them."

According to Slaughter (1995:48), foresight is a competence or a trait. It is a process that endeavours to widen the boundaries of perception in four ways, namely by:

- Identifying and avoiding problems before they transpire (guidance and early warning);
- Assessing the implications of present decisions, actions and events (consequent assessment);
- Taking into account the current implications of possible future events (pro-active strategy formulation); and

---

<sup>9</sup> See for example the diverse views of 108 futurists on future study methods and visions in Volume 2 of the *Knowledge Base of Future Studies* (Inayatullah, 2005b).

- Envisioning aspects of wanted futures (normative scenarios).

Successful foresight requires three consecutive stages: Stage 1 consists of the collection, collation and characterisation of available information, and results in the production of foresight knowledge. Stage 2 comprises the conversion and elucidation of this knowledge to produce comprehension of its implications for the future from the particular point of view of a specific environment. Stage 3 comprises the assimilation and evaluation of this understanding to generate a commitment to action in a particular environment (Horton, 1999:6).

Some individuals challenge the viability of prediction, forecasting or foresight. These individuals are of the opinion that the very idea that someone can predict the future or have foresight, let alone shape the future, seems absurd. Hence, they regard the future as a random occurrence of events – unknowable and untouchable until these events occur, and only fully understood in hindsight (Canton, 2007:8).

In terms of prediction, it is possible to agree with these assertions as the complex nature of change means that predicting events is in many cases impossible, and is quite likely to be dangerous, as it entails inflexibility. This implies the need to become locked into one specific prophecy (Van der Heijden, 2004). However, knowledge about factors shaping the future is possible. What is needed is finding insight and understanding about the things and patterns shaping the future, and their possible consequences for the future. The development and nurturing of foresight, namely the ability to make decisions that are good not only now but also in the long run remains a priority (Roux, 2006: Slide 25). Foresight is the process of developing a range of views on possible ways the future could develop, and understanding these sufficiently well to be able to decide what decisions can be taken at present in order to create the best possible future (Horton, 1999:5). In this study the identification of four plausible scenarios how information warfare possibly might manifest by the 2030s rest upon foresight and knowledgeability.

Foresight can act to promote knowledgeability in humans. As such, it operates as a “higher-order” language. Truly understanding the present is part of such a knowledgeability. Acknowledging that many of the prior actions of foresight have served the interests of those in power is also part of such a knowledgeability. This includes the understanding that language and technology should not be regarded as neutral, and endeavouring to view the present outside the confines of a short-term approach. Instead of seeking stability, understanding surprise, limits, disturbance, consciousness and transformation is likewise an element of such knowledgeability. Noting the bias of many institutions against foresight is also part of such knowledgeability (Hayward, 2005).

### **3.5 SYSTEMS APPROACH**

As indicated in Chapter 2, critical realism served as overarching theory for this study. Similarly, a futures philosophical approach in general also subscribes to a critical realist worldview which

concur with the notion that the absolute truth of knowledge is untenable. In this regard critical realism can provide a satisfactory philosophical approach for the study of information warfare in a futurist context. While science is regarded as a body of linguistic or numerical statements about the nature of reality, this also includes an interest in the activities of scientists and the history of science and its institutions (Bell, 2007:207).

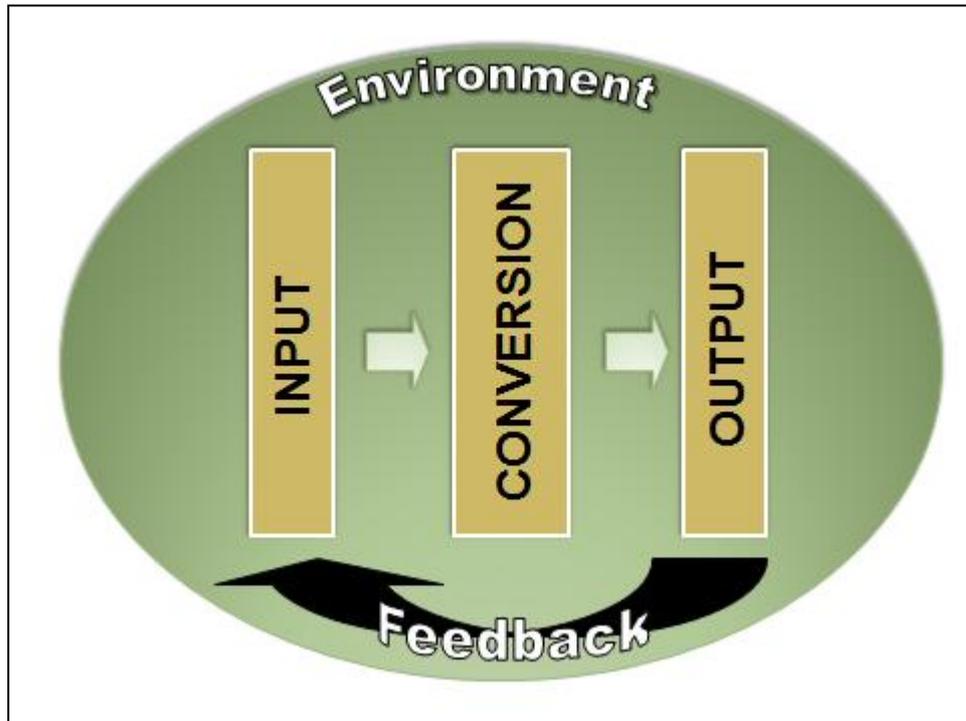
Critical realism accepts the sceptical belief that humanity cannot have certain knowledge, if we define knowledge as justified true belief. However, nor can humanity abandon efforts to know and understand. Knowledge is redefined as “conjectural knowledge”, allowing for the possibility of the fallibility of these conjectures (Bell, 2007:210). Popper (1962:37) argued that science must have a falsifiable hypothesis. He stated that the measure of the scientific status of a theory is its falsifiability, or refutability, or testability. A critical realist view assumes both that there is a reality that exists and that humanity can test many hypotheses about it to see whether they are most likely true or false (Bell, 2007:207-208).

The insights produced by critical realism are enhanced by the international relations worldviews evaluated in Chapter 2, especially where these worldviews have implications for the analysis of the phenomenon of information warfare as a future national security threat. These worldviews showed that the relationships between all social entities and their environments are the source of complexity and interdependence. The challenge is that traditional analytical approaches to societal problems in general tend to ignore this dynamic nature (Dostal, Cloete & Járos, 2007:12).

In order to accommodate these dynamics, especially when possible futures are investigated, a systems approach offers a solution. Systems theory can serve as a useful instrument to identify the dynamics playing a role when information warfare as future national security threat is studied. Currently and even more so in the future, systems thinking is needed because humanity is becoming overwhelmed by complexity. As Senge (1990:69) put it: “Perhaps for the first time in history, humankind has the capacity to create more information that anyone can absorb, to foster greater interdependency than anyone can manage, and to accelerate change far faster than anyone’s ability to keep pace.” Systems thinking provides an opportunity to delve into any problem on different levels of complexity.

A system can be defined as a set of interacting units. At one level, a system consists of a structure, and the structure is the systems-level component that makes it possible to think of the units as forming a set, distinct from a mere collection. A system thus consists of interacting units (Waltz, 1979:40). A system remains a discernible whole that interacts purposefully with its environment and is comprised of interacting and interrelating parts that are organised for a purpose (Dostal, 2007). See Figure 3.1 for a representation of a simplified model of a system in the context of a society.

Connections are being established and broken within and among systems, keeping the world in a state of constant change (Cornish, 2004:49). Any system also consists of parts, which are systems themselves, which can be referred to as sub-systems (Dostal, Cloete & Járos, 2007:7). Systems in this context refer to constructive rather than natural systems (Young, 1967:31).



**Figure 3.1: A simplified model of a system in the context of a society**

Source: Own compilation based on Easton, 1965:32.

To create a futurist relevant theoretical perspective, the logic of a systems approach is especially useful in order to assist in the analysis of the varied relationships of the many aspects of the social world, thus operating against piecemeal analyses of the social world. The systems approach tends to regard all aspects of socio-cultural systems in process terms, especially as networks of information and communication (Ritzer & Goodman, 2004:314-315). Systems thinking is a dominant worldview of the Information Age as information is now abundant and synergistic. Such synergy provides competitive advantages, while information also allows win-win solutions. Information introduces complexity to the world while it also drives technological development (Dostal, 2007: Slide 6).

Systems thinking is therefore a way of seeing and understanding how the world is organised and how people behave in it. A systems perspective highlights important patterns and relationships which if not viewed through a systems perspective may seem to be insurmountably complex and chaotic (Robinson, 2005). Systems thinking implies that there are two types of complexity, namely the detail complexity of many variables and the “dynamic complexity” when “cause and effect” are

not close in time and space and obvious intentions do not produce expected outcomes (Senge, 1990:364).

The systems approach can suggest the sort of things to expect, providing a useful way to understand what is happening in the world around us, especially as it focuses attention on relationships rather than on things. These relationships tend to shape events more than the things themselves (Cornish, 2004:49). Of especial importance is that a systems approach assists in understanding relationships that exist across space, time and domains (Cornish, 2004:50). On a macro level, there are essentially two systems – one of nature and the other being the world that interacts with nature. At a meta-level, systems thinking is holistic thinking whereby it is endeavoured to understand the world in all its diversity as being essentially interconnected and whole (Robinson, 2005). Of specific interest for this study is the interaction between human social systems, especially related to power within the system.

Social systems have a history and are in constant motion, evolving through time. Humans are positioned in these social systems, and these social systems influence human behaviour but are also influenced by human behaviour. In terms of a systems approach there is an appreciation of dynamic interaction not reducible to reified and static categories of social life and structure, a contrast to orthodox social science, which is founded on social facts that stand on their own with claims to general universality. Social reality is understood as a dynamic and systemic phenomenon (Flood. 2001:140).

Velamoor (2005) provided a summary of the systems approach, focusing on the various elements as follows:

1. **System:** This framework views humanity and its environment as major constituents of a hierarchical system comprised of sub-systems and sub-sub-systems that are interacting continuously, both vertically and horizontally.
2. **Control:** An underlying principle of such a system is that not any part of an internally interactive system can have unilateral control over the remainder of any other part.
3. **Symbiosis:** Symbiosis has shaped the features of many structures. It represents the union of two or more structures and yields what is, in essence, a new structure. This is applicable to entities within systems.
4. **Stability:** The tendency in evolution has been to establish stratified stability. The stratification of stability remains fundamental in dynamic systems, and it explains why evolution has a consistent direction in time.
5. **Punctuated equilibrium:** Evolution does not need to be regular but can be staggered or result in interrupted equilibrium. Punctuated equilibrium refers to stasis interrupted by brief bursts of evolutionary change.

6. **Non-linearity:** Linearity, locality and immediate cause and effect have been conveniently used as the fundamental assumptions in pursuing reductionist science, explaining the remaining unexplainable as chance. In modern terms, the Western perspective has regarded nature as a linear phenomenon in which what happens at a given place and time is determined exclusively by what has occurred in nearby places immediately beforehand. The holistic view assumed nature to be non-linear so that non-local influences predominate and interact with one another to form a complicated whole.

The systems approach is introduced to highlight the critical role of systems' elements such as the hierarchy of systems, the problem of control, symbiosis, stability in systems, and non-linearity; all elements relevant to later understand the complexity associated with the manifestation of information warfare. Within the context of exponentially increasing complexity due to the ubiquity of information, a systems theory approach is the only way to overcome complexity.

Using a systems approach, a futures map can be created within which possible future scenarios can be presented. This is also a popular approach applied to long-range planning in order to produce a roadmap that shows the path to the future (Smith, 2005:1).

### 3.5.1 Futures map

A futures map provides a conceptual frame that helps to evaluate how futures researchers have proceeded in the promotion of the purposes defined by Bell<sup>10</sup> and formulated by Spies (2015) as measuring, imagining and designing the future.

Malaska and Virtanen (2009:68) have introduced the concept of a futures map as follows:

*“... a map is a source of information about the scenery, a symbolic replica of some characters of it. There is a relationship between the map's designs and symbols and the real scenery at some level of coarseness and vagueness ... In geographical mapping the elementary symbols and patterns of the map represent different elements of the scenery, e.g. trees, lakes, meadows...In the same way a futures manifold (or map) is a symbolic representation of the future...”*

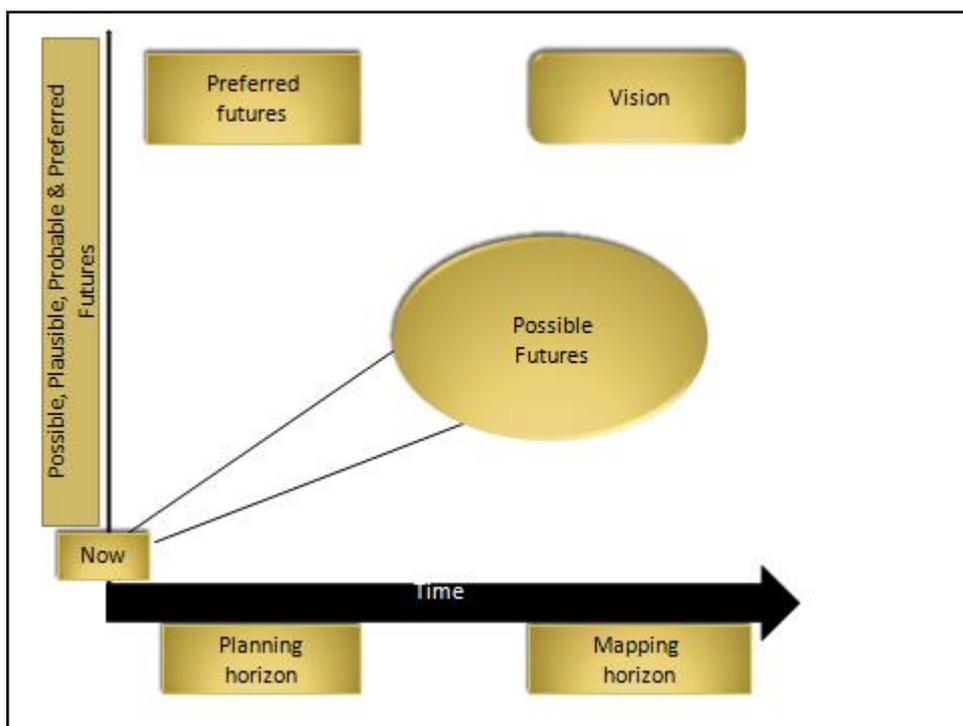
A futures map is a generic design of the various futures and a symbolic representation of what might unfold or be comprehended by human interventions in the material world (Malaska & Virtanen, 2009:69). A futures map is thus the all-inclusive description of the outcomes of a futures research process. It comprises all applicable pictures of the future identified during the process and all relations between these pictures and between them and the present state as well as assessments about the time frames, desirability and possibility of these pictures (Kuusi, Cuhls & Steinmüller, 2015:61).

---

<sup>10</sup> Wendell Bell (2007:73) defined the purposes of future studies as follows: “The purposes of future studies are to discover or invent, examine and evaluate, and propose possible, probable and preferable futures.”

In a futures map the mapping horizon refers to the scenario options which might be relevant during the future, while the planning horizon is linked to a proposed roadmap to the future (Kuusi, Cuhls & Steinmüller, 2015:61). See Figure 3.2 for a graphical presentation of a futures map.

The futures map will be especially appropriate for the global security environment as it is undergoing a qualitative change resulting in higher complexity. This necessitates changes in decision making culture, especially related to taking a more proactive approach and enhancing the networked nature thereof. Here, the futures map provides a visualisation tool, which can leverage numerous internal and external contributors, driving a “strategic conversation” across all levels, and linking strategy, intelligence and learning (Heathfield, 2008:596).



**Figure 3.2: Futures map**

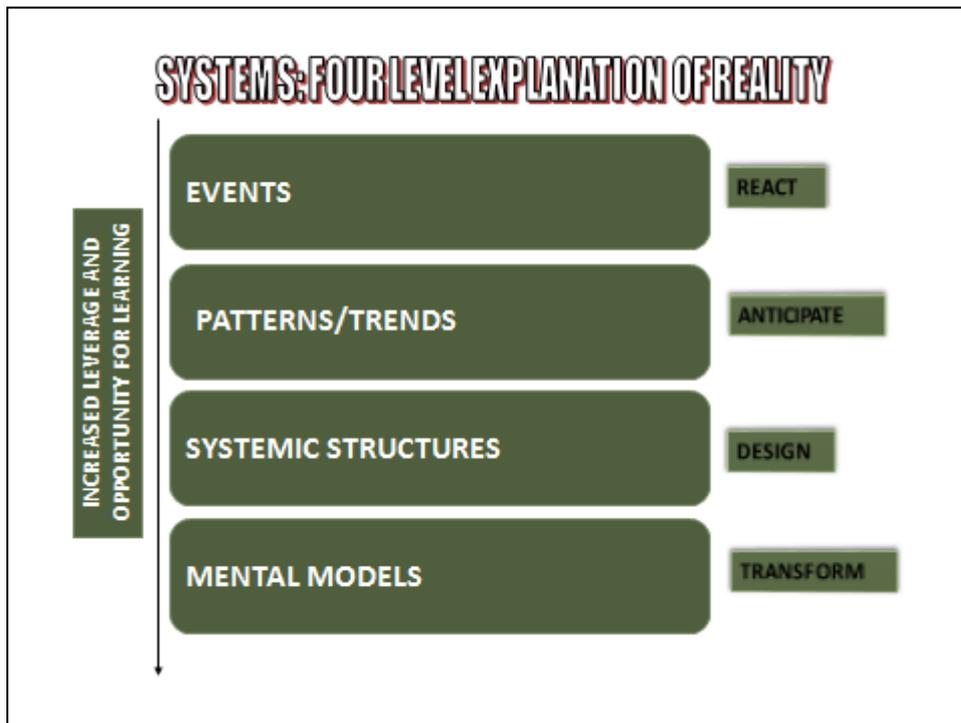
Source: Kuusi, Cuhls and Steinmüller, 2015:63.

An additional analytical element from the systems perspective is to not only focus on the horizontal dimension, but to also take into account the vertical complexity of systems. In terms of the vertical dimension a layered view of systems proves to be constructive.

### 3.5.2 Layered systems approaches as analysis tools

Senge, Smith, Kruschwitz, Laur and Schley (2008:173-176) proposed a four-level systematic explanation of any issue. The first level identifies a specific event or concern. The second level goes beyond the immediate event by viewing the event in a longer timeframe. The focus is on

identifying the patterns or trends within which the event occurred. The third level looks at the deeper forces driving these patterns or trends. This is the systemic structures which are underlying the dynamics driving the trends and patterns. The fourth level refers to the mental models, which is the core thinking within the system, especially related to the authoritative granting of values by the decision-makers within the system (see Figure 3.3).



**Figure 3.3: Layered systems explanation of reality**

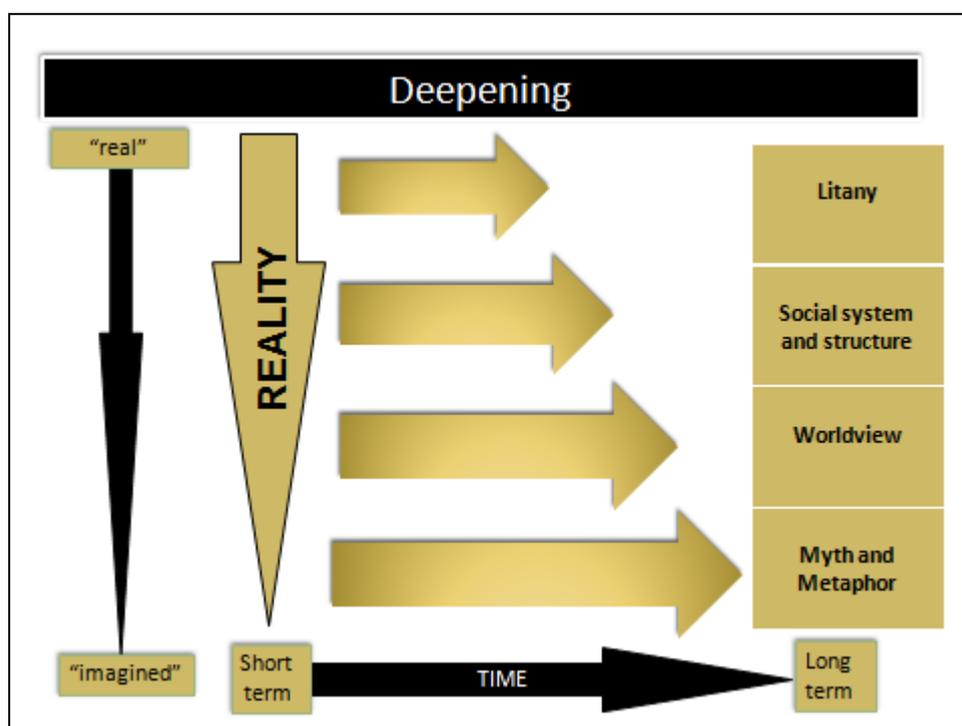
Source: Senge, Smith, Kruschwitz, Laur and Schley, 2008:174.

In terms of information warfare, a layered systems approach allows for the translation of events into their broader patterns and trends. This will provide the opportunity to move away from the need to immediately react to a representation in which the ability to anticipate events will be stronger. Going down one more level puts the focus on the systemic structures underlying the manifestation of information warfare. This provides an opportunity for insight into the underlying dynamics influencing the manifestation of information warfare as well as the ability to design possible futures. On the next level, the view is on the mental models underlying the manifestation of information warfare. Understanding the mental models assists even in the transformation according to which the future can be narrowed to the preferred. These insights are particularly of value to conceptualise a model that will enhance knowledgeability in terms of the future manifestation of information warfare.

### 3.5.3 Causal layered analysis

The four-level system explanation of reality already provides a basis for using a layered approach to the analysis of information warfare. In this regard, a complementary futures-orientated layered

method that can add value is causal layered analysis (CLA). CLA is a method to categorise concerns about futures and/or different views, and then to use these concerns to assist thinking about futures far more productively (World Future Society, 2005:4). See Figure 3.4 for a representation of CLA.



**Figure 3.4: Causal layered analysis (CLA)**

Source: Inayatullah, 2008c:1.

According to CLA, the mode in which a problem is framed changes the policy solution as well as the actors accountable for creating change on the way to find a solution to the problem. CLA presupposes that there are different ways of viewing and understanding reality and assists in identifying trends. CLA is made up of four levels of knowing, namely the litany, social causes, discourse/worldview and myth/metaphor levels of knowing. What is challenging in terms of the application of CLA is that research must be conducted by moving up and down these layers of analysis. This ensures that research is “inclusive of different ways of knowing” (Inayatullah, 2000:1).

The first level is the litany level of knowing, namely quantitative trends, problems, sometimes overstated, often used for political purposes while it is generally presented by the news media. This represents mainly the official, unquestioned view of reality. On the litany level, issues, trends and events are not always connected and appear irregular. The result is often the promotion of a feeling of apathy or helplessness or calls for projected action. This level can be regarded as the conventional level of futures research and can easily create politics of fear. The causes and implications of the mentioned events, issues and trends are not adequately analysed and evaluated.

The second level is concerned with social causes, including political, economic, historical and cultural factors. The data of the litany level are explained and questioned at the social causes level of knowing. In the case of quantitative data, interpretation is given. In general, policy institutes usually articulate this type of analysis. In some cases, the precipitating action is analysed. At this level, academic analysis as well as technical explanations are done. The role of the state and other interests and actors is also often investigated at this level (Inayatullah, 2005a:55-56).

The third level goes deeper and focuses on structure and the discourse or worldview that supports and legitimises it. The undertaking is to find deeper linguistic, cultural and social structures that control or significantly impact on the actors. At this stage, it is important to revise or recast the problem but also the perceptions or deeper assumptions behind the issue being investigated. Now it can be investigated how different discourses (cultural, social and economic) do more than mediate or cause the issue but construct it, as well as how the discourse that the observer uses to understand is complicit in the outline of the issue. Discrete alternative scenarios can be derived on this level based on the varied discourses. The value of such scenarios is that they could add a horizontal dimension to the layered analysis.

The fourth analytical layer is at the level of metaphor or myth. These are the collective archetypes, the deep stories and the unconscious dimensions of the problem. This level offers an emotional or "gut" level experience to the worldview under inquiry: "The language used is less specific, more concerned with evoking visual images, with touching the heart instead of reading the head" (Inayatullah, 2000:5-6).

CLA develops an in-depth dimension to the horizontal approach of scenarios. Focused on going from the litany (or the popular fear-based representations of the future) to the level of policy analysis (the think-tank trends dimension) to that of worldviews (of religion, economic systems or the grander paradigms), it concludes with an examination of the myths and metaphors that support current social and personal structures (Inayatullah, 2005e). CLA, however, does not give advantage to any particular level. CLA promotes going beyond the conventional way of framing issues. In general, scholarly analysis is inclined to focus on the second layer with sporadic forays into the third, but seldom will the fourth layer (myth and metaphor) be explored. As mentioned earlier, ideally research should be conducted by moving up and down these layers of analysis. Such an approach will be inclusive of different ways of knowing. In so doing, it will allow for the creation of integrated transformation and authentic alternative futures (Inayatullah, 2000:11-12).

This method takes futures studies away from pure speculation and moves it to social inquiry. An investigation using such a method is enriched by other levels and layers. By being multi-dimensional, it has a greater efficacious value (Inayatullah, 2005e). CLA is applied in this study in terms of evaluation of the environmental scan, as part of an information warfare futures model and in the compiling of the final scenarios.

### 3.6 CONCLUSION

As information warfare is closely linked to technology futures and the changing manifestation of warfare and conflict, it is a subject already intimately related to the future. Although the interconnectedness of past, present and future complicates any definitive study of the future, an open-minded futurist approach requires insight into the dynamics between the past, present and future. The growth of short-horizon perspectives in terms of most current humanities-related activities has increased the need for a futurist perspective. This futurist perspective does not entail prediction of the future, but strives to provide insight and foresight with the aim to assist (*inter alia* the policy-maker) in creating a preferable future.

Although many futurists agree on the rationale, role and aims of future studies, approaches to future studies differ significantly. In this study the approach to future studies is trans-disciplinary and action orientated. The attainment of foresight, as core aim of future studies, remains a central part of the approach to the future. Foresight implies the capacity to have a notion of what is likely to manifest in the future and to be able to take the appropriate action to aid or avoid it. Foresight can enhance knowledgeability in humans and is of significant value for decision-making impacting the future.

Systems theory is especially useful in assisting endeavours to analyse the varied relationships of the many aspects of the social order and thus operates against fragmentary analyses of the social world. It also significantly assists in preventing the analyst from being overwhelmed by complexity. A system remains a discernible whole that interacts purposefully with its environment and is comprised of interacting and interrelating parts that are organised for a specific purpose. Constant change is maintained by connections being established and broken within and among systems. It has been shown in this chapter that it is constructive to view systems on different levels delving into increasing complexity and analytical levels in an effort to identify underlying causes and broader implications and understanding of events.

Visualising the possible, probable and even preferable futures can be done by using a futures map, which provides a conceptual frame for futures-related research. As extremely swift changes cannot be predicted and may be considered random, the focus of futures studies is mainly the complex field.

Additional analytical capacity, which is based on a systems perspective, can be gained by focusing on a layered approach. This takes into account the vertical complexity of systems. The futures-orientated layered approach that is generally used is CLA consisting of four levels: the litany, social

causes, discourse/worldview and myth/metaphor levels of knowing. By moving up and down these layers it is possible to integrate analysis and synthesis and horizontally integrate discourses, ways of knowing and worldviews, thereby increasing the range of the analysis.

## CHAPTER 4

### DEFINING INFORMATION WARFARE AND NATIONAL SECURITY

#### 4.1 INTRODUCTION

When working with dynamic concepts such as information warfare and national security a clear understanding of these concepts remains vital for the analysis of the possible future manifestation of these phenomena. There is a risk that all forms of warfare in the Information Age can be perceived as information warfare, while at the same time all human-related threats could be viewed as national security risks. As both information warfare and national security are later used in a futurist context, cognisance must also be taken of possible future changes and challenges that could influence the development of these concepts.

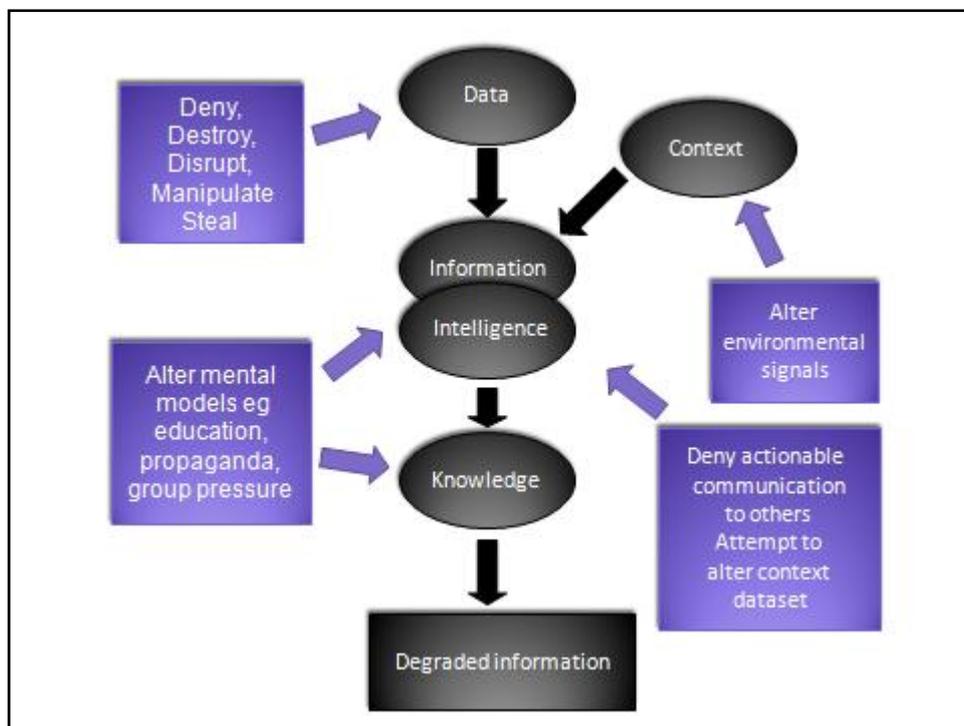
Information warfare became a popular new post-industrial warfare and power projection concept, especially after the end of the Cold War. Initially, it was a USA military concept designed mainly to ensure continued USA military dominance in the post-Cold War era. This led to extensive literature on information warfare theory and practice, much of which is in the public domain (De Landa, 1991; Denning, 1999; Libicki, 1995; Schwartz, 1996; Waltz, 1998). Although still mainly a concept analysed by the developed world, some writers from China, Russia and India have been focusing on information warfare related issues and manifestations since the late 1990s (Hauschild, 1999; Ji, 1999).

Predictably, the prevailing language, images and metaphors related to information warfare are still militaristic in character, blurring the fact that many of the underpinning principles and assumptions have significant national security applications well beyond conventional military contexts (Cronin & Crawford, 1999:257). In the context of national security threats, globalisation and the information revolution, this narrow militaristic view of information warfare has been transcended. At the same time, the traditional concepts of “military” and “warfare” are also increasingly being challenged in the environment of globalisation and technological advancement (Darnton, 2006:141). As information is progressively more drawn into systems of production, governance strategies and modes for power projection, it is quickly becoming a critical resource in the 21st century conceptions of power (Kilibarda, 2003:10). The role of information as instrument for power projection is central to evaluating information warfare as a national security threat, presently as well as in the future.

## 4.2 DEFINING DATA, INFORMATION, INTELLIGENCE, KNOWLEDGE AND WARFARE

As a starting point the differences between data, information and knowledge must be examined. Data, information and knowledge are somewhat ambiguous terms resulting in rather unclear boundaries between these concepts. However, an implied hierarchy of understanding remains evident, with data being the most basic unit, while knowledge is on a higher level than information, and, to take it even further, wisdom signifies a high level of learning combined with well-learned experience and the capacity to apply both judiciously (Webster, 2005:187).

The conventional way to define data, information and knowledge is in a linear way. See Figure 4.1 for an illustration of the concepts and possible challenges associated with this arrangement. Data, which forms the lowest level and describes attributes of things (Hutchinson & Warren, 2001:1), includes individual observations, measurements and basic messages, including human communication, text messages, electronic queries or scientific instruments that sense phenomena (Waltz, 1998:1-2).



**Figure 4.1: Data, knowledge, information and intelligence continuum**

Source: Compiled from Hutchinson and Warren, 2001:2.

Information is organised and collated into sets of data in context (Hutchinson & Warren, 2001:1). It is a resource created from two elements: phenomena (data) that are observed, plus the instructions (systems) required to analyse and interpret the data to give it meaning (Wilson, 2007:2). The organisational process may include sorting, classifying or indexing and linking data to

place data elements in a relational context for subsequent searching and analysis (Waltz 1998:1-2).

A related but somewhat broader definition of information, namely the "content or meaning of a message", is used in this study (Mader, 1974:3). Information remains a central resource for competition, conflict and warfare in states (Waltz, 1998:49). Information, once analysed, interpreted in the light of experience and understood, becomes knowledge (Hutchinson & Warren, 2001:1). Understanding information provides a degree of comprehension of both the static and dynamic relationships of the objects of data and the ability to model the structure and past (also future) behaviour of those objects. Knowledge includes both static content and dynamic processes.

In the national security context, this level of understanding is referred to as intelligence (Waltz, 1998:1-2). Defined as "information relevant to a government's formulating and implementing policy", the intelligence role has traditionally emphasised the instrumental nature of information in support of a state's power sources, primarily military and security (Shulsky, 1993:1).

All of these concepts, which constitute the building blocks of information warfare, illustrate specific vulnerabilities which begin to allude to the possible destruction and/or manipulation of these elements for purposes of power projection. Measures against data, information, knowledge and context include a wide array of direct as well as indirect actions, resulting in the degrading of information and information systems.

Warfare refers to all lethal and non-lethal actions undertaken to subdue the hostile will of an enemy or adversary. Warfare is not necessarily synonymous with "war". Warfare does not require a declaration of war, nor does it require the existence of a situation widely recognised as "a state of war". Warfare can be commenced by or against state-controlled, state-sponsored or non-state groups. Warfare is hostile activity aimed at an enemy or adversary (Szafranski, 1995). In the context of information warfare, the direct lethal consequence of warfare is excluded.

In warfare, the conflicting parties perceive each other's objectives as mutually exclusive and apply force and other means to achieve victory. Information warfare accentuates the operations that use the mentioned "other means" (Waltz, 1998:1). While this view contributes to the demarcation of information warfare, this still includes a significant range of actions which makes the identification of information warfare related actions problematic.

While information warfare has a distinct meaning in the context of this study (which will be defined later), information has been part of warfare since the beginning of history. Although the term information warfare will be used in its contemporary and futurist contexts, it must still be remembered that it does have strong historical links, which will be briefly described. While some aspects related to information warfare are as old as humankind, many aspects of how it is applied in our contemporary information-driven world are new (Jones, Kovacich & Luzwick, 2002:5).

### 4.3 HISTORIC OVERVIEW OF INFORMATION AND NATIONAL WILL IN A NATIONAL SECURITY CONTEXT

The roots of information in warfare are old and deep. Combatants as well as strategists have long recognised the role of information and knowledge in warfare. Indeed, the age-old warfare principles of surprise and security embody the creation and exploitation of an information differential (Okello, Ayres, Bullock, Erhili, Harding & Perdigao, 1996:1).

The origins of concepts and practices relevant to information in conflict can be identified in the seminal work by Sun Tzu. This Chinese work recognises information as crucial in reducing the uncertainty of war (Magsig, 1995). Much of *The Art of War* (Tzu, 1963), popularised due to Tzu's holistic view of warfare, focuses on the role of information and knowledge in the successful conduct of war. Tzu made the following four assertions regarding information (Waltz, 1998:1-2):

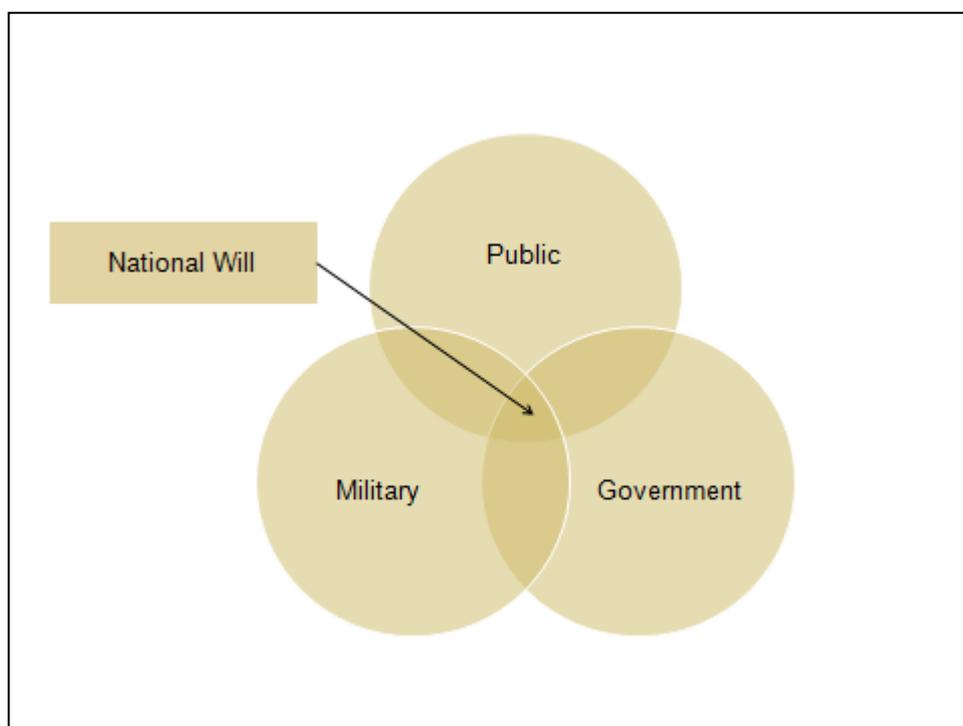
- Information is critical for purposes of surveillance, situation assessment, strategy development, and assessment of alternatives and risks for decision making. Tzu stated: "In respect of military method, we have, firstly, measurement; secondly, estimation of quantity; thirdly, calculation; fourthly, balancing of chances; fifthly, victory."
- Information in the form of intelligence and the ability to forecast possible future outcomes distinguishes the best warriors. Tzu said: "Thus, what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge."
- The control of some information communicated to opponents, by deception (seduction and surprise) and denial (stealth) is a contribution that may provide transitory misperception to an adversary. Tzu stated: "All warfare is based on deception (of the enemy)" and "O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible".
- The supreme form of warfare uses information to influence the adversary's perception to subdue the will rather than using physical force. Tzu declared: "In the practical art of war, the best thing is to take the enemy's country whole and intact ... Hence to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."

Since the mid nineteenth century, Carl von Clausewitz's classic text *On Warfare* (1989) has dominated military thinking for a considerable time into the twentieth century. He regarded information as generally unreliable in war. This can be clarified by his focus on operational and tactical level issues, and his pre-Industrial Age frame of reference. However, Von Clausewitz so dominated earlier strategic or national security thinking that his bias against information (and

intelligence) continued and, in some cases, according to Magsig (1995), even undermined the acceptance of the precepts of information warfare.

Von Clausewitz's insight regarding national will in the context of conflict remains relevant in terms of how governments respond to national security threats in general. He referred to the nature of war as a "paradoxical trinity", balanced by a combination of the public, government leadership and the military in a viable mutually supportive relationship. According to Crumm (1996:7), the often debated area common to all three forces represents national will. See Figure 4.2 for a graphic illustration of Von Clausewitz's national security trinity and national will.

In the current context, the military dimension can be replaced with the national security infrastructure of the state which includes national security assets such as the police, intelligence services and other security structures of the state. National will remains an important component in responding to national security threats and managing that response.



**Figure 4.2: Von Clausewitz's national security trinity and national will**

Source: Crumm, 1996:6.

Lonsdale (2004) after an assessment of both historical and contemporary case studies (including the events following September 11 and the recent war in Iraq), concludes that although the future will see many changes to the conduct of warfare, the nature of war, as given theoretical form by Clausewitz, will remain essentially unchanged. Information is regarded as just one dimension of strategy and as deficiencies in the technological dimension can be compensated for by other means, it can be done with information. A force without information dominance can still operate,

although it may be more vulnerable and less effective at the tactical and operational levels (Lonsdale, 2004:189).

Despite Von Clausewitz's and Lonsdale's views on information in war, in general the importance of information and intelligence has been understood and practised by state leaders, commanders and military strategists since the advent of conflict and war. Actually, all of the cardinal principles related to conflict and applied since ancient times, relied on the acquisition, processing and dissemination of information. While these principles did not change, the means of acquisition, processing and dissemination have changed. The importance of information has been significantly boosted by the advent of electricity and even more so since the digital age.

The increasing dependency on digital involves the management of large volumes of information, and the increasing value of that information has made the information itself a lucrative target and valuable weapon of warfare. These changes are revolutionising the role of information, the conduct of warfare and the projection of power in general (Waltz, 1998:2-3). As technology develops to fully exploit big data, this will provide significant future military, tactical and strategic advantages. Big data is a loosely defined term used to describe data sets so large and complex that they become awkward to work with using standard statistical software (Snijders, Matzat & Reips, 2012:1).

#### **4.4 DEFINING INFORMATION WARFARE**

##### **4.4.1 Challenges in finding a definition**

Although information warfare is a recent concept, only being used since the early 1990s, a wide range of meanings have been attached to this concept and related concepts such as info war, cyber warfare, netwar, information operations, command and control warfare, sixth-generation warfare, hactivism, network centric warfare, operational net assessment, iWar, cyber terrorism, cyber vandalism and knowledge war. The differing and sometimes overlapping nature of all these concepts has also contributed to confusion on the exact scope of the phenomenon of information warfare. In this study, the term information warfare (in the USA, information operations is now the preferred term) will be used as an overarching term referring to related but also differentiated uses of information in a national power projecting context. Certain concepts or parts of concepts will, however, be excluded in an effort to focus on what is understood by the term information warfare.

There is no single generally accepted definition of information warfare (Candolin, 2003). This is because information warfare represents a rapidly evolving and, as yet, imprecisely defined topic of growing interest for security academics, planners and policymakers. The most significant sources of both the interest and the imprecision in this field is the information revolution led by the ongoing

and rapid evolution of cyberspace<sup>11</sup>, microcomputers and associated information technologies (Molander, Riddile & Wilson, 1996:xi).

As illustrated in the historic view of information in warfare, one of the aims of warfare has always been to destroy and affect an opponent's information systems. In the broadest sense, information systems include every means by which an adversary arrives at beliefs or knowledge. A narrower view espouses that information systems are the means by which an adversary maintains control over, and direction of, power projection capacities. Taken together, information systems provide a comprehensive set of the beliefs, knowledge and the decision-making processes and systems of the adversary. At every level the outcome sought by information attacks is for the adversary to receive sufficient messages that persuade the adversary to stop resisting (Szafranski, 1995).

Common understanding of the significance of information warfare has expanded beyond its initial primarily military application. It was realised that information warfare, as both a security threat and instrument for power projection, has potentially much wider implications for society at large in a networked age. Information warfare has also become a popular concept in the corporate/economic, community/social, and personal spheres. Certain information warfare concepts, strategies and applications are common to all these and the military settings although there are some interpretative differences as well as differences in the perceived legality, ethicality and social desirability of the outcomes pursued by different actors under different conditions (Cronin & Crawford, 1999:258). Another problem in finding a definition of information warfare is related to the scope of information warfare (Taipale, 2006: Slide 3). Does information warfare refer to the tactical or strategic domain of warfare?

Existing definitions of information warfare have many limitations, such as being too broad or too vague. Unfortunately, information warfare has become such an expansive term that it threatens to become a tautology by encompassing nearly everything beyond the most primitive forms of combat (Dinardo & Hughes, 1995:4). The USA military-centric nature of the existing definitions also remains a serious stumbling block in the search for an appropriate definition.

#### **4.4.2 Broad definitions**

A broad definition focusing on the central role of information in strategic posturing is provided by Stein (1995:32): "... information warfare, in its largest sense, is simply the use of information to achieve our national objectives." Using this definition, however, would make it impossible to

---

<sup>11</sup>

Arquilla and Ronfeldt (1997:41) described cyberspace as follows: "... is a bioelectronic environment that is literally universal, it exist everywhere where there are telephone wires, coaxial cables, fibre-optic lines or electro-magnetic waves. This environment is inhabited by knowledge, existing in electronic form." Cyberspace consists of two measurable elements: connectivity and content. Connectivity encompasses the physical hardware, software and connecting electromagnetic or cable media that permit the generation, transfer, storage and sharing of data. The second element of cyberspace is content which influences behaviour and decision-making (Campen, 2008).

exclude any diplomatic, military or international interaction from this definition, even if it is only routine and in line with most state practices through the ages.

Denning's effort (1999:12) to deepen the definition of information warfare to encompass "information in any form and transmitted over any media, from people and their physical environments to print to telephones to radio and television to computers and computer networks" identifies the modern technology environment within which information warfare could flourish. This definition does, however, not distinguish between normal messages communicated over these media and what could be interpreted as information warfare.

Libicki (1995:1) was more specific on what could be construed as information warfare, but then included some tactical and strategic elements which would render any constructive effort to make generalised assertions on information warfare practically impossible. Highly divergent aspects are included in Libicki's concept of information warfare. He identified seven distinct kinds of information warfare, namely:

1. Command-and-control warfare (C2W), which has the objective of decapitating the enemy's command structure from the body of the command.
2. Intelligence-based warfare (IBW), which occurs when intelligence is fed directly into military operations (notably targeting and battle damage assessments) rather than being used as input for overall command and control.
3. Electronic warfare (EW), which is the use of operational techniques – such as radio, electronic and cryptographic techniques – to degrade the physical basis for transferring information.
4. Psychological operations (PSYOPS), which is the use of information against the human mind.
5. Hackerwar software-based attacks on information systems, which refer to the computer-related disruption of IT networks and applications.
6. Information economic warfare (IEW), which is an effort to cause information blockades and information imperialism.
7. Cyber warfare, which is combat in the virtual realm, such as semantic attacks.

Although concepts such as C2W, IBW, EW and IEW have elements related to information warfare, these are also specific military and strategic terminology encompassing a much broader range of actions than merely information-related activities.

Another broad definition, especially formulated to include the non-military perspective, has been proposed by Jones, Kovacich and Luzwick (2002:5), namely information warfare "... is a coherent and synchronized blending of physical and virtual actions to have countries, organizations, and

individuals perform, or not perform, actions so that your goals and objectives are attained and maintained, while simultaneously preventing competitors from doing the same to you". This definition potentially includes most of the actions that these mentioned actors perform and thus also actions that strive towards mutually beneficial outcomes, which could hardly be seen as information warfare.

Curran, Concannon and McKeever (2008:6) described information warfare as a societal-level conflict waged, in part, through the worldwide interconnected means of information and communication. This definition does provide a useful insight into the broader scope of information warfare but does not refer to the aim of the mentioned conflict. It would be difficult to exclude issues such as business conflict and political contestation which would include subjects not directly relevant to the national security implications of information warfare.

#### **4.4.3 Definitions limited to the ICT component**

Some definitions of information warfare are limited or largely limited to attacks on the ICT infrastructure and capacities of countries and/or entities. According to Elbirt (2003:2-3), information warfare may be defined as an unauthorised and deliberate attack on an adversary's information infrastructure through the use of computer intrusion techniques while preventing the adversary from performing (or making it extremely difficult for the adversary to perform) similar attacks upon the initiator's information infrastructure. These attacks include information exploitation, denial of service, and the modification, manipulation, corruption or deletion of data. This definition only highlights the technology aspects of information warfare and excludes the potential strategic implication that it could be only the method for a larger objective to downgrade the decision-making potential and subsequent power of an adversary. The ICT-related conceptualisation of information warfare will be regarded as cyber warfare for the purposes of this study.

#### **4.4.4 Military definitions**

According to Kuehl (2007:10), information operations (which is the preferred term for information warfare in the USA military) are defined in the *Information Operations Road Map* published in October 2003 as the integrated employment of the core capabilities of electronic warfare, computer network operations, military deception and operations security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting your own. While this definition is somewhat more focused than the Martin Libicki definition, in essence, it is a purely military perspective and similarly includes a broader range of actions than merely information-related activities.

Alger (1996:12) described information warfare as "actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending one's own information, information based processes and information systems". This

definition does provide the strategic aim of information warfare in a clear and concise manner. Its limitation is that it does not demarcate these mentioned actions more precisely. Even within the limitations facing the political or military leader in the past, information superiority has been vital in the successes and failures of strategic positioning and warfare. What thus needs to be further defined is what these actions entail.

In this regard, Widnall and Fogelman added action elements by defining information warfare as "... any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions" (Widnall & Fogelman, 1997).

Hutchinson and Warren (2001:2-4) also contributed in this regard by conceptualising information warfare as an attack on the elements of data, context, information and knowledge (see Figure 4.1). Information warfare is explained by them as information operations conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. It is the act of influencing civil or military decision making, operational capability and public opinion by using information and information processing both as a target and a weapon, and to protect oneself against such influence. Thus, information warfare has both an offensive and a defensive side. Information warfare can be carried out by civil, political, psychological, social, economic and military means on a strategic, operational or tactical level (Candolin, 2003). Most of the military orientated definitions also refer to the non-military environments in which information warfare could manifest.

#### **4.4.5 Synopsis of information warfare definitions**

Evaluating information warfare definitions identified three types namely broad, ICT related and military definitions. Although all definitions highlight some relevant aspects of information warfare, not one of these definitions does justice to the full spectrum of activities, which could be regarded as information warfare. An important unifying factor in these definitions is that information warfare is therefore an attempt to bring together all facets of power projection to bear on an adversary in a synergistic manner to achieve objectives (Armistead, 2004:18).

#### **4.4.6 The relationship between information warfare and power**

An important factor not highlighted in many information warfare definitions is the relationship between information warfare and power. Many practical and theoretical activities related to the manipulation of data, information and knowledge do not directly diminish or influence the political, socio-economic and military power of governments and governing elites. These activities, which could be economic, social or criminal related, will not be regarded as information warfare in terms of this study.

National power is increasingly dependent on broad-based competitiveness in the creation and use of the dominant technology (Gompert, 1999:59). The advances in technology, particularly in telecommunications, information technology and media fields, have changed the worldview of power over especially the past two decades. The importance of information as an element of power lies in the use of information and its fungibility, which makes it different from the past. The ability to transform information, to move it or display its power all relates directly to its transferability. This is where technology has revolutionised the power structure. The merging of what were once stovepipe and separate areas has opened the access to power for everyone, through the use of information, and has given people a means to distribute it around the world (Armistead, 2004:13).

Information has consequently evolved as an element of national power along with diplomatic, military and economic power while at the same time information has become woven through the other power elements since their activities also have an informational impact (Murphy, 2006:vii). However, the information revolution has not equalised power among states (Nye, 2005:233). The relationship between information warfare and the capacity of the state to maintain and expand its ability to project its power remains one of the key factors differentiating between information warfare as security issue and information warfare as societal phenomenon.

#### **4.4.7 Definition of information warfare**

Taking the above-mentioned evaluation of the different definitions of information warfare into account, a definition for the use of this term is proposed:

*Information warfare is defined as actions focused on destabilising or manipulating the core information networks of a state or entity in society with the aim to influence the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state.*

The focus of information warfare is thus on disrupting and manipulating an adversary's decision-making processes (Wilson, 2007:2). This can be done on two levels, namely on the cognitive and the technological levels. Flowing from this, information warfare manifests itself in two distinct but also related ways (see Table 4.1 and Figure 4.3). The distinction between the two manifestations of what is deemed to be information warfare is important in terms of this study since the implications of these phenomena in terms of the future impact on national security are to be investigated. One manifestation, which encompasses both netwar and psychological operations, is closely related to the state's capacity/vulnerability in terms of networking, perceptions, deception, decisions, influence and knowledge. The second, cyber warfare, refers to the technical infrastructure supporting the state's power capacity in terms of digital networks, critical ICT infrastructure protection, computer software and hardware. There are some similarities and commonalities between these two manifestations of information warfare but the main differential

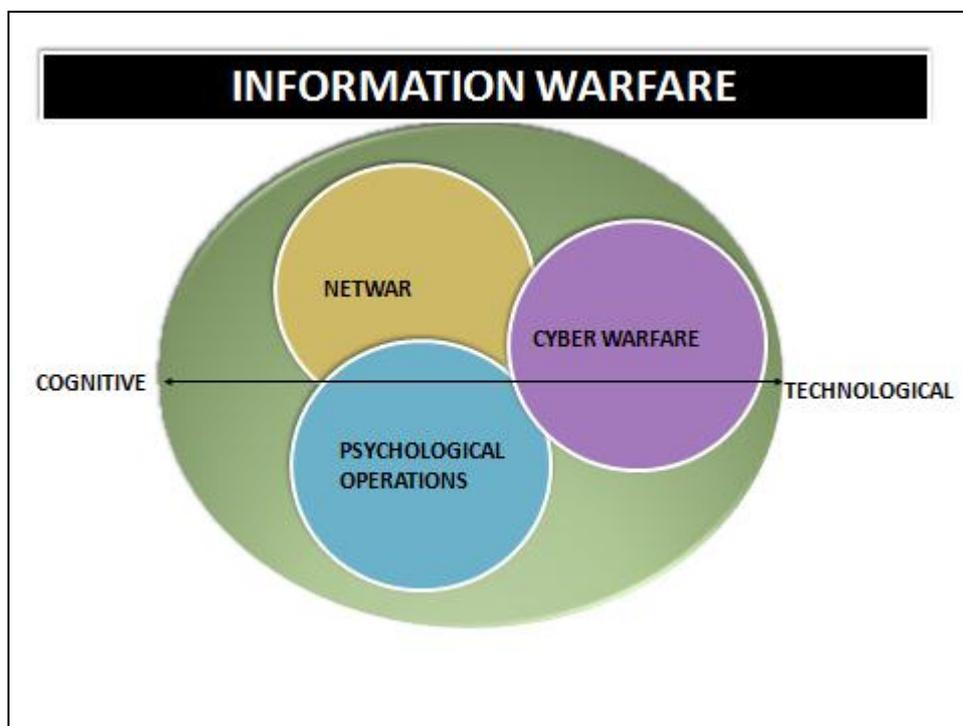
lies on the cognitive-technical continuum identified within the broader concept of information warfare (see Figure 4.3).

**Table 4.1: Manifestation of information warfare**

<b>Information warfare</b>	<b>Type 1: Netwar / Psychological operations</b>	<b>Type 2: Cyber warfare</b>
<b>National security threat</b>	Yes	Yes
<b>Sphere</b>	Networked relationships / cognitive level  Human decision-making level	Cyberspace technological level
<b>Target</b>	Networked relationships, decision-making processes by influencing perceptions	Information systems, by altering data and information
<b>Aim</b>	Corrupt decision making / focus diverse forces on selected targets	Corrupt / disrupt modern management processes
<b>Method</b>	Influence within networked societies, propaganda	Cyber methods
<b>Approach</b>	Deception	Disruption / destruction
<b>Strategy</b>	Asymmetric / symmetric	Cyberspace operations
<b>Enablers</b>	Mass media / networked relationships	Internet / ICT networks
<b>Counter</b>	Social networking; counter propaganda and public relations	Network security
<b>Technology used</b>	Broadcasting / ICT / social networking	ICT
<b>Timeline</b>	History / present / future	Present (early stages) / future
<b>Scope</b>	Largely strategic but also tactical	Largely tactical (with strategic implications)
<b>Location</b>	Local – global	Global
<b>Actors</b>	State and non-state	Individual, non-state and state
<b>Prime drivers</b>	Human mind	Technology

<b>Training ground</b>	Higher education / experience	Technical training and education / technical experience
<b>Battle space</b>	Mind space	Cyberspace

Source: Own compilation.



**Figure 4.3: Components of information warfare**

Source: Own compilation.

#### **4.4.8 Netwar, psychological operations and cyber warfare defined**

Netwar is described by Arquilla and Ronfeldt (1997) as follows: “Netwar refers to an emerging mode of conflict at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the Information Age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command.”

The spectrum of netwar may also seem broad at first glance, but there is an underlying pattern that cuts across all variations. This is the use of network forms of organisation, doctrine, strategy, and technology attuned to the Information Age (Arquilla, Ronfeldt & Zanini, 1999:83). Mass and mobility will not necessarily decide the outcome of conflict. Instead, decentralised and networked forces with superior command, control and information systems will disperse the fog of war while

enshrouding the enemy in it. Historically, in the 12th and 13th century, Mongol armies for example successfully employed netwar doctrine<sup>12</sup> (Magsig, 1995). A modern example in terms of netwar tactics in employing decentralised networked protests is the #feesmustfall student movement against increases in study fees at South African universities in October 2015 (Dasnois, 2015).

Closely connected to the networking model of netwar is the concept of psychological operations. This refers to an intangible sphere, in essence the conflict area is people's minds, and criteria for winning or losing are also heavily culture-dependent (Eriksson, 1999:58). Some scholars argued that strategic advantage does not lie in the concentration of facts and figures, but in "... the complementarily and singularity of the brains who interpret them". National and widespread sense-making capability matters more than electronic information highways, according to Baumard (1996). Psychological operations can also be conducted continuously to influence perceptions of opponents favorable to the source's own strategic and tactical objectives (Goldstein & Jacobowitz, 2002:4). Thus efforts to influence this sense-making encompass more than just using electronic and digital means in terms of both netwar and psychological warfare. Both of these are as old as warfare and conflict itself and have many historic examples. Advances in ICT have the potential to impact both of these phenomena in the 21st century.

Cyber warfare (cyberwar) is a term used to describe a type of conflict that takes place in cyberspace (the virtual world and the internet) instead of in the physical world. This may include attacks on (Computerhope.com, 2007):

- Government and/or military run websites gaining confidential or classified information, disrupting or disabling the agency from doing everything it was meant to do, and/or creating backdoors for future attacks
- Individual or a collection of websites that prevent them from being accessed
- Major utilities such as power, water and communication systems, causing disruptions or complete outages
- Financial institutions, such as banks and stock markets, causing disruptions, outages and/or false information
- Major backbones, routers or other sections of the internet, causing disruptions in all internet traffic.

While information warfare is only in its early stages, it creates the probability that future adversaries might exploit the tools and techniques of the information revolution to hold at risk (not to destroy but to cause large-scale or massive disruption) key national strategic assets such as the initial elements of the national political will, decision-making processes, the capacity to communicate and

---

<sup>12</sup> The Mongols, a classic example of an ancient force that fought according to netwar doctrine, were organised more like a network than a hierarchy. More recently, the combined forces of North Vietnam and the Viet Cong, a relatively minor military power that defeated a great modern power, operated more like a network than an institution. In both cases, the defeated opponents of the Mongols and the Vietnamese were large institutions whose forces were designed to fight set-piece, attrition battles (Arquilla & Ronfeldt, 1995).

information processes within the national infrastructure sectors (Molander, Wilson, Mussington & Mesic, 1998:3).

At this stage, some fundamentals of information warfare need to be identified with a view to serve as an introduction to the definition of national security. While different targets for information warfare can be identified, it is possible to recognise the common fundamentals underpinning all forms of this phenomenon.

#### **4.5 THE FUNDAMENTALS OF INFORMATION WARFARE**

Taking cognisance of information warfare as an overriding term, while also noting the history of information in conflict as well as criticism on existing definitions, the following fundamentals endeavour to identify some common elements as well as significant characteristics of information warfare:

- Information in especially a networking<sup>13</sup> capacity is central to the information warfare concept with attaining information superiority as a tactical and strategic aim.
- Information warfare refers to the cognitive and technological disruption linked to conflict and war but not to the kinetic aspects associated with war and terrorist activities.
- Information warfare is linked to using information as instrument for manipulation, power projection, leveraging and creating an advantage.
- The strengthening of network-orientated organisations and interactions, while consequently hierarchical orientated organisations and interactions are weakened because of the information revolution and expansion of global communications (Arquilla & Ronfeldt, 2001:1).
- The global network ecology is transforming itself from a purely communications medium to a social environment of growing political and security significance (Vlahos, 1998:77).
- The exponential growth of technology, globalisation and increasing significance of networking are enhancing the future significance of information warfare.
- Information warfare is in essence a transdisciplinary concept covering a wide array of interests, including the political, governance, technological, psychological, social, media, economic and military fields.
- Both offensive and defensive roles are envisaged for information warfare.
- Information warfare is not bound by geographic limitations.
- The cost of conducting information warfare would in most cases be much lower compared to other forms of power projection.
- It is widespread and available to any country, and, in most cases, to any individual or group that wants it (McLendon, 2008). Some technological skills barriers exist in the case of cyber warfare.
- The increasing dual-use nature of especially information technology results in many technologies having both military and civilian applications (Schneier, 2008).

---

13

A network can be understood very simply as a series of nodes that are connected. The nodes can be individuals, organisations, firms or computers, so long as they are connected in significant ways (Williams, 2001:66).

- Information warfare invokes asymmetric action. Asymmetry is about the qualitative difference in the means, values and style of opposing powers. Once a state or entity insists on superiority in power projection, its disadvantaged opponents resort to unconventional asymmetrical means to oppose it, avoiding its strengths and concentrating on its vulnerabilities (Bishara, 2001).

These fundamentals of information warfare as well as the content of information warfare (netwar, psychological warfare and cyber warfare) are revisited in Chapter 5 where the consequences in terms of the environmental scan are evaluated. Now that the fundamentals of information warfare have been established, it is necessary to focus on defining and understanding national security.

## **4.6 DEFINING NATIONAL SECURITY**

### **4.6.1 Context for finding a definition for national security**

Security is a problem of a special kind. It embraces all those exchanges between humans and their agents, such as states, international organisations, companies, associations and other entities that have as their aim the pursuit of their preferred outcomes while also being prepared to use coercive intimidation and even violence in this process (Kolodziej, 2005:23).

Trager and Simonie (1973:36) defined national security as “that part of government policy having as its objective the creation of national and international political conditions favourable to the protection or extension of vital national values against existing and potential adversaries”. Brown (1983:4) explained this on a more practical level when he defined national security as “the ability to preserve the nation’s physical integrity and territory; to maintain its economic relations with the rest of the world on reasonable terms; to protect its nature, institutions and governance from disruption from outside, and to control its borders”. Traditionally, security is conceived as “inherently politically conservative precisely because it emphasizes permanence, control, and predictability” (Dalby, 1992:98). Security was regarded within narrow, almost exclusively military terms, and the Cold War definitions of national security use the national state as referent of security. Wing (2002:16) argued that this approach regards security as a burden that must be borne by national states.

Traditionally, the threat or reality of interstate war was regarded as the primary cause of insecurity and most of the times the main priority for serious consideration by national security decision-makers. However, since the mid-1980s (perhaps even since the oil shocks of the 1970s), this limited traditional concept of security has become increasingly untenable. While the thinking about security has changed throughout history, this has been boosted significantly since the end of the Cold War and the rise of globalisation (Wing, 2002:iii). Threats that have been largely overshadowed by the risks of nuclear war between the superpowers during the Cold War emerged more prominently (Jones, 1996:207).

Non-military issues such as economic, environmental and human rights related issues have increasingly forced their way on to the global security agenda (Sheehan, 2000:471). A United Nations (2004) report titled *Report of the High-level Panel on Threats, Challenges and Change* states: "... security threats do not respect national boundaries – from invasion, war and conflict within states they extend to poverty, infectious diseases and environmental degradation." Security threats also include "the spread and possible use of nuclear, chemical and biological weapons as well as terrorism and transnational crime". One of the key driving forces in this expanding global security agenda is the role and implications of technological advancement. Most technologies occupy a rather problematic space by both enabling and undermining conditions of security (Rappert & Croft, 2007:7).

The Information Age has a significant influence on national security. The contemporary challenge now is how to meet national security needs in this new and ever-changing technology environment (Goldman, 2004:11). The control and use of information and knowledge is a central engine driving human activity and progress. As individuals, organisations and states interact more and more in cyberspace, political, military and economic leaders are under increasing pressure to manage, deter and reduce the level of associated risks. Threats to cyberspace range from the systematic and persistent to the decentralised and dispersed and to the accidental and non-malevolent (Goldman, 2004:1). At this level, cyber warfare poses a significant national security threat.

In addition, national security threats include both tangible and intangible threats. Security is not only concerned with the state of strategic affairs but also with a state of mind. Perceptions related to a sense of security are an important determinant of security policy in its own right (Mangold, 1990:6). Society's degree of confidence, clarity of purpose and level of trust in the leadership are all potential targets to undermine security (Durodié, 2007:193).

The change from the traditional single focus of national security also created diversity in terms of the challenges posed by national security threats. It is useful to evaluate five basic dichotomies relevant to national security and to refer to the information warfare implications for all. These dichotomies are: security of the state versus security of humans; hard or direct versus soft or indirect interference; legality versus legitimacy; pre-emption versus prevention; and non-state actors versus states (Slaughter, 2004:2):

#### *State security versus human security*

Traditionally, national security was equated with state security. This referred to the capacity of sovereign states to defend against outside threats to their survival as states by way of military defeat, subjugation, or economic and political control (Slaughter, 2004:2). Dr Mahbub ul Haq first drew global attention to the concept of human security in the United Nations Development Programme's 1994 Human Development Report and sought to influence the UN's 1995 World Summit on Social Development in Copenhagen (UNDP, 1994). Since then, human security has

been receiving more attention, in particular from key global development institutions such as the World Bank.

The UNDP's 1994 Human Development Report defined human security as freedom from want and fear. The UNDP argues that the scope of global security should be expanded to include threats to security in seven areas, namely economy, food, health, environment, personal, community and political (UNDP,1994:2). Growing dependency on networked information systems and ICT in managing these aspects of society also ensures that human security related issues remains relevant from an information warfare perspective.

#### *Hard versus soft interventions*

Options for intervention on national security have widened. In reality, the rising interdependence between states are leading to the gradual reduction of independence of states within the international system. Progressively, the international system endeavours to formalise this interdependence and thereby to generate globally accepted mechanisms for “soft” interferences in the affairs of the different states (Nye, 1990b:153-171). These interferences can be diverse, including accords limiting states’ freedom of action. These limitations can be implemented in different ways – from a more invasive evaluation of state actions to international sanctions and elaborate inspections that have to be applied (Bildt, 2004:37). The information realm also offers a wide array of possible soft power interventions which were not that feasible in the past.

#### *Legality versus legitimacy*

National security finds itself increasingly in the environment of new threats versus old rules. The international legal rules and institutions that form the basis of the world order were mostly fashioned after World War II in reaction to the political and economic trends that resulted in the Great Depression and two world wars. Security threats such as the 9/11 attacks and global radical religious terrorism severely challenge the strict interpretation of the legality of actions in terms of international law. An international commission appointed after the NATO intrusion in Kosovo without any earlier UN sanction in 1999 was deemed illegal but regarded as legitimate by the international community (Slaughter, 2004:5). The distinction between legality and legitimacy is part of the change from one legal order to another. It refers to bringing specific legal rules up to date in order to meet shifting economic and political conditions (Slaughter, 2004:6). This distinction is especially pertinent in terms of information warfare as the international law on this is still largely non-existent, creating many legal and legitimacy issues in terms of possible action regarding information warfare.

### *Pre-emption versus prevention*

The USA Bush Administration's 2002 National Security Strategy unilaterally assured a greatly extended concept of the customary international pre-emption legal doctrine as a reaction to upcoming security threats. Another option more in line with international multi-lateral norms is a policy of prevention. According to Slaughter (2004:7), once a threat has materialised, whether it is imminent, near-imminent or potentially imminent, a pre-emptive strike is a meagre and likely unproductive alternative for a policy of thwarting its surfacing before it manifests. While military pre-emption will probably not be accepted by most states, in the information environment pre-emption could possibly be more commonly used as it would be much easier to deny involvement and accountability. However, the challenge to identify perpetrators and actors also severely limits the effective identification of an imminent danger which may increase the possibility of pre-emptive actions against the wrong targets. Pre-emptive actions in an information warfare context could be manipulated and the potential for unintended consequences such as the serious escalation of tensions would be a real danger.

### *State versus non-state actors*

Taking into account state versus non-state actors' contestation, it is acknowledged that what are now regarded as non-state actors<sup>14</sup> pose dominant threats to regions and the world in general (Slaughter, 2004:7). The non-state challenge has again regained focus at the turn of the twentieth and twenty-first centuries, because of three developments (Bailes, 2012:121):

- the shift in overall frequency of major armed conflict worldwide to consist almost exclusively of intra-state conflicts, thus focusing attention on the agents of violence who typify such conflicts, and on the indirect as well as direct damage they cause for people, states, and global security
- the perceived vulnerability of the developed states to non-state opponents exploiting new technologies and 'transnational' modes of recruitment, procurement, and operation.
- the effects of globalisation in enhancing the relative power of all types of non-state or trans-state actors, from multinational corporations through to violent extremists. Globalised conditions help non-state antagonists to access and attack both state and non-state targets, in virtual as well as physical space, both on home territory and abroad. This dark side of globalization is almost inextricable from the productive side: the risk comes as much from states' and societies' growing dependence on worldwide economic partnerships and communication lines, as from the ability of hostiles to exploit global reach and mobility.

In the future, the challenges posed to national security by these dichotomies could potentially be overshadowed by the rise of non-linear<sup>15</sup> challenges to national security. Information warfare is one

---

<sup>14</sup> Historically non-state actors included rebel movements, traders fighting among themselves or as proxies for states, and 'mercenary' soldiers working for both state and non-state interests (Bailes, 2012:121).

<sup>15</sup> Non-linear systems refer to the arrangement of nature – life and its complications, such as warfare – in which inputs and outputs are not proportional; where the whole is not quantitatively equal to its parts, or even qualitatively recognisable in its constituent components; and where cause and effect are not evident. It is an environment where phenomena are unpredictable, but within bounds, self-organising; where unpredictability frustrates conventional planning, where solution as self-organisation defeats

such non-linear challenge that can manifest in the future. Security has become a complex affair, pursued across three basic dimensions: physical space (territory, atmosphere and ocean), infrastructure (networks and systems that determine how societies are organised) and ideas (norms and perceptions that shape social action). As security is transforming, it could be expected to see changes in the way states and societies are organised to achieve security through space, infrastructure and ideas (Latham, 2003:6-7).

#### **4.6.2 Definition of national security**

As explained above, the contemporary national security environment contains elements of both continuity and change. Globalisation, the information revolution and technology's influence on geopolitics are all factors accentuating change. From the perspective of any particular point in time, including now, the unique set of forces and events of the moment may seem to predominate the evolving system. It should, however, be taken into account that some forces that are seemingly unique in a narrow perspective appear less so when viewed within the general evolution of the international system (Snow, 2004:156). Both change and continuity underlie the security dynamics which the national security decision-maker faces.

Taking into account the major fault line of continuity and change, the following definition for national security is proposed:

*National security refers to all government-sanctioned actions and measures driven by the application of national will<sup>16</sup> and taken with the aim to create an environment in which the country's population, state structures, territorial integrity, interests and sovereignty are protected.*

The growing complexity of today's security environment results in governments' increasingly having to deal simultaneously with multiple, often inter-related and yet distinct challenges, while the underlining economic and political changes are driven not only by governments but increasingly by "multinational corporations, state-owned enterprises, NGOs and even by super-empowered individuals" (Bremmer, 2006:66).

#### **4.7 CONCLUSION**

While certain aspects of information warfare are as old as human civilisation, the Information Age has created unique and new opportunities for information warfare to manifest as a national security threat. As a concept, however, information warfare is fairly new as it has only been used since the early 1990s. This resulted in diverse and sometimes contradictory definitions, with no consensus on the exact meaning of this concept. In this study, information warfare is defined as the

---

control; and where the bounds are the actionable variable, requiring new ways of thinking and acting (Alberts & Czerwinski: 2002:xiii-xiv).

manipulation of networking communication by entities with the aim to influence power relationships between countries and the states' governing capacity. Information warfare is taking place on a cognitive-technological continuum. Within the cognitive sphere, information warfare manifests as netwar and psychological operations. Cyberwar manifests within the technological sphere.

Although information warfare can occur on all levels of society, this study focuses on the implications of information warfare for the security of the state. A range of information warfare fundamentals have been identified. As many of these fundamentals are related to the mind space and cyberspace environment within which information warfare takes place, these fundamentals provide a new dimension to power projection and security-related activities. With national security defined as the application of national will by the state with the aim to create an environment in which the country's population, state structures, territorial integrity and sovereignty are protected, information warfare presents a plethora of potential threats and risks to the modern state. The rising scope of the non-state actor as a significant national security concern does present a major national security challenge. Non-state antagonists exploiting new technologies and 'transnational' modes of recruitment, procurement, and operation coupled with the advantages globalisation present in enhancing the relative power of such non-state antagonists to *inter alia* exploit information warfare as a power projection tool.

In Chapter 5, an environmental scan will be used to evaluate the current milieu within which information warfare manifests, with the capacity to also provide some level of insight into the driving forces that will influence how information warfare might manifest in the future.

---

<sup>16</sup> In this context, national will refers to the "paradoxical trinity" as formulated by Von Clausewitz (see Figure 4.2).

## CHAPTER 5

# ENVIRONMENTAL ANALYSIS OF INFORMATION WARFARE AS A NATIONAL SECURITY THREAT

### 5.1 INTRODUCTION

After defining information warfare and national security, and providing the international relations as well as futures theoretical framework within which this phenomenon of information warfare is examined, the attention shifts in this chapter to the current manifestation of information warfare within the context of the multiple environments in which it occurs.

An environmental scan refers to the informational process through which the scanner is attentive to the environment with the creative goal of discovering insights and reducing future uncertainty (Chalus-Sauvannet, 2011:103). This environmental scan is mainly focused on areas that have a direct bearing on information warfare as a national security threat. However, an environmental scan is not only of value to explain the current environment; it is especially useful as a futures methodological tool. This is because scanning the horizon provides a way to identify new developments that can challenge past assumptions as well as new perspectives on future threats or opportunities (Gordon & Glenn, 2003:3). As indicated in Chapter 2, scientific work should investigate and identify relationships and non-relationships between what individuals experience and what actually happens, and the underlying mechanisms that produce the events in the world (Danermark, Ekström, Jakobsen & Karlsson, 2005:21). Environmental scanning provides a unique capacity in this regard.

In this study environmental scanning is primarily used as a futures analysis method to investigate uncertainties about the future in a systematic fashion (Heinonen, 2008:53) with the aim to assist in identifying the main drivers relevant to the manifestation of information warfare as a national security threat by the 2030s. Information warfare is a phenomenon that includes cognitive as well as technological dimensions and the involvement of highly networked spheres while both tactical and strategic ranges are covered. Information is thus gathered from the broader environment with the aim of developing a better understanding of those factors and forces that may have a bearing on the way possible, probable and preferable futures take shape (Roux, 2007:1).

Environmental scanning has become increasingly useful for planners and analysts because of its value as functional tool for future studies, allowing for the analysis of information on specific topics of interest and on the environment influencing the area of interest (Masini, 1993:102). An additional element of futures thinking and environmental scanning is the concept of risk. Risks are primarily linked with the notion of uncertainty, which is an inherent quality of the future (Heinonen, 2008:53).

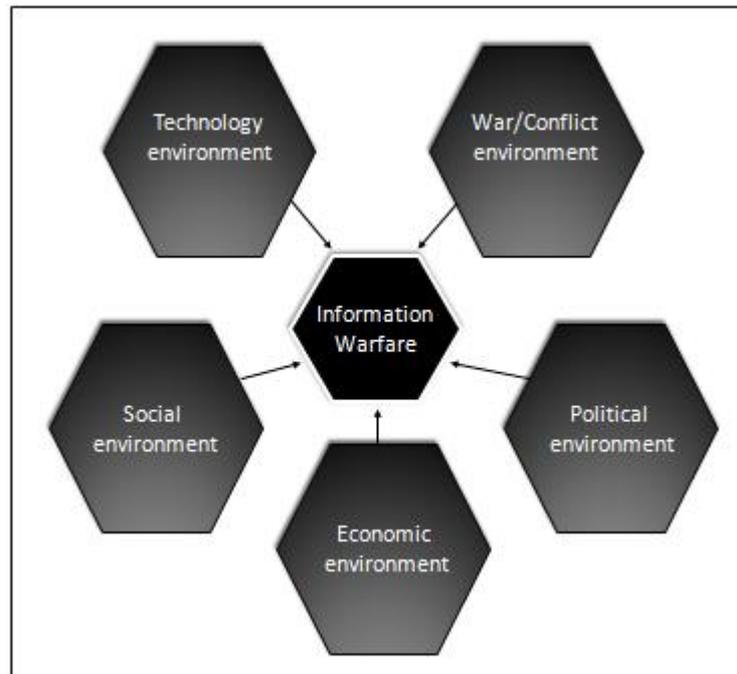
In this chapter the focus is also extended to information warfare targeting as well as the current manifestation of information warfare. Next, the challenges presented by the future control and management of information warfare are highlighted. Some initial insights into how information warfare could manifest in the future are shared. This all informs the development of an information warfare future analysis model presented in Chapter 6.

## **5.2 ENVIRONMENTAL SCANNING CONCEPTUALISED**

Environmental scanning is the acquisition and use of information about events, trends, risks and relationships that form part of the external environment of any given phenomenon. This knowledge assists in identifying the future development of these phenomena (Choo, 2001). Breaking this down further, it is possible to identify in more detail what objectives should be pursued in an environmental scanning process. While environmental scanning is primarily focused on the current situation, already future-related thinking issues are raised. This future-orientated nature of environmental scanning is of particular value as scanning can increase and enhance communication and critical thought about future-oriented issues in general (Choo, 1999).

The concept “environment” is defined by Armstrong (2001:780) as conditions surrounding a situation where the “environment includes information about the ranges and distributions of cues, the correlations among them, and the relations between the cues and the event being judged”. Most futurist definitions of environmental scanning are extremely narrow and only refer to the environment outside a commercial company. Often, environmental scanning is done with the view to advance and maintain a sustainable competitive advantage (Choo, 1999). In this study, a broader application of environmental scanning is used. At its broadest level, namely the macro environment, the focus is on the Social, Technological, Economic, Environmental and Political (STEEP) sectors (Kurian & Molitor, 1996:814). Various futurists use different systems to uniquely classify the focus area of their studies (Haberman, 2013). As the focus of research is on information warfare, the applicability of the STEEP sectors would need to be critically evaluated. Haberman (2013) identifies the Environmental (Ecology) Scanning sector as encompassing the natural world around us and understanding how the nature affects humanity and how humanity affects nature. Issues of concern are inter alia global warming, clean water, air quality, agriculture and increasing severity of storms. While these phenomena do have a significant influence on the world currently and in the future, these phenomena do not significantly manifest in the information warfare domain. Additionally the absence of the phenomena such as war and conflict, which go to

the core role of information warfare in society as an additional fully-fledged sector, can be regarded as a significant gap. Therefore, the environmental sector is replaced with a War/Conflict sector creating the Technological, War/Conflict, Economic, Political and Social (TWEPS) macro-environmental hexagon. See Figure 5.1 for a graphical representation of the TWEPS macro-environmental hexagon.



**Figure 5.1: The TWEPS macro-environmental hexagon**

Source: Adapted from Spies, 2005.

This type of model is popular due to its simple structure and application. However, this simplicity is also the model's main drawback because its application often fails to generate a satisfactory degree of precision and comprehensiveness. The risk is that such analyses address no more than the usual surface phenomena (Pillkahn, 2008:86). In order to overcome this constraint a layered and systematic evaluation has been incorporated in the information warfare futures model used in Chapter 6 to identify the main driving forces emanating from this environmental scan.

In scanning the environment of information warfare, it is important to analyse vast amounts of literature and to determine what lies within the ambit of information warfare, what remains outside, and what can transform it. While some of these outcomes are generally seen as unlikely, if they occur, they will have a significant impact on human endeavours. However, being merely unlikely or having a high impact are not sufficient conditions for the manifestation of, say, information warfare; there must also be causes, motivations and reasons why a particular issue is emergent. Emerging issues analysis searches for "small ripples that might one day become tidal waves" (Inayatullah, 2005b).

Building on this, an environmental scan must be equally attuned to the speed, scope and significance ( $S^3$ ) of each challenge identified. Anticipating how, when and why different contexts may interact to disrupt society requires the development of “ripple intelligence” which could serve as an early warning system. Visualising the interactions of simultaneous events as ripples on a pond can help leaders to expect the unexpected and thus be more prepared to seize opportunities (Heidrick & Struggles, 2015:3). However, new concepts usually begin as undeveloped thoughts. Shaping these thoughts into coherent form, informal deliberations and oral discussions are necessary. Over time, new ideas find their way into more permanent media (Molitor, 2003:67).

Masini (1993:83) explained that there appears to be a general awareness among decision-makers that the complexity of reality is such that it has become imperative to look into the future, beyond any one specific field of interest, taking into account national, regional and/or global contexts. Using Coates' observations (1985), the following objectives of an environmental scanning method can be identified:

- Detecting technical, scientific, political, economic and social events and trends important to the phenomena.
- Defining the potential changes, opportunities or threats for the phenomena implied by the mentioned events and trends.
- Promoting a futures orientation in the thinking regarding the phenomena under investigation.
- Alerting policy-makers and other interested individuals to trends that are diverging, converging, slowing down, speeding up or interacting.

Morrison (1992) identified four types of scanning which need to be considered:

- Undirected viewing, which consists of reading a variety of publications for no specific purpose other than to be informed.
- Conditioned viewing, which consists of responding to this information in terms of assessing its relevance to the user.
- Informal searching, which consists of actively seeking specific information but doing it in a relatively unstructured way.
- Formal searching, which is a proactive mode of scanning that entails formal methodologies to obtain information for specific purposes.

As information warfare is a new phenomenon, conditioned viewing is the main approach followed in this study, with the researcher detecting events, trends and risks from the environment that are likely to influence information warfare as national security threat. The environmental scan is also attuned to especially the  $S^3$  (speed, scope and significance) of trends identified.

### 5.3 ENVIRONMENTAL SCANNING IN THE INFORMATION AGE

With the world confronting multidimensional challenges, environmental scanning is one way of managing this complexity. Factors facing humanity include changes in power structures because technology changes, economic contradictions, social and cultural polarisation, which have created new problems of control, understanding, choice and policy-making (Slaughter, 2005b). In order to assist sense-making and analysis, the environmental study is thus focused (as indicated in Figure 5.1) on the TWEPS environments while also taking into account the fact that these environments are exceptionally linked and interdependent. The environmental scan is conducted within the context of the Information Age, in which a knowledge-based society surrounded by a high-tech global economy influences results in cross-cutting impacts of the different environments.

Harknett (2004:18-22) identified at least five inescapable features that can be ascribed to the Information Age. They revolve around the occurrences of accessibility, availability, speed, affordability and recursive simplicity:

- **Accessibility:** The increasing networking of individuals and computers has led in turn to the networking of individual networks. This high (and ever-growing) degree of connectivity has reduced significantly the obstacles to information retrieval. An important advantage brought about by the Information Age is that information retrieval became global and not primarily dependent on being in geographic proximity to the information storage depositories.
- **Availability:** Cyberspace offers significant progress in availability by creating the opportunity for multiple concurrent retrieval of information. Access is also less geographically dependent, meaning that much more information is available than in the past.
- **Speed:** There is an enormous increase in computational and communicative speed. What is distinctive about this age is that vast quantities of accessible information can be disseminated and processed in seconds.
- **Affordability:** The resource base required to utilise the advantages of information technology is relatively low and decreasing rapidly. This does not imply that there are no skill-based or financial barriers, but it proposes that such barriers are becoming less and less significant for general access. Information technology is affordable in the broad sense. In general, it requires the investment of less time for training and money.

- **Recursive simplicity:** The final feature of the Information Age is the inherent recursive nature of computer technology, which supports a clear trend of ever-expanding growth in access, availability and speed with a simultaneous reduction in cost and skill barriers.

These features of the Information Age are impacting the general environment in which information warfare manifests and have become central themes through all environments under investigation. In order to ensure a focused approach, the environmental scan is not an all-encompassing collection of facts pertaining to the mentioned sectors, but centred on the current interrelated trends, changes, relationships and risks in the different environments that have a strategic bearing on information warfare as a growing security threat.

A globalised interconnected future (in terms of the threats posed by information warfare) is awaiting South Africa. Borders have a negligible effect on the two most crucial identified aspects of information warfare, namely the cognitive and technological domains. As information warfare is an issue that transcends borders and other barriers, it is necessary to take an inclusive approach with regard to the environmental analysis.

### **5.3.1 Technological environment**

Technology, in the context of this study, does not only refer to artefacts (devices, machines, equipment or material objects) but also to knowing how to achieve practical purposes in the world. It includes systems and methods which are the result of scientific knowledge being used for practical reasons. Material technologies are much more visible because their roles in change are more identifiable than social and intellectual technologies (laws, institutions and theories) (Cornish, 2004:14-15). As humanity's scientific understanding grows, so too does the ability to engineer instruments to manipulate the world (Rappert & Croft, 2007:5). Intellectual technologies do, however, play a significant role in the changes in society's power structures and remain relevant in terms of the use of information as a power instrument in a world where there is increased consciousness of certain values such as human rights that cross national frontiers (Nye, 2005:260).

Technological progress provides a useful perspective to analyse the rapid phase of change currently experienced in global society. Over the last 100 years, there has been more rapid technological change than ever before in human history (Strange, 1996:7). The main driving force in recent socio-economic development seems to be the accumulation and use of technological knowledge. Therefore, changes in society have speeded up significantly due to rapid technological innovation and progress, which leads to substantial change in the economy, government and institutions of society (Cornish, 2004:20). Through the ages, technological development has been an indispensable trigger for change. In this regard, see Table 5.1 for a summary of the benefits,

uses and effects of the three major technological revolutions experienced by humanity, namely the Agricultural, Industrial and Information Ages. The Agricultural and Industrial Ages have not disappeared; they have become sequentially layered parts of humanity's history of socio-economic and political evolution (Houle, 2013:13).

**Table 5.1: Three technological revolutions**

	<b>Agricultural</b>	<b>Industrial</b>	<b>Information</b>
<b>Origin</b>	Near East, 9000 BC	Britain, 1750	United States, 1944
<b>Catalytic technology</b>	Grain cultivation (wheat)	Steam engine	Computer
<b>Benefits</b>	More food per unit of land; grain storable and tradable	Inexpensive, dependable source of power	Fast, cheap decision-making for problems soluble by algorithms
<b>Uses</b>	Feeding people, safeguarding food supply, trading goods (functions like money)	Mechanised pumps, machine-powered vehicles, power machinery in factories	Mathematical calculations, processing records, word processing, database management, telephone exchanges, etc.
<b>Effects</b>	Population increase, early cities, roads, shipping, accounting, metal-working, wheeled vehicles, writing, scholarship, science	Factory towns, urbanisation, railroads, automobiles, rising living standards, airplanes, surging demand for natural resources – metal ores, coal, petroleum	Faster, cheaper information handling; better management of communications; tighter inventory controls; better distribution of goods; higher standard of living

Source: Cornish, 2004:16.

The current age can also be called the "age of technology", but the more apt name is the Information Age. The idea of the Information Age comes from the writings of Toffler (1970 & 1980), whose "wave theory" of technological and civilization enhancing development argues that human history can be seen as the unfolding of three successive and overlapping technological revolutions or waves (i.e. the agricultural, industrial and informational). Currently, humanity is experiencing the ascendancy of the Third Wave, namely the Information Age, with its associated developmental transformations (Kilibarda, 2003). The benefits of pervasive technologies include economic productivity, e-commerce, global collaboration, efficiencies and change in government and society, information richness, data-rich scientific and technological advances, societal knowledge and political transparency (Pick & Sarkar, 2015:1).

Increasingly, in the Information Age, technology and information are interdependent, with advances in one entailing and dependent on advances in the other. The expanding flow of information, the evolution of the global economy and the creation of the internet are all factors in development, boosting innovation and globalisation (Masini, 2005). ICT remains central to ongoing innovation, strengthening a global networked-based system.

In a network-based system, computers communicate with computers. Information is stored digitally in electronic databases, and because the computers are connected, this means that every digital database in the world is, in principle, accessible from anywhere else in the world by anyone with the authority to access it. All this happens at a very high speed, so there are only insignificant lags. The locations of the individuals and the data have become irrelevant. In this "virtual world" consisting of the information and communication layer, proximity does not matter anymore. Delays remain minimal, with the binding economic constraint not so much how much information can be found, but rather how much information can be processed. Network-based information technology has considerably reduced transaction costs (Spence, 2010:227). Based on developments in the fields of the Internet of Things (IoT), additive manufacturing (commonly referred to as 3D printing) and computing everywhere, the merging of the "virtual world" and the "real world" is an upcoming trend (Carter, 2014).

While computing devices are the most visible symbols of globalisation, ICT is also proving to be one of the most potent agents of change. No area of the world and no arena of politics, economics, society and culture are immune from the pervasive impact of computer technology (Kegley & Wittkopf, 1997:251). ICT can be regarded as a force multiplier. Miniaturisation, growing capacity and software innovation have propelled the rapid worldwide spread of computing devices. These devices owe their growth and impact to a phenomenon dubbed Moore's Law (after Gordon Moore, the founder of Intel), which says that computing power and capacity double every 18 months. Hence, the cost of digital information processing and computing started a long and rapid decline (Spence, 2010:226). This exponential growth has led to the digital revolution influencing practically all spheres of life (Kegley & Wittkopf, 1997:251).

Although ICT and especially the internet are agents of a rapidly globalising world, significant differences exist in the ability of countries to shape (and be shaped by) a computer-driven technocratic world (Kegley & Wittkopf, 1997:252). Despite overall growth, a global digital divide remains pervasive. Worldwide, the geographic patterns of technology utilisation differ widely, with continents and countries having relatively high or low levels of information technologies. Likewise, within states, provinces and regions have uneven geographic distributions of information technologies (Pick & Sarkar, 2015:1). Although the digital divide is a problem throughout the world, developing states struggle far more than industrialised states because of the unequal distribution of digital infrastructure (Parks, 2013:8).

Focusing on the immediate future, key ICT trends include ongoing innovation in integrated applications, storage, display technology, wireless transmission media, the omnipresence or pervasiveness of technology, and continuous innovation with software applications (Butler, 2008: Slide 11). Additional upcoming major developments include the expansion of mobile applications, big data<sup>17</sup> analytics (ITWeb, 2014) and the expanding IoT. The IoT has been defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ITU, 2015). In general, the effects of ICT trends and the Information Age are much more profound than just the explosion of the use of information. Today, ICT has a significant impact on most aspects of modern society and the economy. Intelligence will in effect spread to practically all human artefacts. The decreasing cost and increasing performing power of computing devices have led to the application of information technologies in virtually all corners of society (Arquilla & Ronfeldt, 1997:52). Information technology presents humanity with a remarkable ability to network and to simultaneously localise and globalise (glocalisation), decentralise and centralise, fragment and integrate (Linstone, 2005).

The information revolution is transforming the role that various types of actors play in international relations. The information revolution has altered the role and operation of governments and their policy-makers in four ways. First, more information is available to governments; indeed, governments may have access to too much information. Paralysis through information overload is a real and growing threat, urging policy-makers to prioritise. Second, global networks provide decision-makers with options to centralise or decentralise decision-making. Third, global networks erode the monopoly of information available to governments. Fourth, global networks advance transparency and accentuate global interest and involvement in issues such as environmental challenges, making it difficult for countries unilaterally to take national policy decisions when the problem is global (Aronson, 2001:549). Although states will remain the dominant actor globally, they will be challenged and they will find it increasingly difficult to remain in control. A much larger

part of the population, both within and among countries, has access to the power that comes from information, potentially challenging some governance functions traditionally controlled by government (Nye, 2011:114).

While technological development, especially in the ICT/digital fields, is exponential, this should not be viewed from a technology determinism vantage point. Complexity and change are not all new to the contemporary world, but were already widely discussed in the 1960s and 1970s. Back then, as now, developments in the technical sphere continually seemed to outpace the capacity of individuals and social systems to adapt. Thus, the notion of “out-of-control” technology and fears of vulnerabilities due to dependency on technology are recurring themes in political and philosophical thought (Cavelty, 2007:21). Although fears of technology slipping out of human control now or in the near future are unfounded, technology is having a significant influence on human society in general. Enabled by technological change, humanity is experiencing a series of social, economic and cultural adaptations leading to a fundamental transformation of how the information environment is used by individuals, entities and governments (Benkler, 2006:2). The level to which information technology enhances the potential power projection potential of the individual, entity and government, present potential future challenges.

Technology development in the Information Age frequently results in technology competitive disruptions when technological breakthroughs result in players changing the rules of competition. This can lead to hyper-competition and conditions that are analogous to warfare (Ashton & Klavans, 1997:56). This competition, coupled with the fragmenting consequences of technology, poses significant challenges to government and social harmony, if misused. Changes brought about by technology and especially ICT-related technologies have as mentioned earlier both globalising and fragmenting consequences. See Table 5.2 for the globalising and fragmenting consequences of transport, telecommunication, television and IT technologies. Despite the positive consequences of these technologies, there are also negative influences resulting in potential fault lines in society. This influences the nature of conflict and war in society.

**Table 5.2: Consequences of agents of globalisation**

<b>Agent</b>	<b>Globalising</b>	<b>Fragmenting</b>
Technology, transport, military	Shrinking distance nationally and then internationally	Facilitating Hobbesian tendencies; facilitating terrorism and civil war
Technology,	Extending size and	Social emulsification,

<sup>17</sup> Big data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage and process data within a tolerable elapsed time (Snijders, Matzat & Reips, 2012:1).

telecommunication	complexity of individual's moral community; breaching authoritarian rule	increased loneliness, social differentiation between those with and the majority without access; increased fear of surveillance; facilitating narrow and shifting patterns of relationships; auto-manipulative personalities
Television	Informing; facilitates simultaneous shared images	Desensitising, homogenising, stimulus overload makes superficial, encouraging passivity and intellectual laziness; alienating, reason-destroying
Technology, IT, computers, e-mail, game consoles	Facilitating new institutional agents; convenience; abolishing distance; cyberspace and information highways; can be used as political force multiplier by poor and weak against rich and conventionally strong	Huge increase in surveillance potential; trivialising communication; alienating, reason-destroying games, desensitising, homogenising; excessive powers of processing information trigger feedback crises, especially in global electronics and financial markets; suppressed ability to identify key indicators

Source: Prince, 2002:112-113.

Technology developments, especially networking related technologies, are critical elements influencing the global security environment in the Information Age. Transformative power relations boosted by technology are coming to the fore to stimulate transformative social change (Dator, Sweeney & Yee, 2014:20).

It is expected that the disruptive and destructive potential of technology will play a noteworthy role in the future as individuals and entities explore the potential power projection value of these technologies. While the technological impact has a significant effect on all identified environments, the links between the technological and war/conflict environment are especially relevant for the manifestation of information warfare.

### **5.3.2 War / conflict environment**

Changes brought about by the advancement of technology, especially during the Information Age, also had a profound effect on the war and conflict environment. As Toffler and Toffler (1993:3) stated: "A revolutionary new economy is arising based on knowledge, rather than conventional raw materials and physical labor (sic). This remarkable change in the world economy is bringing with it a parallel revolution in the nature of warfare."

Warfare is the management of violence, not merely its generation. With rare exceptions, it entails the organisation and orchestration of a diverse set of means to achieve definable and often measurable effects. Mobs and terrorists usually ignore these rules in seeking the unrestrained expression of passion or the creation of spectacle almost as ends in themselves (Libicki, 2007:95). While they are rarely a match for a professional military, should it come down to a confrontation this could change the future.

Just as the development of technology was central to the three ages, these ages also resulted in different manifestations of conflict and war. Each age is defined by its primary source of wealth (Toffler & Toffler, 1993:21). The agricultural, industrial and information bases of wealth also decide how conflict is managed. This is so because the way wealth is created largely determines how it is distributed and how society is structured (Hammes, 2004:10). Linked to the ownership of wealth is society's power structures and the potential fault lines for future conflicts.

During the Agricultural Age, war was waged for control of purely local resources. The warriors were either members of the parties in direct control of the disputed land or resources, or, in the case of feudalism, conscripted tenants. However, instead of a tribal system where every person fought, the rise of civilisation led to a professional class of warriors. These warriors became experts in the application of violence to protect the wealth that agriculture allowed a society to produce. Often, another duty was to protect the ruling class from the rest of society (Hammes, 2004:10-11). Despite military innovations such as the use of metal, mobility and machinery, military resources were largely limited to what could be produced and sustained in an agricultural society. This did not prevent the largest military conquests in history such as the Roman Empire and the Mongol conquest from happening, but technology and control did limit the application of military power projection.

During the Industrial Age, which started around the middle of the 17th century, industrialisation allowed a major increase in wealth while simultaneously providing the ability to mass-produce key weapons of war (Hammes, 2004:11). The industrial revolution put society on a mass-driven footing. Larger sectors of the populace came to control resources and assets. This was also the case with the conduct of warfare. It became an attack of society against society, with the involvement of millions of people, including civilians, on each side (Toffler & Toffler, 1993:21). Coupled with this was a significant increase in the sophistication, destructive power and reach of weapon systems as well as the professional management of logistical support for the military. The high point of the Industrial Age was the atomic devastation of Hiroshima and Nagasaki illustrating the mass destruction potential of the Industrial Age.

The Information Age brought with it an increase in management, precision and reaches into new domains of cyberspace and space. This has resulted in new opportunities to build capacity and capabilities based on infosphere developments and not only the traditional industrial power base. According to Grant (2008), the USA armed forces for example face “peer” adversaries in only one area, namely military cyberspace. Hammond (2001) argued that due to globalisation and the emergence of new weapon systems, the character of war is changing in a revolutionary way. The technological transformation in areas such as sensors, communication and computers, space assets, missiles, drone capacities and precision-guided munitions (PGM) is changing war and warfare. Changes impact the mentioned new arenas of conflict, namely space and cyberspace, as well as the way in which it is conducted, referring to the speed and weaponry of conflict. According to Hammond (2001:3), “We are in the process of transforming space, time, energy, matter and information of war and warfare”. The civilian as target of warfare is also a continuing issue (Downes, 2008:2). This is likely to be even more noticeable in future conflicts in which information warfare will play a greater role.

While the core nature of warfare does not change, its character does (Tuck, 2008:116). It can also be expected that states will continue to pursue military technological advantage. However, evolutionary technological development will probably be punctuated by revolutionary departures. Offensive breakthroughs can dictate the pursuit of defensive countermeasures, and defensive advantages will compel the pursuit of offensive innovations. Technological developments will be both seemingly autonomous and directed. As new military technologies emerge, the global diffusion of weapons and military technology is bound to confront policy-makers (Ross, 1993:131).

The notion that a single focus or one conventional military doctrine can guarantee victory in war or conflict is suspect. It is also important to distinguish between levels of war by dividing it into strategic, operative and tactical levels. The levels of war, however, do not only serve analytical purposes in order to understand a complex reality, but also have more direct and practical purposes. The levels of war usually coincide with levels of command, and are therefore a critical part of how armies organise and prepare for war. In this way, levels of warfare are not just a way to

analyse and understand war, but also a tool to plan and wage war (Angstrom & Widen, 2015:168). Military effectiveness may lie more with intangibles, such as the capacity to adapt relative to the opponent, than with technological tangibles, such as information systems or precision firepower. Military effectiveness, in terms of the capacity to defeat an enemy's conventional capabilities, does not necessarily relate in a linear fashion to overall political success, which is the aim in most cases (Tuck, 2008:118-119). This assisted in a significant re-think of military integration of capabilities within a technological driven environment.

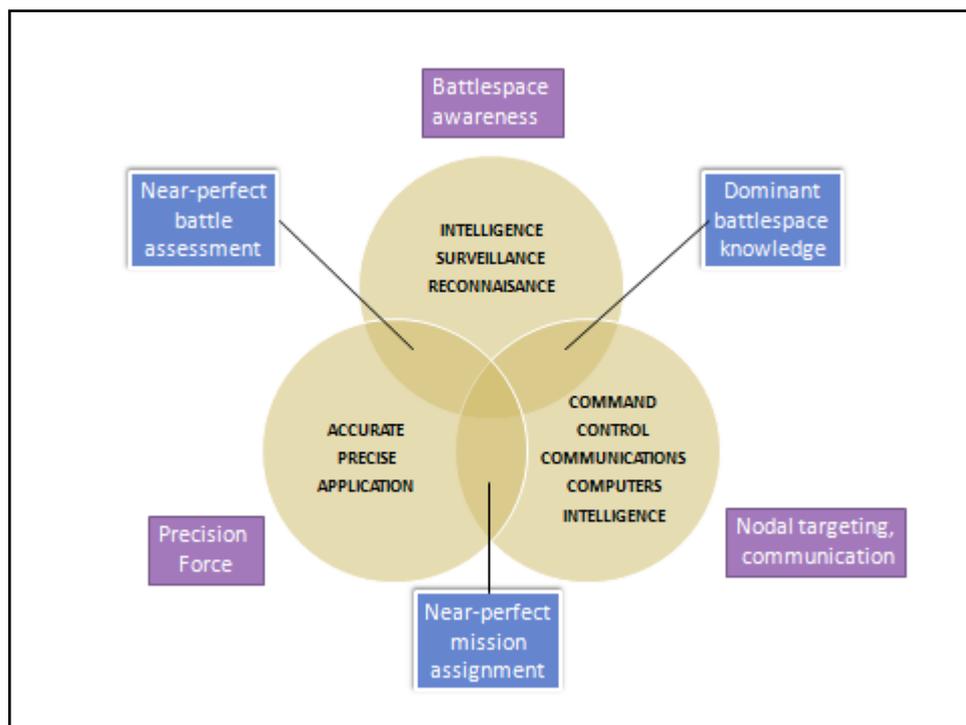
The notion of a revolution in military affairs (RMA) has since the early 1990s gained popularity, especially in the USA strategic community. The RMA, it is claimed, is the result of the interaction between technological change, system development, operational innovation and organisational adoption (Larsdotter, 2005:135). RMA, which applies recent technological developments to the whole range of weapon systems, information-gathering, communication and surveillance, regards the global information environment as having become a "battlespace in which ... technology is used to deliver critical and influential content in order to shape perceptions, manage opinions, and control behaviour" (Kuehl, 2004:4).

Although RMA is a broader concept than information warfare, the two concepts are closely related. In terms of RMA and the hallmarks of the information revolution, such as the transparency of events and the global immediacy of coverage, the concepts of information warfare and cyber warfare play an increasingly important role to the extent that, for some "the most – perhaps only – effective weapon in this battlespace is information" (Kuehl, 2004:4). One of the changes in the conflict/war environment is the blurring of the boundaries between the civilian and the military realms (Cavelty & Brunner, 2007:7), especially regarding the infosphere.

In line with these blurring boundaries, where wars traditionally have regular and irregular components in different areas of operation, modern "hybrid wars" have the tendency to combine these aspects. Hybrid war practitioners apply "conventional capabilities, irregular tactics and formations, and terrorist acts including indiscriminate violence, coercion, and criminal activity" simultaneously (Hoffman, 2007:8). In terms of this model, war takes place in a variety of operating environments, has synchronous effects across multiple battlefields, and is marked by asymmetric tactics and techniques (Hoffman, 2007:24). These tactics are difficult to defeat for militaries that lack the flexibility to shift mindsets on a constant basis, especially since the interconnected nature of modern society is such that hybrid war takes place on three distinct battlefields: the conventional battlefield, the indigenous population of the conflict zone, and the international community (McCuen, 2008:107).

Contemporary thinking about militaries as systems has led to the emergence of two concepts: the "system of systems" and "systemic shock". A system of systems is created through intense networking between systems, utilising new technology (especially digital communications) and

associated procedures to create a more unified whole out of the distinct elements. This allows information to flow much more quickly and efficiently, which, in theory, dramatically increases the speed at which decisions can be made and the tempo at which operations can be conducted. In this regard, see Figure 5.2 for an illustration of the RMA system-of-system argument. Conversely, it is possible to render enemy forces ineffective by destroying their capacity to function as a system, even if the enemy combat elements are still intact. It can be done by introducing systemic shock in the enemy: paralysing the ability of the individual elements in an army/armed group to function together. This can be achieved through a variety of related means, including disrupting enemy communications; attacking command-and-control infrastructure; undermining enemy decision-making through high-tempo operations; denying the enemy information; and undermining their morale (Tuck, 2008:111).



**Figure 5.2: The RMA system-of-system argument**

Source: Baker, 1997:10.

The RMA emphasises the importance of quality intelligence and decision-making in military success. John Boyd developed the notion that conflict can be dissolved through “decision cycle dominance”. The decision cycle laid out by Boyd follows the sequence of “Observe – Orient – Decide – Act”. This became known as the OODA loop. The aim of decision cycle dominance is to get inside the opponent’s OODA loop and to conduct the decision cycle more quickly than the adversary, causing the opponent to lose situational awareness and to become more confused about what is happening. As confusion mounts, the enemy would become paralysed and unable to resist (Jordan, 2008:200-201).

A challenge posed to RMA and other views of the future of warfare is the ability to distinguish that which is transient from that which constitutes long-term change. This is reflected in the tendency to take current and specifically Western experiences, to extrapolate them into the future and to accept them generally as the “nature of future warfare”, ignoring the contingent character of warfare (Tuck, 2008:115).

The roughly 300-year period during which war was primarily associated with the state – first in Europe and then, following the latter’s expansion, in other parts of the globe as well – is coming to an end. If developments since the 1950s provide any guide, future wars will overwhelmingly be of the type known, however inaccurately, as low intensity. Both in terms of organisation and the equipment at their disposal the armed forces of the world will have to adjust themselves to the situation by changing military doctrine, largely jettisoning heavy military equipment to become more like the police (Van Creveld, 1999: 36). The tendency is to predict the war that the military elite would want to fight in the future. It should be noted that since 1945 90% of conflicts have been civil wars fought with relatively simple weapons (Tuck, 2008:116). Confronted with the availability of large-scale nuclear weapons to major powers, interstate war has receded quite significantly (Van Creveld, 1999:33). Governments are thus considering the future of national defence forces based on the ideas of future “wars of efficiency” and “wars of destiny”. Wars of efficiency refers to gradually adjust to what evolves and adjust armed forces accordingly, while wars of destiny refers to choose future military involvement and prepare accordingly (Vreÿ, 2005:372).

Victory in the modern conventional context still requires ground battles, with support from technology and air power. However, the technologies in land warfare are more sophisticated and fundamentally more effective as they combine arms warfare, dispersal, coordination, fire-and-manoevre, and mission command (Tuck, 2008:112-113). In general, political leaders and military planners cannot fully comprehend the new technology with which they must work. The one consistent winner of modern warfare has been technology; the consistent loser has been humanity (Ziegler, 2000:19).

Another way of evaluating change in terms of conflict and war is to look at the main target or Centre of Gravity (COG) of any conflict. An operational centre of gravity is generally an object towards which concerted military force is directed (Duyvesteyn, 2005:75). Hammes (2004) argued that the contemporary conflicts in Iraq and Afghanistan are symptomatic of a new “fourth generation” in warfare. First-generation warfare was horse-and-musket warfare, exemplified by the Napoleonic Wars. Second-generation warfare was the rifle-and-railway warfare that evolved from the American Civil War to the First World War. Third-generation warfare encompassed blitzkrieg and manoeuvre warfare. Fourth-generation warfare (4GW), on the other hand, represents an evolution in insurgency. Fourth-generation warfare is marked by a focus on the higher-level political decision-making of the enemy. Using political, economic and social networks, as well as military action, fourth-generation warfare seeks to undermine the enemy’s political will to fight

(Tuck, 2008:117). In this regard, see Table 5.3 for the evolution of warfare. In essence, these modern hybrid wars simultaneously combine conventional, irregular and terrorist components in a complex challenge that requires an adaptable and versatile military to overcome (Deep, 2015).

Information has a leveraging role in almost all of the modern-day warfare trends, which significantly increases its impact in the war and conflict environment.

**Table 5.3: Evolution of warfare**

<b>Generation</b>	<b>Paradigm</b>	<b>COG</b>	<b>Leverage</b>	<b>Strategy</b>
First-generation warfare	Agrarian (classical)	Manpower	Massed formations	Napoleonic
Second-generation warfare	Industrial (pre-modern)	Assets	Massed firepower	US Army: “Steel on target”
Third-generation warfare	Nonlinear (modern)	Control	Manoeuvring	United States Marine Corps (USMC): “Keep moving”
Fourth-generation warfare	Chaotic (postmodern)	Moral[e]	Information	Special Operations Forces (SOF): “Hearts and minds”

Source: Taipale, 2006: Slide 9.

Practically all developments and expected future advances related to warfare and conflict management emphasise the increasing role of system-based approaches and enabling technologies to strengthen information, intelligence and knowledge in conflict and warfare. The shifting COG reinforces the relevance of information warfare in the Information Age. In the end, the aim of war and conflict remains primary political. As Von Clausewitz (1989) stated, war is an act of violence to compel the opponent to fulfil your will, shifting the focus to the political environment.

### **5.3.3 The political environment**

The political environment encompasses a wide range of issues concerned with the allocation and transfer of power in national governments. In this context, the role of information is crucial. Public policies, rules in the form of legislation and regulation, decision making, stability, allocation and the

arbitration of access to resources form the basis of government functions and constitute the broad political environment. Although there are similarities between the domestic and international manifestations of the political environment there are also differences. International political processes can be seen as the realm of fate, as an anarchic interplay among unequal powers, or as government activities in which some element of choice and consensus may be possible (Bromley, 2004:128). This argument was central to the evaluation in Chapter 2 of the broad strategic international worldviews. The realist, rationalist, critical realist and postmodern worldviews are not representing mutually exclusive perceptions about international relations and security, but are highlighting diverse insights about the functioning of international relations.

While the traditional principles of international relations have at least initially been common to all these worldviews, these principles have never been fully respected. Since the advent of the Information Age and end of the Cold War these principles seem to be increasingly under attack.

These traditional principles of international relations include the following (Ziegler, 2000:118):

- A sovereign state is legally autonomous. It makes its own laws, decides its own legal cases, and is subject to no competing authority.
- A sovereign state has exclusive rights within its borders over its resources and over its population.
- Jurisdiction is territorial, i.e., laws apply to territory, not persons.
- Sovereign states cannot be entered without permission.
- Intervention in internal affairs of a sovereign state is not permitted.
- All international law is consensual. States can give up some sovereign rights but only by their own agreement.
- Consent to agreements can be revoked at any time.
- States may use any means necessary to defend themselves.

Since the end of the Cold War these challenges have included the “extraterritorial application of law” (Ziegler, 2000:118), the impact of international terrorism and efforts by international entities to expand their jurisdiction at the cost of sovereignty. These changes include the following:

- Shifts from strategic geo-political priorities to geo-economic challenges
- The movement from one-party states to the increasing introduction of multi-party democracies in many developing states
- Decreasing inter-state conflict and increasing intra-state conflict

- Regional entities increasing their influence at the expense of national entities
- A shift in the balance of power in the global system where collective security is becoming increasingly significant (ACCORD, 2004).
- A change in the identity of the influential actors in international politics which increasingly includes non-state actors (Weltman, 1995:208).

The initial hope entertained by the “hyper-globalists” actors that the security function of the state would increasingly be absorbed in a globalising world by a multilateral body like the UN proved to be illusory (Patman, 2006:24). The contemporary global political environment is characterised by the interaction of a multitude of actors with various interests in a world that is changing economically, politically and technologically, and that is increasingly becoming interconnected because of globalisation (Balaam & Veseth, 2001:203). According to Oman (1999:37), the core of globalisation is “growth, or more precisely the accelerated growth, of economic activity that spans politically defined national and regional boundaries”. This growing economic but also political, social and technological interconnectedness associated with globalisation creates security challenges.

Globalisation has shown a tendency to empower some while marginalising others, and has at times heightened the combustible tension between individual and group identity. Although it contributes to a steady rise in shared economic interests between and among countries, globalisation provides no sure remedy for international rivalry and suspicions (North Atlantic Treaty Organisation, 2010). The security debate associated with globalisation is increasingly about the effect of modern technology as well as the inequality of power. One of the most significant consequences are the large number of actors and overlapping layers of security policy that create more potential for conflict and make it more difficult to take decisive action in case of disagreement or against disruptive states and terrorist groups. The large number of actors who must be consulted slows down the taking of decisive action by states. Media coverage adds a disincentive to strong action because harm to civilians and innocent bystanders can easily and effectively be communicated. The loss of a single soldier, an everyday occurrence in war, can become a national or even international media event today. These circumstances can give disruptive states and terrorist groups greater room to manoeuvre, turning them into a different and potentially more serious threat to security than in the past (Balaam & Veseth, 2001:204).

The ability of countries to build and sustain partnerships to combat discontent will increasingly depend on bolstering a country’s credibility with the broader global population and forging an ethic of common purpose (McHale, 2009:2). It can be expected that political credibility and international esteem will probably grow in political significance in the future. The Western model of political development and values was dominant up to the 20th century but is increasingly being challenged by the rise of Asia, especially China. The political democratic models as conceived and developed

by the West will not necessarily represent the models for the political environment of the future. At the same time, questions about equality will continue to be raised.

While the 20th century was characterised by war and confrontation, it is possible that the 21st century will be one of competition and marginalisation. All states, especially world powers, will be under increasing pressure to seize strategic opportunities and make sustainable development their top national priority, or face political marginalisation (Lai, 2009:4). At the same time, instant global communication is weakening most forms of vertical authority and strengthening the interests of networked communities. One of the human institutions being weakened is the nation state itself (Nye, 2005:249). National governments, including democratic ones, are losing some of their functional and constitutional importance. Even nation state power, which is concentrated in the free-market democracies, will experience losses to non-state actors, some of whom will exploit national vulnerabilities (Gompert, 1999:66). In the political environment, the role of information has become central, especially in terms of its role in networking.

#### **5.3.4 Social environment**

The communications and information revolution has transformed human interaction and the social environment. In the interconnected world, humanity is inundated with information and more engaged with the wider world than ever before (McHale, 2009:1).

Mobility, expanded networks and information pervasiveness are underlying the social fabric of modern society – now and in the future. Mazarr (1997:11) reiterated that the most important technological advance in the future would be a revolution in information technology as profound as the one that has already taken place, namely a “pervasive knowledge network” in which people have anytime/anywhere access to voice or video communications and the internet or other networked computerised systems. This tidal wave of globalised information is expected to have a substantial influence on national and industry boundaries, autocratic organisations and governments as well as individuals. Disparity in wealth and access to the “pervasive knowledge network” will, however, continue to highlight the causes of social equality.

Another social environment issue of strategic importance for the future is the rise of social media and social networking. Social media are media designed to be disseminated through social interaction, using highly accessible and scalable publishing techniques. Social media support the human need for social interaction with technology, transforming broadcast media monologues (one to many) into social media dialogues (many to many). This trend supports the democratisation of knowledge and information, transforming people from content consumers into content producers (Social-Media.com, 2009).

The consequence of this development is that the following characteristics form the core of social media (Social-Media.com, 2009):

- **Participation:** Social media encourages contributions and feedback from everyone who is interested. It blurs the line between media and audience.
- **Openness:** Most social media services are open to feedback and participation. These services encourage voting, comments and the sharing of information. Consequently, there are rarely any barriers to accessing and using content.
- **Conversation:** Whereas traditional media is about “broadcast” (content transmitted or distributed to an audience), social media is seen as a two-way conversation.
- **Community:** Social media allows communities to form quickly and communicate effectively. Flash as well as longer term communities sharing common interests are created locally and/or globally.
- **Connectedness:** Most kinds of social media thrive on their connectedness, making use of links to other sites, resources and people.

Social media have created changes where the significance of institutions is being replaced by the significance of processes. Where distribution was significant during the Industrial Age, distribution through the internet now makes content, conversation and community even more important (Stacy, 2008). However, digital social developments are also linked to threats. Firstly, new digital technologies have a profound impact on everyday life, social relations, government, commerce, the economy and the production and dissemination of knowledge. People's movements and their purchasing habits, online searches and online communication with others are now being monitored in detail by digital technologies. Humans are increasingly becoming digital data subjects (Apple, Ball & Gandin, 2010:9). Secondly, every conflict or war is now also a social-media conflict or war (Ingram, 2012). Various threats, such as social media vulnerabilities, malicious code and social engineering, illustrate that social media is a tool that can be used offensively in information warfare (Van Niekerk & Maharaj, 2013:1177).

The shift to participation and content creation has increased the significance and influence of the general public in terms of participating in the current political, conflict and economic dialogues. Efforts to control such interaction by governments are much more difficult, while the global opportunities for like-minded individuals to cooperate and agitate have been boosted significantly.

### 5.3.5 Economic environment

Just as the social environment has changed, the global economic environment is also being transformed with growing interdependence, automation, collaboration and globalisation as major trends. There is an emergent interdependence among states, especially in the economic spheres. This is a consequence of the rapidly growing transaction rates between societies worldwide. Closer and multidimensional contact between societies and entities constitutes one of the fundamental

forms of recent system changes (Holsti, 1980:23). According to Naisbitt (2009), this global integration could lead to national economies eventually being integrated into the global economy.

These trends are causing a fundamental shift in the global economic order. The changes in the global economic order is said to produce a new multi-polar world with more mid-level powers from various regions. One of the dominant features of the new multi-polar world is the dramatic increase in the diversity of cultures, religions, worldviews, economies, political regimes and legal systems. The new order will increasingly require, and be reflected in, a change in existing institutions and how they operate, as well as the creation of new institutions. Although the rise of new powers has often resulted in war in the past, there are some grounds to hope that this time will be different. But even if military conflict between old and new powers is avoided, a new vision for a more equitable world, combined with feasible development agendas, is urgently needed to ensure a more just world in which global resources and burdens are more fairly shared by all (Peerenboom, 2011:43).

Economic integration and the opening up of international trade have helped many countries to grow more quickly. International trade continues to assist countries in which exports drive economic growth. Export-led growth was key to the industrial policy that resulted in lifting millions of people in Asia out of poverty. Globalisation has reduced isolation in the developing world and has provided many people with access to knowledge which is unprecedented in history (Striglitz, 2002:4). This growth has been diminishing since the economic crisis of 2008, calling the sustainability of this approach to growth into question.

Globalisation also comes with negative economic consequences. A growing divide between the haves and the have-nots is leaving an increasing number of people in the developing world in dire poverty, living on less than a dollar a day. Despite repeated promises of poverty reduction, made since the last two decades of the twentieth century, the number of people living in poverty (with an income of less than US\$2 a day) is 2.2 billion (2011 statistics) (The World Bank, 2015). According to the UK charity Oxfam, the richest 1% now has as much wealth as the rest of the global population combined (BBC News, 2016). This continuing inequality will result in a change in the identity of the economic powerful and a change in their relative position due to uneven economic development. It is likely to increase the propensity of conflict (Weltman, 1995: 220). Thus, globalisation has not succeeded in reducing poverty; neither has it succeeded in ensuring sustained stability (Striglitz, 2002:6). The digital divide between the developed and developing world continues to endure. Despite some progress, a high level of inequality persists in access to ICT: 82% of people in the developed world use the internet compared to 35% in the developing world and 10% in the least developed countries (LDCs) (itu4u, 2015).

Pressure will mount on the multi-lateral level to promote sustainable equality and stability globally. The marginalisation of many countries in the global economy, particularly those in Africa, and the question of coherence in global economic policy-making between the global financial institutions,

such as the International Monetary Fund (IMF), the World Bank and the Asian Infrastructure Investment Bank (AIIB), constitute key challenges confronting the international community in the context of an integrating global economy and multi-lateral participation in efforts to restrain global environmental challenges.

Economic vulnerabilities have also increased. Robb (2007:14-15) observed that guerrillas or terrorists now possess “the means to bring a modern nation’s economy to its knees and thereby undermine the legitimacy of the state sworn to protect it. Furthermore, attacks can derail the key drivers of economic globalisation: the flow of resources, investment, people and security.” Those who adopt this form of warfare are global guerrillas who represent “a broad-based threat that far exceeds that offered by terrorists or the guerrillas of the past”. Many of these mentioned capacities are within the information domain.

The most globally advanced economies have made two parallel shifts that, paradoxically, reduce the limitations that market-based production puts on the pursuit of the political values central to tolerant societies (Benkler, 2006:14):

- The first shift has been in the making for more than a century. The centre of the global economy is shifting to be based on information (such as provided by science, accounting, financial services and software) and cultural production (such as provided by films, fiction and music). The manipulation of symbols is increasingly becoming a significant part of the contemporary economy.
- The second is the shift towards cost-effective communication technologies, built on inexpensive processors with high computation capabilities and interconnected in a pervasive network, such as is currently the case with the internet.

The second shift has strengthened the role of non-market production in the information and cultural production sector, which is organised in a radical and more decentralised pattern than during the 20th century. The first shift means that these new patterns of production, namely radically decentralised and non-market orientated production, will emerge at the core rather than at the periphery, especially in the more advanced economies. This will enable social exchange and production to play a much larger role alongside market-based and property-based production than ever before (Benkler, 2006:14-15). The collective outcome of trends such as growing automation, digitalisation, stagnant wages, the rise of artificial intelligence (AI) and globalisation will all potentially contribute to unemployment becoming a significant future challenge (Ford, 2015:24).

This greater reliance on the information economy and its cyber elements have increased the vulnerability of most of the advanced economies as well as emerging economies such as South

Africa. These vulnerabilities will be impacted by the increasing manifestation of information warfare.

### **5.3.6 Enhancement of the power of networks, innovation and transformation**

Three cross-cutting trends have been identified that are fundamental to all five environments. These three trends are substantially different in the contemporary world compared to anything in past human experience. These trends also adhere to the identified speed, scope and significance requirements to warrant their identification as “ripple intelligence” issues. The first cross-cutting issue is the level of integration of the world community and the rise of networks, especially social networks. The second issue is rapid innovation, especially in the spread of technology, which has resulted in the simultaneous emergence of a host of new middle-ranking military, political and economic powers across the world, while at the same time generating significant inequality between states, groups and individuals (Harvey, 2003:10011). The third issue is accelerated societal change which is resulting in transformation being a constant reality that affects nearly all social entities.

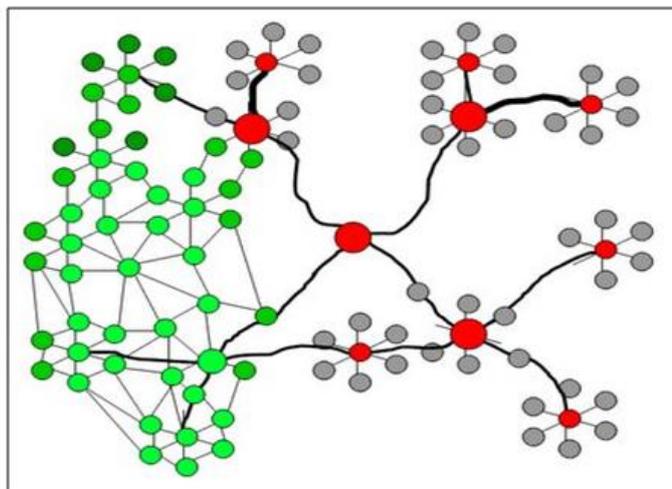
Decentralised non-hierarchical information systems are becoming more prominent after centuries in which centralised bureaucracy has been in the ascendant. As shown in the environmental analysis, this is largely because of ever-expanding global digital communication networks. The centralised model had all the advantages within an environment in which communications are slow and unreliable. In the hierarchical design, limited connecting links exist between any two nodes in the network. The distributed model, on the other hand, may require many more intermediate links (hundreds or even thousands) to connect a given pair of nodes. When all communication has to pass through a central node, the system gets congested at the command point. In contrast, distributed structures in a flat network can form, emerge, perform their mission, and disappear in a short time span (Bodissey, 2007).

Even within the distributed network, certain individuals and entities in the network remain significant. Key issues impacting the centrality of the individual and/or entity in the network include the number and quality of ties to other actors; the notions of closeness and distance based on communication paths among the actors in the network; the notion of cohesive sub-groups; the extent to which the relationships and transactions within the network are regulated by explicit or tacit rules; and the diversity and number of actors within the network (Williams, 2001:67). Taking into account the asymmetric nature of information warfare, as explained in the previous chapter, the nature of the network remains significant for the manifestation of information warfare. In this regard, the rhizome<sup>18</sup> network manifestation is relevant.

---

<sup>18</sup> Deleuze and Guattari first used the term “rhizome” as an analogy for patterns of human organisation.

The rhizome approach to networks offers a useful model for the future manifestation of information warfare. Rhizome takes its name from botany, namely from plants such as bamboo, aspen and ginger that spread via a connected underground root system. Deleuze and Guattari (1980:29) used rhizome as a metaphor to refer to a non-hierarchical form of organisation. Vail (2007) has extended this metaphor, referring to rhizome as an alternative mode of human organisation consisting of a network of minimally self-sufficient nodes that leverage non-hierarchical coordination of economic activity. The two key concepts of rhizome are self-sufficiency, which eliminates the dependencies that characterise hierarchy, and loose but dynamic networking that uses the "small worlds" theory of network information processing to allow rhizome networks to overcome information processing burdens typical of hierarchies. Rhizome therefore refers to an organisational pattern characterised by interconnected but independent networks of entities. See Figure 5.3 for an illustration of a rhizome network.



**Figure 5.3: Rhizome network**

The rhizome network provides application possibilities for both the cognitive and technological elements of information warfare. This includes using cyber networks for malicious software applications and for cyber mobilisation. Cyber mobilisation is a process of mobilising support to concentrate force against critical points. In essence, cyber mobilisation is a form of conflict requiring popular participation; is not the normal cyber-related activities that aim to disrupt websites. Cyber mobilisation requires public participation for success. Cyber mobilisation offers non-state and state actors three main advantages: reach, discretion and movement-building. Followers who are unable to directly participate in a struggle, such as Diaspora groups, are now given the ability to contribute and strengthen their bonds to causes such as participating in psychological operations or carrying out crude hacking attacks. As the efforts of many different geographically dispersed users are incorporated, cyber mobilisation also allows movements and states to multiply the effectiveness of their actions (Elkus, 2009).

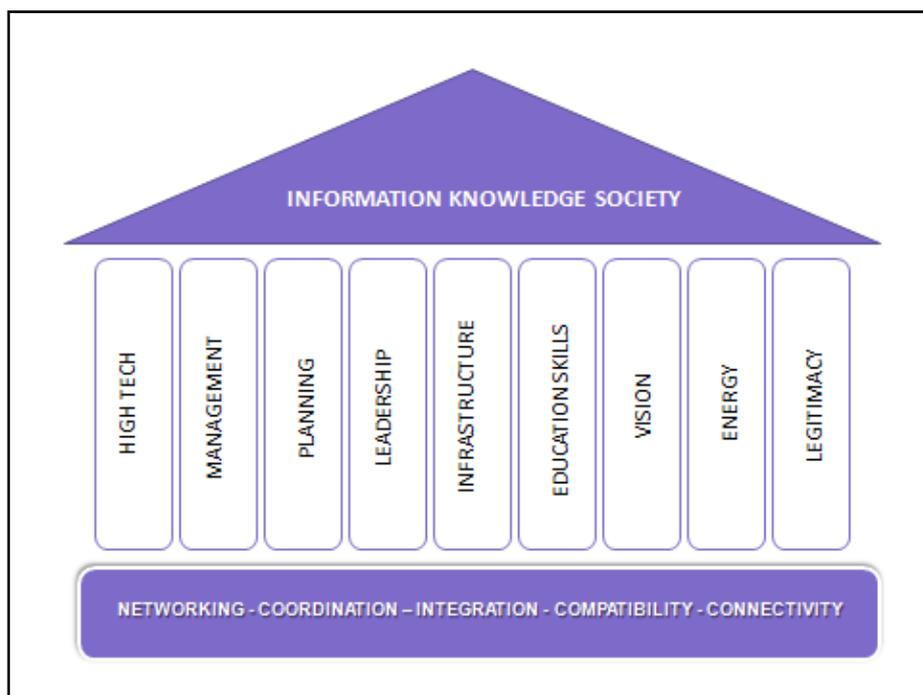
The environmental scan also highlighted the strategic and tactical risks that are ingrained in the information-relevant issues in the TWEPS macro environments. The three cross-cutting trends are compatible to rhizome-like behaviour increasing the threats posed by information warfare to national security. A crucial next step is to focus on the identification of the targets of information warfare and on how information warfare currently occurs.

#### 5.4 INFORMATION WARFARE TARGETS

Information warfare targets are multi-dimensional, focusing on tactical and strategic targets. The environmental scan highlighted the significance of growing interdependence and globalisation in economic prosperity, exposing the commercial networks and the global service sector as highly vulnerable to all constituent elements of information warfare, namely netwar, cyberwar and information operations.

In Chapter 4, two different but related broad targets of information warfare were identified, namely the cognitive and the technological structures that manage modern society. Netwar and psychological operations target networked relationships and decision-making processes. These targets are accessed mainly by influencing perceptions. Cyber warfare, on the other hand, targets information systems with the intention to alter data and information.

Information warfare is primary targeted at the power structures in any state. These structures are part of the complex and inter-related processes and services underlying the information structures in society. In this regard, see Figure 5.4 for an illustration of the pillars of an information society.



**Figure 5.4: The pillars of an information society**

Source: Own Compilation

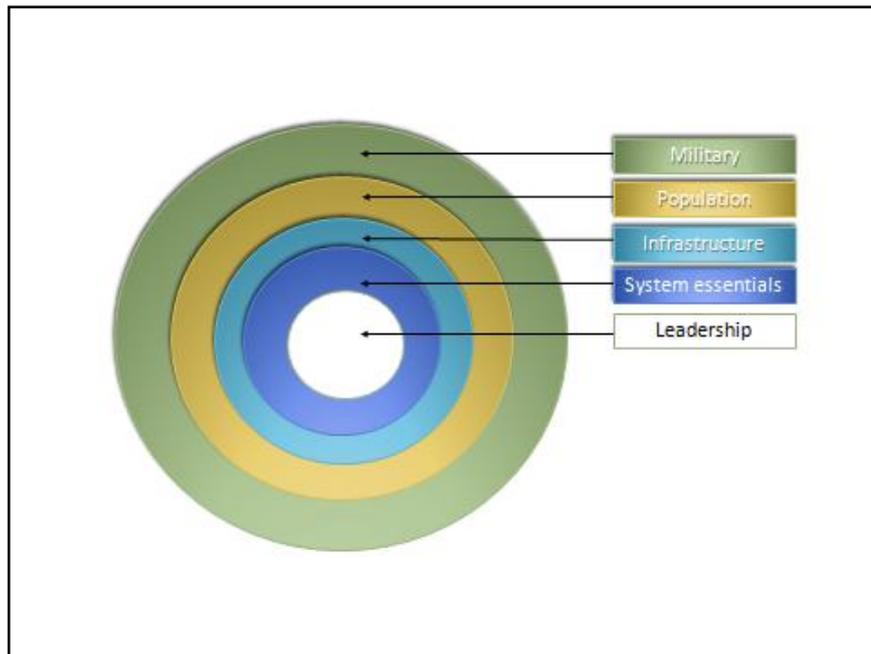
Power structures in the information society include the following:

- Structures and processes ensuring the diffusion of high technology in the economy.
- The effective management of physical, digital, financial and knowledge infrastructures.
- Planning and forecasting to ensure good governance and development.
- Leadership with the aim of overcoming challenges pro-actively, not reactively.
- Infrastructure functioning effectively, especially in terms of ICT infrastructure.
- An education system that produces the skills levels appropriate for a knowledge society.
- Grand/strategic vision for the future and progress.
- The effective management of energy resources to ensure sustainable growth.
- The legitimacy of the government and other role-players in society.

All of these pillars present potential targets for information warfare related actions. In the case of developed and developing states, all the pillars are fairly vulnerable to current and potential future disruption. In an information society, these pillars represent three types of assets which could be identified as information warfare targets, namely physical assets, soft assets and psychological assets (Cronin & Crawford, 1999:258). The physical assets which can be targeted include the adversary or enemy's information and communications systems using conventional warfare techniques. The soft assets can be degraded by using external actors and corrupt insiders to break firewalls and degrade the targeted information systems using malicious software. The psychological assets can be negatively influenced by the silent penetration of the target's information and communication system to manage perceptions, shape opinions and foster deception.

In this study, kinetic energy, or the use of military firepower to eliminate targets such as communication or computer nodes, will not be regarded as information warfare as this is not materially different from attacks on infrastructure during war. Information warfare is not directly lethal and thus in essence non-lethal. The increased utilisation of sensors, especially in terms of the IoT, might make some information warfare actions lethal in the future, but this will probably not become a central information warfare capacity. A layered view of information warfare targets is

presented by Taipale, stretching from national leadership at the core to the military structure at the outer layer, as illustrated in Figure 5.5 below.



**Figure 5.5: Warden's five targeting rings**

Source: Taipale, 2006: Slide 23.

While the risk of information warfare posed to states may be generally regarded currently as low to medium, taking into account the growing interest and spending by governments, groups and individuals on such a capacity, this risk is rising. The medium and long-term threat assessment of information warfare is significant. Already the World Economic Forum (WEF) identified cyber attacks as well as data fraud and theft among the 10 most likely global risks (World Economic Forum, 2015:3).

Even a cursory survey reveals that developing states possess highly developed information warfare capabilities, and they continue to develop a new and more sophisticated information warfare arsenal. Most of the developed and some developing countries have at least tested their capabilities, if they are not already using them in actual attacks against their adversaries. Therefore, it would be prudent to assume that these capabilities have been tested and even used in the recent past (Singer & Friedman, 2014:31).

In most developed and developing countries, five key vulnerable access points exist which, if intruded, abused, manipulated or destroyed, could cause serious damage to society, namely:

- Critical infrastructural components regulated by information-driven electronic communication systems: These include all computer-managed systems affecting

routine daily life, such as the ICT systems, media, electricity, water and transport, particularly in large metropolitan areas.

- The computerised financial world: Due to unauthorised intrusions, large sums of money are electronically diverted internationally. Institutions like the World Bank are constantly investigating measures to curb this.
- The communication systems of government departments.
- The military/intelligence environment: The management of sophisticated countries' military infrastructure is computerised and dependent on centrally coordinated electronic communication.
- The internet: The internet is increasingly becoming central to public, economic and social activities within society. Disruption represents a significant power projection capability.

The manifestation of information warfare related attacks on government and business networks during conflict situations are compelling cases of state-sponsored governmental information warfare power projection activities. As information technology is constantly advancing and as information warfare can be carried out anonymously with a high probability of success, state-sponsored information warfare attacks on networks are expected to rise in frequency and sophistication.

## **5.5 THE MANIFESTATION OF INFORMATION WAR**

While the concept of information warfare has largely been developed on a theoretical level, based on the start of the Information Age and the resulting technological change, it has also manifested as a distinct power projection instrument in the contemporary international system. It is necessary in this chapter to provide an overview of how information warfare has recently manifested globally before using futures methodologies to identify the most significant driving forces leading to the possible future manifestation of information warfare.

Information warfare has become so prevalent that incidents are reported in the international media on a daily basis. In order to illustrate this contemporary manifestation of the constituent elements of information warfare – namely netwar, psychological operations and cyber warfare – its manifestation from the early 1990s to 2015 will be briefly discussed. As indicated in Chapter 4, some elements of information warfare, in particular those related to netwar and psychological operations, have been part of warfare since the earliest times. Cyber warfare, however, is new. Cyber warfare is associated with the large-scale use of ICT during the Information Age, while the capacity for both netwar and psychological operations have also increased exponentially as a result of modern technological innovation, high levels of inter-connectivity and general progress within the ICT sector.

### 5.5.1 Overview of information warfare manifestation from 1990 to 2015

The 1991 Gulf War led to widespread realisation of the importance of information superiority in modern conflict. This war was regarded as the first information war (Campen, 1992:vii). During this conflict the USA significantly relied on information superiority in terms of both operations and weapon systems. In the USA, this realisation had an almost euphoric quality (Eriksson, 1999:57), resulting in interest in the notion of a revolution in military affairs (RMA). RMA, it is claimed, is the result of the interaction between technological change, system development, operational innovation and organisational adoption. These developments combine to fundamentally change the character and execution of war in general (Larsdotter, 2005:135). The notion that conflict reflects the nature of society is not new, but the insight that information society warfare may be quite different from its industrial society counterpart is significant (Eriksson, 1999:57). RMA, which is developed because of the application of recent technological developments to the whole range of weapon systems, information-gathering, communication and surveillance, regard the global information environment as having become a “battlespace in which ... technology is used to deliver critical and influential content in order to shape perceptions, manage opinions, and control behaviour” (Kuehl, 2004:4).

One of the first active utilisations of the internet for advancing a political agenda during a conflict situation was the so-called Zapatista rebellion in Mexico. On 1 January 1994, rebel leader Marcos led Zapatista<sup>19</sup> (Ejército Zapatista de Liberación Nacional, or EZLN for short) rebels in a series of attacks in the Mexican state of Chiapas. What made this unrest unique was the fact that the Zapatistas in Mexico were among the first to supplement their actions with psychological operations, extensively using the internet. Long after all military operations ceased, news of the Zapatistas and their struggle was distributed through the internet to media around the world. While the Zapatistas have not gained from military operations their internet strategy proved far more successful in obtaining political concessions from the Mexican government (Mayer-Schoenberger & Brodnig, 2001:24). The Zapatistas caught the Mexican government unprepared for cyber-mobilisation. The Zapatistas showed how effective networking using the new media could be. In so far as these networks can influence and constrain the actions of governments at all levels, they become an important element in power projection beyond the traditional influence that a small local insurrection could have (Riordan, 2003:6).

During the mid-1990s, netwar and psychological operations were used during the North Atlantic Treaty Organisation led (NATO-led) operations in the former Yugoslavia as Western leaders responded to the use of the media by Bosnian, Serb and Croatian political leaders to mobilise

---

<sup>19</sup> The Mexican rebels, drawing support from the indigenous (Indian) population, called themselves “Zapatistas” after Emiliano Zapata, a prominent figure in the Mexican Revolution (1910-1920) (Ziegler, 2000:122).

support. Originally, the Serbs used government-controlled media to target only Serb citizens with its messages (rather than the international community) (Richter, 2009:104).

After the USA deployment as part of the Dayton Accord Implementation Force (IFOR) in December 1995, USA commanders soon found that the Information Operations (IO)<sup>20</sup> doctrine failed to recognise the effect that public information had on local populations. Local and international news media, as well as the growing online community, had a remarkable influence on the population that IFOR was attempting to stabilise. Given IFOR's mission to enforce the Dayton Peace Accords and public information's predominance on the populace, it became virtually impossible to completely separate public diplomacy from information warfare (Richter, 2009: 104). While not ignoring the role of technology, these lessons emphasise the human dimension and the need to develop an understanding of social and cultural structures, both formal and informal (Richter, 2009:105). Public diplomacy has become a significant part of both combating and conducting the psychological operations part of information warfare.

Although only revealed in 2010, the first known case of confirmed physical damage caused by a cyber warfare related action was Stuxnet, the sophisticated digital weapon the USA and Israel launched against industrial control systems in Iran in late 2007 or early 2008 to sabotage centrifuges at a uranium enrichment plant. Since then experts have warned that it was only a matter of time before other destructive attacks would occur. Industrial control systems were found to be rife with vulnerabilities, since they manage critical systems in the electric grid, water treatment plants, chemical facilities and even in hospitals and financial networks (Zetter, 2015).

In 2007, the first known incidence of a cyber warfare assault on a state also took place. During May 2007, Estonia was the victim of a sustained cyber attack which lasted for three weeks. The attacks were provoked by the removal of a war memorial statue of a Soviet soldier from a location in central Tallinn, the capital of Estonia (Kobilnyk, 2008). This attack, which temporarily brought down Estonian ICT networks, began with a flood of bogus messages targeting government servers through "distributed denial of service" or DDOS attacks.<sup>21</sup> This approach harnessed "botnets" (massive networks of interconnected computers) to bombard targeted networks with information requests while masking the location of the primary attacker. This is done by hackers who took control of tens of thousands of computers around the world without the knowledge of their owners and directed computer traffic at Estonian servers (Bruno, 2008). Estonian ministers blamed the Russian government for instigating the attacks, an accusation Russia denied. Only one person has ever been charged over the attack, a member of Estonia's ethnic Russian minority (Leyden, 2009).

---

<sup>20</sup> In the USA the term information operations is used for information warfare.

<sup>21</sup> Most of the ICT infrastructure in Estonia was built after the 1991 breakup of the Soviet Union. Consequently, the infrastructure is heavily dependent on the internet, more so than most other states. In addition, because Estonia is a small state, internet access to the entire country can easily be disrupted. The flow of consumer staples such as food was hampered in Estonia when the internet went down (Richards, 2009).

Following the Estonia experience, the North Atlantic Treaty Organisation (NATO) began to recognise that cyberwar and information warfare in general have become a new sphere of conflict and that they needed to develop strategies to counter it. The growing significance of the internet and connectivity for the global economy will increase the potential negative impact of hackers launching devastating attacks on the world economy. In order to counter such threats, a group of NATO members, including the USA and Germany, in 2008 established an internal cybersecurity think tank in Estonia. The Cooperative Cyber Defence Centre of Excellence analyses emerging viruses and other threats, and passes on alerts to sponsoring NATO governments (Morozov, 2009). Cyber defence is now part of NATO's core task of collective defence (North Atlantic Treaty Organisation, 2015).

Although, as stated earlier, for the purposes of this study, the kinetic aspects of war are not regarded as part of information warfare, it should be noted that, in practice, information warfare can be used in conjunction with kinetic operations. An example of this was the use of cyber warfare techniques and bombing by the Israel military prior to its 6 September 2007 strike on an alleged nuclear facility at Dayr az-Zawr, Syria. This was done to blind Syrian air defences. Unnamed USA intelligence and Israeli military sources stated that the main attack by the Israeli Defence Forces (IDF) was preceded by an engagement with a single Syrian radar site at Tall al-Abuad near the Turkish border. The radar station "was assaulted with what appears to be a combination of electronic attack and precision bombs", causing the whole Syrian air defence radar system to go offline "for a period of time that included the raid". The sources said the Israeli attack "involved both remote air-to-ground electronic attacks and penetration through computer-to-computer links" (UPI, 2007).

Preparations for future larger-scale cyber warfare are being increased in developed countries in particular. During a war game that the USA Department of Homeland Security sponsored in March 2008, called Cyber Storm II, a large, coordinated attack against the USA, Britain, Canada, Australia and New Zealand was envisioned. It studied a disruption of chemical plants, rail lines, oil and gas pipelines and private computer networks. This exercise and similar studies concluded that when attacks go global, the potential economic repercussions increase exponentially (Sanger, Markoff & Shanker, 2009).

The Georgian-Russian war of 2008 illustrated that information warfare has also become an integral part of inter-state conflict. This war started when Georgian forces at midnight of 7 to 8 August 2008 launched a heavy artillery barrage against the breakaway South Ossetia and sent at least two battalions into the capital of Tskhinvali. Russian forces responded with a full-scale invasion and air war (Hahn, 2008). The cyber aspect of this conflict started soon after the invasion of South Ossetia with Georgian web pages being defaced and servers crashing as a result of dedicated DDOS

---

attacks. Pro-Georgian hackers responded, attacking local government sites in South Ossetia and Russia (Thomson, 2008). There were, however, no reports of attacks against critical infrastructure, such as the electronic jamming of stock exchanges (Antonopoulos, 2008). Georgia also launched a significant psychological operation aimed at drawing the West into the war (Hahn, 2008).

Both netwar and psychological operations have also been extensively used in Iraq. The decrease of hostilities in early 2008 has been attributed to the USA military dropping its mainly techno-centric approach to conducting the war and starting to focus on psychological approaches linked to Iraq's social, political, tribal and cultural networks instead (Mediatechno Blog, 2008).

The social network dimension of this phenomenon is, however, probably even more important for the future manifestation of information warfare. The creation of social networking groups is sometimes supported by governments. In this regard the USA government, for example, supported the creation of the Alliance of Youth Movements (AYM) launched in December 2008 with a summit in New York; the AYM gathered together an ensemble of media corporations, presidential consultants, social network entrepreneurs and youth organisations, under the auspices of the State Department. The USA State Department focused specifically to harness the power of social media. The AYM produced a Field Manual and a series of How-to videos (How to Create a Grassroots Movement Using Social-Networking Sites, How to Smart Mob, How to Circumvent an Internet Proxy). The goal was to have youth leaders from around the world learn, share and discuss how to build powerful grassroots movements (Bratich, 2009).

These initiatives are neither completely emerging from below (grassroots) nor purely invented by external forces (the astroturfing<sup>22</sup> done by public relations groups). However, these emergent groups are seeded (and influenced) to control the direction of the movement. Methods used extensively in the election of President Obama in the USA presidential election are being used for sanctioned "democracy" movements elsewhere in the world (Bratich, 2009). The development of the so-called coloured revolutions (popular uprisings which resulted in governments falling or placed under pressure) which started in Georgia, has a strong information warfare base, encompassing netwar, psychological operations and sometimes even elements of cyber warfare. During these uprisings the use of communication technology and the psychological operations to mobilise opposition against governments have been central to its successes.

During 2009, the Israel-Hamas conflict in Gaza expanded the use of social media as an instrument to support conflict-related actions in especially cyberspace. In Gaza, after a provisional ceasefire has been declared in February 2009, the information warfare related to the cyberwar, netwar and

---

<sup>22</sup> Astroturfing is a term describing formal political, advertising or public relations campaigns, especially within the blogosphere, seeking to create the impression of being spontaneous "grassroots" behaviour, hence the reference to the artificial grass, AstroTurf (Webopedia, 2009).

psychological operations continued for some time. Israel and its opponents have taken to the internet to wage cyberwar against each other, deploying especially crowd-sourced information “militias”. The Israeli IDF and Foreign Ministry extensively utilised YouTube and Twitter to advance their positions. A group of Israeli supporters set up a botnet that allowed users to add their computers to create a substantial launch pad for disrupting pro-Hamas servers (Elkus, 2009). The Israeli government also launched a campaign to dominate the blogosphere, while the Israeli military kept the international press off the battlefield to minimise negative publicity (Hodge, 2009). Opposing Israel, a pro-Hamas group with the moniker “Team Evil” launched attacks against pro-Israeli hacker groups using DDOS attacks. Anti-Israeli protests were also organised through Twitter, Facebook and other participatory social networks (Elkus, 2009).

Increasingly, states and non-state entities are expanding the scope of intelligence collection using the internet. For example, in early 2009, cyber experts based at the Munk Center for International Studies at the University of Toronto, Canada, have discovered that since 2007, the Tibetan government-in-exile in Dharamsala, India, was the focal point of a computer monitoring network called GhostNet, which has penetrated the computer systems of the private offices of the Dalai Lama and other Tibetan targets. GhostNet was the biggest cyber-espionage network discovered up to that stage, as it infiltrated 1 295 computers in 103 countries over a period of 22 months. According to the study, close to 30% of computers infiltrated can be regarded as high-value diplomatic, political, economic and military targets, including computers of the Asian Development Bank (ADB) and NATO. These targeted computers were in the USA, Germany, India, Pakistan, Indonesia and the Philippines. Although the Munk Center experts refrained from naming the Chinese government as the perpetrator of these attacks, the report stated that their discoveries were the result of an investigation into alleged Chinese cyber espionage against Tibetan institutions. A study of the computer systems of the Tibetan government-in-exile led them to GhostNet computers, most of which were located in China (Basu, 2009).

During June 2009 the Iranian government “turned off” the internet right before, right up to and during the election. As soon as it was restored there were DDOS attacks on then President Ahmadinejad’s personal website and several government sites in which an estimated 500 000 botnet computers participated (Coleman, 2009). In the aftermath of the Iranian election, Web 2.0<sup>23</sup> and social media technology played a vital role in organising protest actions in the wake of a media blackout by the Iranian government (Dale, 2009). Online sites have been uploading amateur pictures and video, and Twitter, Facebook and blogs have been platforms for protesters to

---

<sup>23</sup> Web 2.0 refers to a perceived second generation of web development and design that facilitates communication, secure information sharing, interoperability and collaboration on the internet. Web 2.0 concepts have led to the evolution of web-based communities, hosted services and applications such as social-networking sites, video-sharing sites, wikis and blogs. The term Web 2.0 was first used by Eric Knorr, executive editor of InfoWorld, in the December 2003 special issue of the business IT magazine CIO, in an article titled “Fast Forward 2010 - The Fate of IT”. The term Web 2.0 refers not to a specific development but to the cumulative changes in the ways software developers and end-users use the web (Balagangadharan, 2009).

coordinate and exchange information (BBC News, 2009). With the authorities blocking text messaging on cell phones, Twitter became an alternative source of information and coordination of activities. While the Iranian government endeavoured to block Twitter posts, opposition supporters used proxy sites or other methods to circumvent the official barriers (Landler & Stelter, 2009). The value of Web 2.0 for information warfare includes user participation, dynamic content, metadata, web standards and scalability. Further characteristics, such as openness, freedom and collective intelligence by way of user participation, can also be viewed as essential attributes of Web 2.0 (Balagangadharan, 2009).

During July 2009, the Chinese government disconnected Xinjiang, China's far western province, from the internet. This followed when a protest in the capital Ürümqi by young Uighur men (of the area's indigenous Turkic population) turned into a riot against the Han Chinese, in which at least 197 people were killed. This action resulted in a change in information strategy from Uighur dissidents by not pursuing mobilising activities on the internet. The Uighur continued to consume digital media, but increasingly in off-line form, by using DVDs, CD discs and flash drives (Palmer, 2015).

A series of coordinated cyber attacks were also launched during July 2009 against major government, news media and financial websites in South Korea and the USA. The attacks also involved botnet computers, causing websites to crash. The South Korean National Intelligence Service (NIS) estimated that approximately 20 000 hijacked computers, most of them in South Korea, had been used to conduct a DDOS attack on the USA and South Korean websites. The timing and targeting of the attacks have led to suggestions that they may be originating from North Korea, although these suggestions remain unsubstantiated (McDevitt, 2009).

The Arab Spring brought the role of social media in political power conflict to the fore. The Arab Spring refers to a revolutionary wave of demonstrations and protests (both non-violent and violent), riots and civil wars in the Arab world that began on 17 December 2010 in Tunisia with the Tunisian Revolution, and spread throughout the countries of the Middle East. Social media and digital technologies played a significant role in providing citizens within areas affected by "the Arab Uprisings" with a means for collective activism to circumvent state-operated media channels (Watson, 2012). New media such as YouTube, Twitter and satellite television made a significant impact on the Arab Spring (Van Notten, 2014:2). Social media use more than doubled in Arab countries during the protests. Collective intelligence and the dynamics of the crowd in participatory systems such as social media have immense power to support a collective action, such as the fomenting of political change (SiReBi, 2011).

The rise of social media has opened up unique opportunities to influence large numbers of people, as illustrated by the USA's psychological operations launched against Cuba. In 2010, the ZunZuneo platform, a "Cuban Twitter" which was text based on the cellular network, went live on

the island. It was in fact a programme put in place by the United States Agency for International Development (USAID). It was likely a covert programme controlled by the Central Intelligence Agency (CIA), and it ran until about 2012. At the end, ZunZuneo had about 40 000 users on the island. The overall aim of the project was to have the Cubans generate their own interaction around dissident ideas and to allow them a means to text one another outside the controls (ostensibly) of the Castro government. However, this was not successful; nor was the programme a success from the standpoint of mass demonstrations happening (Krypt3ia Blog, 2014).

In December 2014, Germany's Federal Office for Information Security (BSI) reported that hackers had gained access to an unnamed steel mill in Germany and caused "massive" – though unspecified – damage. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down. The attackers gained access to the steel mill through the plant's business network, then successively worked their way into production networks to access systems controlling plant equipment. The attackers infiltrated the corporate network using spear-phishing attacks, sending targeted emails that appear to come from a trusted source in order to trick the recipients into opening a malicious attachment or visiting a malicious website where malware is downloaded to their computers. Once the attackers got a foothold in one system, they were able to explore the company's networks, eventually compromising a "multitude" of systems, including industrial components on the production network (Zetter, 2015).

During February 2015, the global hacker collective known as Anonymous announced that it had taken down several Islamic State (IS) websites, Facebook and Twitter accounts linked to IS. The campaign against IS started in 2014 but it was intensified after the attack staged by IS militants that killed 12 employees of the Charlie Hebdo newspaper on 7 January 2015 in France (vcpost.com, 2015).

Also during February 2015, the Australian government announced that it would launch information warfare related attacks on IS related targets. The Australian Security Intelligence Organisation (ASIO) director general Duncan Lewis revealed that intelligence agencies were examining the work of the British Home Office which had authorised "take-downs" of IS websites and developed rapid response units to develop "counter narratives" to terrorist propaganda. Lewis stated that it was now clear that radicalisation online among young Australian Muslims was as great a threat as the risk of returning foreign fighters. He warned that the risk underlined the need for new laws on metadata to prevent agencies "going dark" due to a lack of information (Maiden, 2015).

In March 2015, it became known that the Chinese government diverted from its tradition of denying everything related to digital espionage and network attack capabilities, and explicitly revealed that it had specialised units devoted to using computers as weapons. China organised its offensive information security groups into three categories: operational military units, teams within civilian organisations that have been given authorisation to operate and "external entities" (Knibbs, 2015).

In May 2015, the Chinese Ministry of National Defence published China's Military Strategy, which *inter alia* discussed China's cyber strategy. According to this strategy; "As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability" (FireEye, 2016). The development of both offensive and defensive cyber capacities are increasingly the norm in many states.

## 5.6 THE FUTURE OF INFORMATION WARFARE

As indicated, in the current manifestation of information warfare related issues, governments worldwide are actively investing and researching information warfare capabilities. Most developed states and some developing states have conducted information warfare related exercises and established national monitoring entities (Bower, 2007). At the same time non-governmental entities are also getting involved in information warfare related activities (Cronin & Crawford, 1999:259). Information warfare is a global phenomenon, which makes it difficult if not impossible to evaluate in a domestic context. This will become even more so considering the future of information warfare.

Despite these capacities being created by governments and interest groups, the dynamics of emerging emergencies and the unintended consequences of information warfare make the control of information-driven dynamics highly problematic. Controlling the potential power of information war in terms of its netwar and psychological dimensions will be difficult, if not impossible, in the future. The emergence of various other information warfare actors other than government controlled entities remains a strong possibility.

Protest movements and/or governments are massing force in the infosphere as well as cyberspace for viral propaganda and debilitating DDOS attacks. As a result, there is a renewed focus on mass cyber-mobilisation and concentration as part of information warfare. As indicated earlier, networked actions, cyber-mobilisation and rhizome organisation are underpinning popular forms of conflict and not only lower impact cyber-related activities such as the disruption of websites. These activities require public participation for success and social media like viral organisations (Elkus, 2009).

It can be expected that in the future this form of mobilisation will even be more effective. The rise of artificial intelligence will probably change the nature of cyberwar in particular. Instead of relying on human hackers to carry out their attacks, antagonists will in the future continue to automate information warfare, relying on artificial intelligence systems to probe opposing defences, carry out attacks, and defend against opponents' artificial intelligence. It is probable that this competition could eventually outstrip human control or even monitoring (Matthews, 2009).

In the modern field of struggle between a sovereign country and non-state actors it also becomes necessary to refer to the information warfare that is taking place in the new and traditional media as well as other technological platforms, from the internet to virtual reality and computer games. Such groups, including terrorist organisations, continue to invest efforts in information warfare tools, which enable them to bridge the physical gap between these entities and their conventional law enforcement and security forces. Some of these entities' irregular capacities will probably outstrip the competencies of states in this regard (Gilat, 2009).

These largely asymmetric warfare capabilities, which include information warfare, are even empowering the individual to conduct war. While the concept of asymmetric warfare dates back to ancient times, most modern conflicts have redefined the nature of such struggles. As the manifestation of information warfare indicates, warfare is being transformed from a closed, state-sponsored affair to one where the means and know-how to do battle are readily found on the internet and social networks. This open and global access to increasingly powerful technological tools is in effect allowing small groups to declare war on states. Insurgent groups can be expected to increasingly form loose and non-hierarchical networks to pursue a common vision. United by that vision, they exchange information and work collaboratively on tasks of mutual interest (Charette, 2007).

## **5.7 CONCLUSION**

The environmental scan on information warfare as an upcoming national security threat focused on the technology, war/conflict, social, economic and political environments. Events, trends, risks and relationships relevant to information warfare have been analysed to highlight the phenomena that could impact the manifestation of information warfare in the future.

Transformation, networking and the impact of technological innovation in all the environments investigated are highlighted as central to the manifestation of information warfare currently as well as in the future. These meta-trends influence not only the entities involved in power relations in society, but also enhance the potential influence and power of small and marginalised entities in society. New forms of network-related actions, such as the rhizome phenomenon (of small, highly interconnected networks) using social networks for cyber mobilisation, are identified as of particular use for information warfare in the future.

When taking into account the security dimension in terms of potential information warfare targeting, a wide range of pillars supporting the information society could become potential information warfare targets. The key vulnerable access points include factors underlining the networking, coordination, integrating, compatibility and connectivity of the information and knowledge society.

As most of the discussion about information warfare has been theoretical and future orientated, it is also useful to evaluate how this phenomenon has manifested itself in the recent past. Nearly all

recent conflict situations have had an information warfare dimension. While information warfare is enhancing military power, especially in developing countries, it is also creating new vulnerabilities. It can be assumed that this trend will continue and nearly all future conflict situations will have an information warfare dimension.

It can, however, also be expected that the sophistication of information warfare actions will advance exponentially in the future. Broad individual and cooperative participation, on a world-wide scale, has now become possible. Artificial intelligence can also be expected to play a significant role in the conduct of information warfare in the future. Social media and the internet or mobile device platforms for such media empower most net-enabled individuals with the interest to participate in practically any global issue. This has created platforms for involvement and participation in social and political issues on a level never seen before in the history of humankind. Increasingly, it does not matter what the majority's views on issues are; it matters more what the majority of empowered individuals are doing.

In Chapter 6, based on the environmental scan driving forces critical for the manifestation of information warfare as a national security threat by the 2030s are identified.

## **CHAPTER 6**

### **IDENTIFYING DRIVING FORCES FOR INFORMATION WARFARE FUTURES**

#### **6.1 INTRODUCTION**

In this chapter the driving forces critical for the manifestation of information warfare as a national security threat by the 2030s are identified. The environmental scan on information warfare as an upcoming national security threat done in the previous chapter, provided the basis from which the driving forces creating the four possible information warfare scenarios for the 2030s can be identified.

Qualitative text analysis is used to evaluate and code the content of the TWEPS macro-environmental scan. This is done by following content analytical rules and step-by-step coding, without rash quantification (Mayring, 2000:1). Knowledge is perceived as actively constructed with meanings of existence only relevant to an experiential world. The environmental scan provides a view on that experiential world, which is then evaluated through qualitative text analysis. Coding software developed by the University of Pittsburgh is used to assist with this qualitative text analysis process, including to create a graphical representation of the coding outcome. While qualitative analysis is an iterative, open process (Zickmund, 2009: Slide 10), it can also be useful for the building of theory by utilising grounded theory.

The coding of text remains useful, identifying categories and subcategories vital for assisting in the identification of driving forces, later in formulating the scenarios but also in the development of a model for integrating theory and practice to develop practical foresight.

In order to achieve this grounded theory provides analytically related structures to create perspectives on the actual environments in which insights are generated. Essentially, grounded theory is mostly applied with the aim to generate theory to provide a fresh angle on existing knowledge or where little is already known (Baszanger, 1998:354). In this study grounded theory is not used for theory building but for the creation of a model, which presents a visualisation and mental tool to provide a framework for identifying and understanding the dynamic driving forces influencing information warfare futures.

The model reflects and provides content for the futures map for information warfare futures. This futures map provides the broad conceptual frame within which to discover or invent, examine and evaluate, and propose possible, probable and preferable futures (Bell, 2005:73). The model is built

on the environmental scan from which the three<sup>24</sup> common cross-cutting trends flow that influence the future manifestation of information warfare.

A significant part of this model is causal layered analysis (CLA), in order to provide depth to the insights and macro-driving forces within the model; it is used with the mapping horizon of the model. CLA allows for a multilayered and integrated analysis, which identifies the main information warfare related driving forces. The methodology of CLA, as discussed in Chapter 3, makes it possible to start to narrow down and integrate the key driving forces that will be influencing the manifestation of information warfare by the 2030s.

The model assists in providing some theoretical futures study insights, which illuminates the systemic nature of futures studies and illustrates the layered nature of creating knowledge. These broader futures study insights provide input to start the process of developing probable scenarios on how the future could manifest.

In order to understand the dynamic nature of the driving forces in a futurist context, one needs to embrace the changing contradictions that humanity is facing. This can be done by moving from one fault line to another as one contradiction runs out of energy because some kind of preliminary harmony point has been found. With this type of approach the image of the future becomes even more contradictory but also very open. The vision ensures that the future is viewed more dynamically but not necessarily less confrontationally (Galtung, 2005).

After the prioritising and validating the driving forces identified through the Delphi study and opening up the future by formulating four possible information warfare scenarios for the 2030s, the model is again evaluated to ensure that it can serve as a useful tool that provides insight in the TWEPS macro environment. Using the model to examine integrated security-related issues could assist to make a positive contribution towards a better life in South Africa and Africa.

## **6.2 CODING OF THE ENVIRONMENTAL SCAN OUTPUT**

The focus in this study is on qualitative data. Where qualitative data deals with meanings, quantitative data deals with numbers. This has implications for analysis because the analysis of meanings is done through conceptualisation whereas the analysis of numbers is done through statistics and mathematics (Dey, 2005:3). In this study, coding is used to facilitate conceptualisation.

In qualitative inquiry, a code is mostly a word or short phrase that symbolically assigns a summative, salient, essence-capturing and/or evocative attribute to a part of language-based or

---

<sup>24</sup> The three trends as identified in Chapter 5: (1) The level of integration of the world community and the rise of networks, especially social networks; (2) innovation, especially the spread of technology which is resulting in the simultaneous emergence of a host of new middle-ranking military, political and economic powers across the world while also creating significant inequality between states, groups and individuals; (3) societal change, which has been accelerated to new levels, resulting in transformation being a constant reality affecting nearly all social entities.

visual data (Saldaña, 2009:3). Coding thus means assigning codes to specific phenomena in the data material (Kuckartz, 2014: 23). Coding can be done using structured or unstructured data as source material. The best results are obtained by using qualitative text analysis of documentary source material (Kuckartz, 2015).

In qualitative research, codes are typically words or devices used to identify themes. Coding data can be used as a data reduction method. However, this study does not focus on data reduction; instead, it focuses on coding data as a means to search for themes and eventually the driving forces impacting information warfare futures. As the research focuses on theme-related issues associated with the current and future manifestation of information warfare, thematic qualitative text analysis is focused on the environmental scan's text in its entirety.

Qualitative coding involves creating categories based on the interpretation of the data (Charmaz, 1983:111). The term category stems from the Greek word *Κατηγορία*, which originally meant class, charge or even accusation, and which can be found in various scientific disciplines. Within the context of social sciences, the term *category* usually denotes a sense of class. For example, a category is the result of some sort of classification. In terms of knowledge systems this can refer to indexes, taxonomy charts and encyclopaedias (Kuckartz, 2014:38). Strauss and Corbin (1998:101) defined categories as concepts that stand for phenomena. Categories have properties, dimensions and subcategories (Kuckartz, 2014:23). These terms can be defined as follows (Strauss & Corbin, 1998:101):

- **Properties:** Characteristics of a category, the delineation of which defines and gives it meaning.
- **Dimensions:** The range along which general properties of a category vary, giving specification to a category and variation to the theory.
- **Subcategories:** Concepts that pertain to a category, giving it further clarification and specifications.

The analytic tasks in terms of qualitative text analysis include naming concepts, defining categories and developing categories in terms of their properties and dimensions (Strauss & Corbin, 1998:102). Even after categories have been assigned, the text itself, i.e. the wording of the statements, is relevant and also plays an important role in the preparation and presentation of results (Kuckartz, 2014:66).

After studying the text, the summative, essence-capturing codes are identified, which are applicable to all text in the environmental scan narrative. Three such overarching codes have been identified. The three coding concepts overlap to some extent but for each paragraph the essence-capturing categories and then subcategories were conceptualised. The source of these qualitative text analysis thematic coded categories, identified as **Innovation**, **Networks** and **Transformation**, is the three cross-cutting trends identified from the environmental scan.

Firstly, the rapid spread of technology and innovation has a major impact on states, organisations and individuals while also contributing to significant inequality. Secondly, the world community has reached a new level of integration, accompanied by the rise of networks, especially social networks. Thirdly, societal change has been accelerated to new levels, resulting in transformation as a constant reality affecting nearly all social entities. The outcome of the environmental scan is coded using Coding Analysis Toolkit (CAT) software developed by the University of Pittsburgh's Qualitative Data Analysis Program (QDAP) (University of Pittsburgh, 2015). (See Appendix A, Table A: 1 for a representation of the coding exercise.)

The first step of the analysis process focuses on the initial text, during which specific text passages related to the main thematic categories are highlighted. During the next step, the main thematic categories are allocated to the text via the coding process (Kuckartz, 2014: 71). After studying the content, the three main categories are identified in line with the earlier identification of the three cross-cutting environmental scan trends, namely Innovation<sup>25</sup>, Networks and Transformation.

While innovation at first can be understood as the introduction of new things or methods, what is significant includes the content (what is the innovation), creation (how has innovation been created), and impact (what are the effects and consequences of innovation). In many cases innovation can be disruptive by fundamentally changing and shaping the broader environment (Weis, 2015:15). As innovation is closely related to technology and science is thus linked with knowledge and learning (Vernardakis, 2016:25).

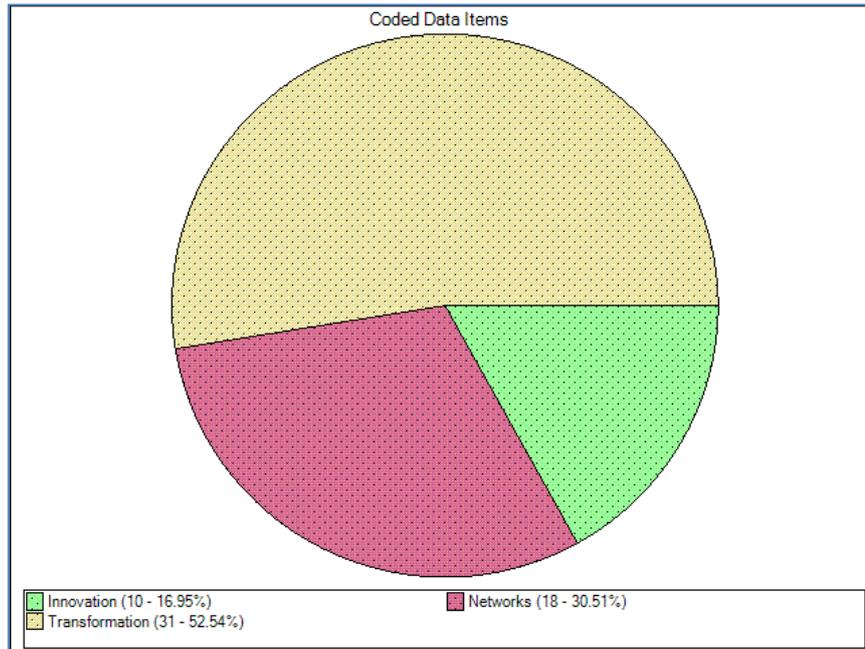
A network is a series of points or nodes interconnected by communication paths (SearchNetworking.com, 2015). The social dimension of networks is especially relevant in the environmental scan. A social network is a social structure made up of a set of social actors (such as individuals or organizations), sets of dyadic ties, and other social interactions between actors. The social network perspective provides a set of methods for analyzing the structure of whole social entities as well as a variety of theories explaining the patterns observed in these structures (Wasserman & Faust, 1994:1-27).

Transformation refers to a change in form, appearance, nature or character in a modern context can be understood as a shift from social orders defined by stratificatory social differentiation to those dominated by functional differentiation. While stratification is about hierarchies of rank and class, it is characteristic of social orders defined by dynasticism and caste. Functional differentiation is about the coherence and interdependence of specialized types of activity, the creation of a complex division of labour, and the rise of legal, political, military, economic, scientific, religious and other specialized roles (Ritzer, 2007: 98-100).

---

<sup>25</sup> Although the category refers to technical innovation, the more encompassing term innovation is used as category term.

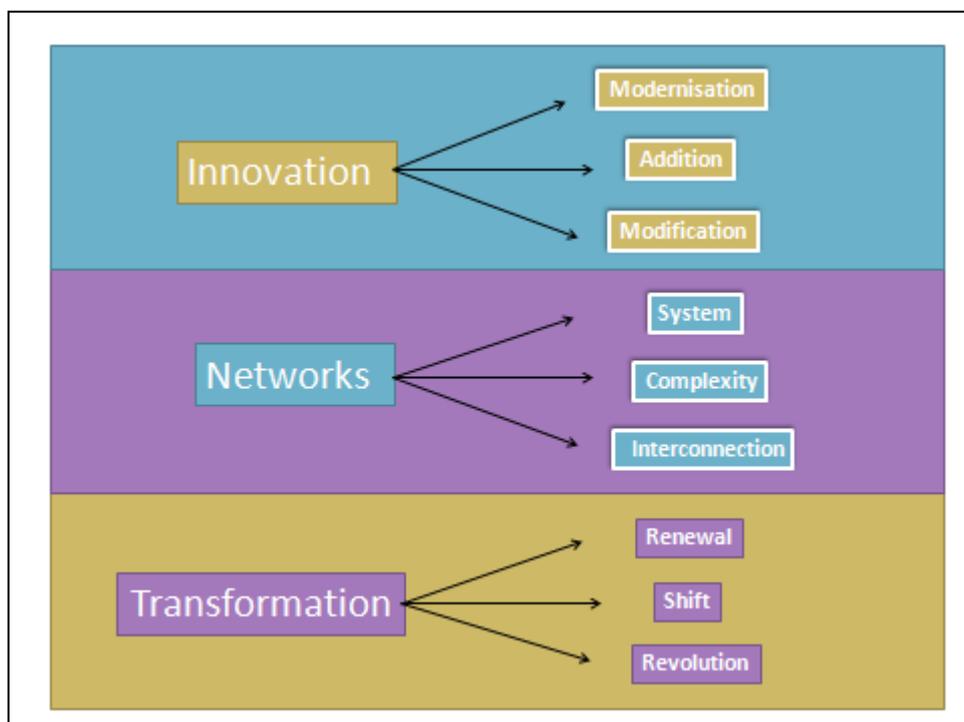
After coding based on the main categories, Transformation was identified as the main category, followed by Networks and Innovation. See Figure 6.1 for a graphical representation of the outcome of the coding exercise.



**Figure 6.1: Qualitative text analysis of the three environmental categories**

Source: Output of CAT coding, 20 May 2015.

The next step in a category-based analysis is highlighting the relationships between the subcategories and categories (Kuckartz, 2014:71-84). Three subcategories have been identified for the three main categories. (See Figure 6.2 for the identified subcategories for Innovation, Networks and Transformation.)



## Figure 6.2: Subcategories for Innovation, Networks and Transformation

Source: Own compilation based on coding exercise using CAT.

**Innovation** is related to the subcategories of modernisation, addition and modification, all focusing on different aspects of innovation. **Modernisation** refers to a model of progressive transition encompassing the improvement of systems and technologies. It is more than the process of change as it also includes the responses to that change (Knöbl, 2003:96-97). In all environments, improvements brought about by technological enhancement as well as organisational and system efficiencies are regarded as crucial for improvements and development. In particular, rapid technological innovation is mentioned as a central modernisation innovation factor.

**Addition** is the process of adding or joining something to something else, typically to make it larger or more efficient (Thefreedictionary.com, 2015). In all environments, innovative addition resulted in systemic and practical improvements. However, inequalities as well as the digital divide are also highlighted in all environments for which addition or any other innovative development does not always have an answer. Another negative aspect brought about by addition is increasing the capacity for using innovation for negative purposes.

**Modification** refers to both the act of modifying as well as the condition of being modified, which result in mutual adjustment and change between human social systems and the environment (Lill, & Gräber, 2006). Modification is the way in which most innovation is taking place in practical ways (O'Callaghan & Evans, 1973:51).

In all environments, methods and systems, which are the result of scientific knowledge being used for practical reasons, are impacting these environments in innovative ways. Pervasive technologies, for example include progress in economic productivity, global collaboration, e-commerce, with all efficiencies leading to change in government and society. However, this impact has globalising as well as fragmenting consequences, empowering some individuals and entities while marginalising others. Some of the modifications have significantly increased the influence of the general public in terms of participating in the current political and economic dialogue while also expanding the broad-based threat of general instability that far exceeds that offered by the dissidents, terrorists and guerrillas of the past.

Identified subcategories for **networks** are system, complexity and interconnection. **System** refers to a set of interacting units, forming a unitary whole (Waltz, 1979:40). Within a system, the elements do have mutual relationships between each other and with its environment (Dekkers, 2015:xiii). In all environments, ICT is identified as a significant force multiplier. However, “out-of-control” technology and fears of vulnerabilities due to dependency on technology are also recurring themes in the TWEPS environments. The system subcategory of networks also focuses more on

the intangible factors, such as the capacity to adapt relative to other role-players in the environment. In the war and conflict environment this manifests in so-called fourth-generation warfare which seeks to undermine the enemy's political will to fight by utilising political, economic and social networks as well as military action. On a global level, the significance of multilateral approaches to manage relations promises to be the appropriate institutional policy response to globalisation and the growing interdependence of national economies.

**Complexity** describes the behaviour of a system in which the interaction of many parts takes place, giving rise to difficulties in linear or reductionist analysis due to the nonlinearity of the inherent circular causation and feedback effects (CALRESCO, 2006). Such systems with non-linear interactions do not necessarily behave chaotically. Often, they are characterized by "emergent", i.e. spontaneous coordination or synchronisation (Helbing & Lämmer, 2008: 2). Some of the networked complexity currently experienced in the TWEPS environments can be ascribed to continuous transformative social change. Increasing technological or systemic complexity is impacting the decision cycle, challenging especially human institutions such as the nation state itself. The growth of social media has enhanced global participation, openness, conversations, community forming and connectedness within most environments, but these have also increased the vulnerability of advanced and developing states.

**Interconnection** is to be meaningfully or complexly related or joined (Dictionary.com, 2015). Networking has been stimulated by ICT as the most potent agent of change, establishing regional and global interconnectedness. At the same time, some effort goes to creating a more unified whole out of the distinct elements. More emphasis is also placed on the greater role of system-based approaches and enabling technologies. Globalisation results in growing economic as well as political, social and technological interconnectedness. This creates a pervasive knowledge set of connections assisting networking. Economic integration, especially the opening up of international trade, has helped many countries to grow far more quickly than they would otherwise have done. However, interconnectedness has also brought with it pervasive security challenges.

**Transformation** is related to the subcategories of renewal, shift and revolution. **Renewal** refers in an organisational context to the strategic process that results in fundamental changes necessary to align the organisation with its operational environment (Scholtz, 2009:9). As humanity's scientific understanding grows, so too does the ability to engineer instruments to manipulate and transform the world. Intellectual technologies do play a significant role in the changes in society's power structures. Hence, while computer technology and especially the role of the internet are impacting a rapidly globalising world, significant differences still exist in the abilities of different countries to effectively make use of these transformative tools. Information technology presents humanity with transformative capacity to simultaneously localise and globalise (glocalisation), decentralise and centralise, fragment and integrate. Transformation also makes it important to separate what is transient from that which constitutes long-term change. Humanity is inundated with information and

is more engaged with the wider world than ever before. This also applies to the war/conflict environment, which blurs the boundaries between the civilian and military realm.

**Shift** is referring to change in terms of direction, place or position (Shaughnessy, 2015: 8). Technology and information are interdependent, with advances in one entailing and dependent on advances in the other. A general shift to information or digital economics is taking place globally. While states will remain the dominant actor globally, they will be challenged and they will find it increasingly difficult to remain in control. As new military technologies emerge, the global diffusion of weapons and military technology is bound to confront policy-makers. As humankind is increasingly becoming digital data subjects, the ability for governments to build and sustain partnerships to combat discontents will increasingly depend on bolstering a country's credibility with the broader population of the world and forging an ethic of common purpose. A much larger part of the population, both within and among countries, has access to the power that comes from information. While globalisation has not succeeded in reducing poverty in general, neither has it succeeded in ensuring sustained stability.

**Revolution** refers to any wide-ranging change in society, instituted, perhaps, by social, political, economic and/or scientific/technological change, altering the distribution of power in the society, but also resulting in major changes in the whole social structure (Robertson, 2002:428). Many elements of human induced transformation can be regarded as revolutionary. The Information Age is also called the "age of technology". A radical transformation has occurred in the way in which the information sphere is used by individuals, citizens and members of cultural and social groups. The Information Age brought an increase in management and precision. It also reaches into new domains of cyberspace and space. The social media trend supports the democratisation of knowledge and information, transforming people from content consumers into content producers. However, these same technologies are also increasingly used by authoritarian governments, transnational crime and extremist political and religious entities.

Using the insight gained from the systems approach, the need for a multi-dimensional perspective on information warfare context is evident. The limitations of coding, even when subcategories have been identified, become noticeable once the thematic qualitative text coding has been done. The subcategories provide additional insight into the environmental scan but do not promote a more integrated and multi-layered view of the environment within which information warfare manifests. Hence, it becomes necessary to develop a model for viewing the information warfare environment in order to ensure a more detailed and integrated production of key drivers of information warfare. Subcategories, however, are useful in the development of scenarios on how information warfare will manifest as a national security threat by the 2030s.

### 6.3 FROM GROUNDED THEORY TO A FUTURES MODEL

In traditional social science, the researcher enters a research situation with an *a priori* theory. The purpose of data collection is therefore to “confirm” or “disconfirm” that theory, hence the phrase confirmatory approach to science. In grounded theory, data is not used to test an *a priori* theory. Rather, data is used to evolve a theory. Typically, the data is collected by means of qualitative methods (Jaccard & Jacoby, 2010:256). Therefore, the careful coding of data is central to grounded theory (Kuckartz, 2014:23). Charmaz (2006:46) stated that: “Coding is the pivotal link between collecting data and developing an emergent theory to explain these data. Through coding, you define what is happening in the data and begin to grapple with what it means.”

A model can be created by applying a method such as grounded theory, which is a systematic methodology used in the social sciences to discover theory through the analysis of data (Martin & Turner, 1986:141). Grounded theory, therefore, was intended as a methodology for developing theory that is “grounded in data” that has been systematically gathered and analysed. The theory evolves during the research process itself and is the result of continuous interplay between data collection and analysis. It requires the acknowledgment that enquiry is always context bound and facts should be viewed as both theory laden and value laden (Goulding, 2002:42).

Modelling is a visualisation and mental tool developed to represent reality. A model can be helpful to understand the connections between factors and events, and to examine their dynamics. Models thus constitute a simpler version of reality even though they have a disadvantage as certain factors can be omitted. However, models are central to scientific thinking and essential for various kinds of practical problem solving. Permeated with different meanings in different contexts, the word model implies structure and relationships among variables while also conveying tentativeness and incompleteness (Bello, 2007:108).

In this study, coding is not used to create theory *per se* but a model which is intended to be useful in providing futurist insight into the manifestation of information warfare. Coded categories should be linked to theoretical propositions (Jaccard & Jacoby, 2010:268). Thus, the core of grounded and emergent model construction occurs at the level of data analysis. It is here that the insights gained during the act of data collection are combined with the insights gained from reading past literature, the environmental study and the information contained in the data to derive a model (Jaccard & Jacoby, 2010:269). Such approaches are orientated to identifying connections between social phenomena (Dey, 2005:3).

Process-oriented perspectives in theorising remain common. Merriam-Webster (2015) defined a process as “a systematic series of actions directed to some end” (e.g. the process of homogenising milk) and as “a continuous action, operation, or series of changes taking place in a definite manner” (e.g. the process of decay) (Jaccard & Jacoby, 2010:269). The essence of these definitions involves the notions of action and change situated at the centre of the proposed model.

### 6.3.1 The use of a model

Model building is important for problem solving (Bello, 2007:110). It is important to create a framework showing how insight can be gained into the future manifestation of information warfare. The current TWEPS environments show significant complexity, as illustrated by the environmental scan. The model provides a visualisation and mental tool to add value to the analysis of the environmental scan output.

Social scientists who want to quantify their knowledge find that it is extremely difficult to determine relationships among variables that are not as precise and complete as in the physical world. A model captures an important texture of tentativeness and incompleteness that is needed in describing knowledge (Little, 1993:1). Building a model allows for the use of heuristics and known structures. However, prior knowledge can also hide new directions in problem solving. Breakthroughs are facilitated by conscious efforts to bring new ideas to the problem, often in a sequence of intensive effort, followed by backing away, and, after a delay, the release of a fresh flow of ideas (Little, 1993:8).

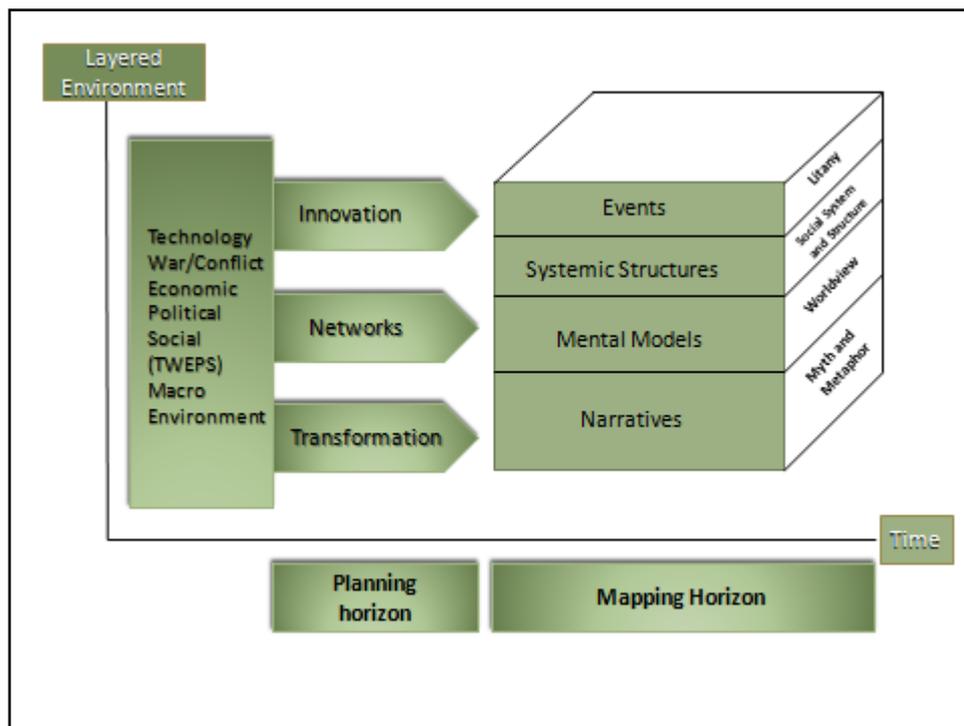
In social science a model represents theory as a system of related concepts to describe an idea or phenomenon (Little, 1993:2). Theorising actions include reaching down to fundamentals, reaching up to abstractions as well as probing into experience. The content of theorising opens up the core of studied phenomena and poses new questions about it. Value added by model-related theorising fosters seeing possibilities, establishing connections and asking questions. A model developed through grounded theory methods provides theoretical opportunities that avoid importing and imposing packaged images and automatic answers (Charmaz, 2006:135).

## 6.4 AN INFORMATION WARFARE ENVIRONMENT FUTURES STUDIES MODEL

A multitude of methods can be used to produce the knowledgeability that brings about insight and eventually foresight. In this study, a model is developed to assist in the process of the identification of driving forces that will be influential in how information warfare manifests as a national security threat by the 2030s. The model is constructed from three different but related constructs, namely the futures map, environmental scanning and CLA. The data collected during the environmental scan, which is coded in terms of the thematic qualitative text analysis method, resulted in the identification of three categories. In terms of grounded theory these categories may become the basis for new theory (Allan, 2003:1). In this model, the three categories represent the three macro-trends influencing information warfare futures.

Figure 6.3 is an illustration of a graphical representation of this model. The value of the model lies in identifying the features that will be key in creating the level of insight into the issue of information warfare as a future national security threat. The model is situated within the framework which is

related to the earlier identified futures map in which the possible, probable and preferable futures could manifest.



**Figure 6.3: Futures studies model applicable to information warfare futures**

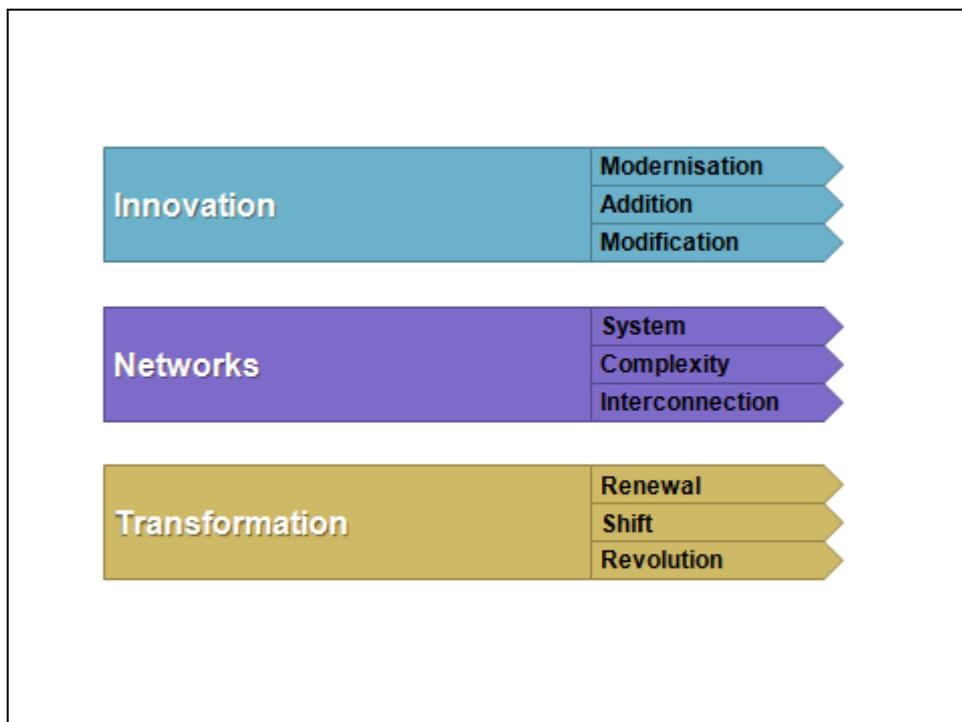
Source: Own compilation using insights from the Futures Map (Kuusi, Cuhls and Steinmüller, 2015:63), Causal Layered Analysis (CLA) (Inayatullah, 2008c:1) and Systems Layered Explanation of Reality (Senge, Smith, Kruschwitz, Laur and Schley, 2008:174).

The environmental scan serves as the source of insight into the driving forces influencing the possible futures of information warfare. In the case of information warfare as an upcoming threat the Technological, War/Conflict, Economical, Political and Social (TWEPS) macro-environmental hexagon is used instead of the frequently used STEEP (Social, Technological, Economic, Environmental and Political) sectors (Kurian & Molitor, 1996:814).

Based on the environmental scan, the mentioned three interrelated trends which influence information warfare futures have been identified. In the contemporary world, these three trends are manifesting at a significantly increased pace and intensity – unlike anything in past human experience. The first trend is the integration of the world community and the rise of networks, especially social networks. The second trend is the impact of innovation, especially technological innovation resulting in the emergence of a host of new middle-ranking military, political and economic powers across the world, but also great inequality between states, groups and individuals. The third trend is societal transformation that has been accelerated to new levels, resulting in transformation being a constant reality affecting nearly all social entities. The outcome

of the analysis of these trends has produced the required forecasting and futures insight, which forms the basis of the futurist dimension around which future scenarios can be constructed.

The trends provide the input and sketches out the planning horizon. The planning horizon is linked to the concept and method of a roadmap (Kuusi, Cuhls & Steinmüller, 2015:64). The roadmap highlights the trends influencing the future manifestation of information warfare. (See Figure 6.4 for an illustration of the trend planning horizon roadmap.)



**Figure 6.4: Trend planning horizon roadmap**

Source: Own compilation.

The mapping horizon is the anticipation horizon of a futures map and consequently of possible futures (Kuusi, Cuhls & Steinmüller, 2015:64). This is the space in the futures map where scenarios are formulated. Before scenarios can be compiled, the output of the environmental scan (inclusive of the three trends) must be evaluated on multiple levels. In this model, the mapping horizon provides an opportunity to evaluate the futures impact of the trends by using a four-layered approach. This four-level systematic explanation of *inter alia* security-related issues is based on proposals by Senge, Smith, Kruschwitz, Laur and Schley (2008:173-176) to provide a guideline for a layered structure which can be used to gain more insight into the phenomena that are being studied. (See Figure 3.6 in Chapter 3 for an illustration of this.) The first level identifies events of concern. The second level goes beyond the immediate event by focusing on the underlying structural aspects within which these events occur. The third level refers to the mental models,

which are the core beliefs within the system, especially related to the authoritative granting of values by the decision-makers within the system. The fourth level focuses on the narratives which are based on the myths and metaphors influencing trends. Human activities result in "systematic relationships" (e.g. governments, corporations, universities, armies, churches) that are interacting with each other to create a multi-layered social reality, which is the focus of study (Searle, 1995:97).

These layers are intimately related to the futures-orientated layered method that Inayatullah called (2008c:1) causal layer analysis (CLA). In Chapter 3, CLA has been identified as a tool to categorise diverse views of and concerns about the future, allowing for more effective thinking about the future (World Future Society, 2005:4). While CLA involves the four levels of knowing – the litany, social causes, discourse/worldview and myth/metaphor levels of knowing – the challenge remains to conduct research that moves up and down these layers of analysis in order to be inclusive of different ways of knowing (Inayatullah, 2000:1). CLA has matured since its development by Inayatullah and developed into a generalized system for viewing the world as made up of distinct layers of reality. Voros (2006: 45) describes the four levels as four major "bands" or "strata" of depth which sit "below" the default "surface" view of discrete events and occurrences. These layers are highlighting; constructs of thinking; contents of thinking; capacities of thinking; and conditions of existence.

The next step is thus the evaluation of the environmental scan of each environment by way of using CLA.

## **6.5 CLA ASSESSMENT OF THE ENVIRONMENTAL SCAN**

The value of CLA is that it explicitly acknowledges that futures relevant factors influencing society can be viewed from different levels; it also facilitates analysis on these different levels. CLA serves both as a theoretical and research framework which deepens analysis and foresight processes. It can also serve as a tool for the redirection of policies which increases the extent of possible solutions (Milojević, 2014:1).

The evaluations done during the environmental scan in Chapter 5 serve as source material (input) for this CLA assessment. CLA is thus used to identify key trends in all the environmental sectors identified as relevant for this study, namely the social, technological, economical, war/conflict and political sectors. Trends can be defined as trajectories, extrapolations, projections, and possibly even predictions, which are continuous and usually monotonic (Walton, 2001:1). Trends refer to the general direction in which something tends to move (Agostini, 2010: Slide 3). Identifying trends is a necessary first step in the process to analyse the potential impact of the current manifestation of human activity on the future. While it is obvious from the environmental scan that various and sometimes contradictory trends can be identified, it is more productive in terms of a futures approach to focus on those with strategic implications.

It is necessary to differentiate between trends and driving forces. Although the two concepts are related, trends do not equate to driving forces (Agostini, 2010: Slide 5). A driving force refers to the impetus, power or energy behind something in motion (Dictionary.com, 2015). Driving forces are theoretical but also practical exercises of thought identified by using the scientific method and systems approach. Thus, developments, especially clusters of developments that precipitate shifts within society so great that they cause significant shifts in other sectors, are identified as driving forces relevant to the creation of the future. Understanding driving forces is important for strategic planning or scenario building (or any other activity that involves anticipating the future) (Caldwell, 2003). In this study, driving forces related to the manifestation of information warfare are collated from the CLA layered analysis of causal factors potentially influencing the future. However, attention should also be paid to potential strategic disruptors. These disruptors are known as “wild cards” in the context of scenarios. Wild cards refer to relatively abrupt changes of particular significance. These include potential catastrophes and other high-impact, low-probability events that would severely impact the human condition were they to occur (Walton, 2001:1).

The CLA assessments of the environmental scan focus on the technology environment (Table 6.1), the war/conflict environment (Table 6.2), the political environment (Table 6.3), the social environment (Table 6.4) and the economic environment (Table 6.5). All of these environments, as presented in Chapter 5, are assessed according to the four CLA levels, namely the litany, social causes, discourse/worldview and myth/metaphor levels of knowing. The CLA process is built on the qualitative text analysis, identifying the core analytical insights on the four levels. These assessments are then collated and integrated to identify the main driving forces influencing the future manifestation of information warfare as a national security threat.

### 6.5.1 CLA assessment of the technology environment

In the context of this study, technology is regarded as more than mere artefacts (devices, equipment, machines or material objects) as it is also about knowing how to achieve practical purposes in the world. The manifestation of technology in especially the communication, information and management fields enhances the domination in society of signs and the systems that produce them to the level where the symbolic is increasingly impacting behaviour. This ensures that technology is at the core of changes in the socio-economic and political environments. Progress in the technological environment, for example, resulted in global communication becoming instantaneous. The outcome of this is that information and communication technology is increasingly embedding itself as a crucial part of nearly all levels in society.

**Table 6.1: CLA assessment of the technology environment**

CLA layers	Assessment
------------	------------

<b>Litany</b>	<p>Technology is the panacea of all humanities problems versus technology as the root of all evil.</p> <p>Technological change is a dominating force in human endeavours driving continuing innovation, consumption, economic growth and human development.</p>
<b>Social systems and structures</b>	<p>World-wide, progress in terms of communication technology is impacting most societies, creating geographically diverse connections and social networks enhancing the general public's influence on events and policies in many societies.</p> <p>Technological development is <i>inter alia</i> driven by the need to expand new relationships and links between individuals and entities.</p> <p>Power relations are directly and significantly altered by technology that creates new and improved infrastructures in society. This is taking place on two levels with communication options for populations expanding but also increasing the potential for authoritarian governments to expand societal controls.</p> <p>Technology has enhanced the shift in society from exploitation and profit to domination by the signs and systems that produce them.</p>
<b>Worldview</b>	<p>Despite continuing global poverty and inequality, technology is creating economic and political opportunities for traditionally marginalised societies by changing their perceptions about the possibilities to change these societies. As a factor that influences the distribution of power in society, technology empowers individuals, entities and societies. While technology creates opportunities for more freedom on the one hand, it also enhances the options for control on the other.</p>
<b>Myth</b>	<p>The transcending of man and the creation of a so-called singularity versus a future of a technological global dictatorship by a small elite or even an artificial intelligence creation.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

### 6.5.2 CLA assessment of the war/conflict environment

While the prevalence of war in the world has decreased, it remains highly unlikely that it will disappear. The environmental analysis suggests that it has become more ingrained in the world with the blurring of boundaries between combatants and non-combatants as well as shifting centres of global power, providing some opportunities for conflict that has not existed before. This increasingly hybrid nature of war has become evident in a variety of operating environments, has synchronous effects across multiple battlefields, and is marked by asymmetric tactics and techniques. Part of this shift is related to enhancing the political, social and economic impact of individuals and sub-state entities in the world during conflict and war. These changes in the character of warfare and conflict are impacting security by increasingly turning security into a more encompassing, globally influenced and network-related phenomenon.

**Table 6.2: CLA assessment of the war/conflict environment**

CLA layers	Assessment
<b>Litany</b>	<p>The modernisation of military capacities, especially the digitalisation of systems, high-technology weapons and modernisation of information management, is needed for military and strategic success.</p> <p>While armed and security forces are increasingly relying on high technology, such forces still remain highly vulnerable to asymmetric threats.</p>
<b>Social systems and structures</b>	<p>Contemporary conflicts contribute to the blurring of differentiation between combatant and civilian in conflict situations.</p> <p>Technological advances have strengthened the system-based nature of war and conflict.</p> <p>Changes in terms of technology and media influence are empowering the previously powerless, enabling individuals and small groups to perpetrate violent actions with significant strategic consequences.</p> <p>The shifting COG strengthens the relevance of information warfare in the Information Age.</p>

<b>Worldview</b>	<p>Increasing progress in capacities and technology are making it progressively more feasible to target higher-level decision-making entities and the management systems of the enemy. The potential value of political, economic and social networks, as entities to undermine the enemy's political will to fight, is increasing.</p> <p>Despite technology's impact on war and conflict as well as the globalisation of conflict, the vast majority of modern conflicts have been civil wars fought with relatively unsophisticated weapons.</p>
<b>Myth</b>	<p>The exponential growth of military technology creates an undeniable position of power for a superpower such as the USA.</p> <p>Dystopian conflict visions based on movie industry depictions create visions of artificial intelligence (AI) threatening the future of humanity.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

### 6.5.3 CLA assessment of the political environment

Non-state actors are increasing their influence on the domestic as well as international political milieu. The national security element within the political environment is closely related to government control, and is made much more complex by the growing political influence of individual and smaller actors. While technology also provides the government with increased capabilities to control the flow of information, total control is becoming more elusive as technology and social networks are integrating globally. Globalisation is spreading transformation, technology and know-how worldwide but it is also highlighting and boosting inequalities. At the same time most states, especially world powers, will be under increasing pressure to seize strategic opportunities and make inequality and sustainable development their top national priority or face political marginalisation.

**Table 6.3: CLA assessment of the political environment**

<b>CLA layers</b>	<b>Assessment</b>
<b>Litany</b>	Government control is enhanced through the implementation of more sophisticated management systems.

	<p>Globalisation ensures that local-level political action can now be linked to global actions more easily.</p> <p>Knowledge and information are progressively more omnipresent in society, making it difficult for governments to unilaterally control populations.</p>
<b>Social systems and structures</b>	<p>Since the end of the Cold War, the global international relations system's traditional principles are being challenged and remain in a transformative stage.</p>
<b>Worldview</b>	<p>Multilateral politics is growing in importance. However, despite efforts to impede sovereignty, multilateralism has not yet been able to overcome the sovereignty principle and is not likely to do so in the near future.</p> <p>The political relevance of individual and smaller actors is enhanced as the global communications infrastructure expands.</p> <p>Governments and global actors are increasingly exposed to domestic and international public pressure.</p>
<b>Myth</b>	<p>A world government is to be created in the future.</p> <p>Severe global economic, social and political inequality will fuel future political instability.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

#### 6.5.4 CLA assessment of the social environment

Significant components of society are excluded from information and knowledge while other components function within pervasive information/knowledge environments. Within the pervasive information components information overload is a significant challenge. Therefore, information filtering has become crucial in the social environment. In addition, the exponential growth in communication is enhancing the opportunity to expand social networks globally. In this, social media has become a significant part of communication and social media's influence is expected to grow even more in the future. Social media provides opportunities for social and economic growth but also new avenues for the misuse of these networks for negative purposes. Polarising and integrating forces are contesting on many social levels.

**Table 6.4: CLA assessment of the social environment**

<b>CLA layers</b>	<b>Assessment</b>
<b>Litany</b>	Information overload is a growing problem. Pervasive information will be available to people with the technical means to access it.
<b>Social systems and structures</b>	A large plethora of communities are created as social media continues to develop. Disparity in wealth and access to knowledge continues to grow.
<b>Worldview</b>	Social networks are becoming a major factor with communities establishing themselves as dominant actors in society.
<b>Myth</b>	<p>Society has become a truly global community in which real-time interaction is now a reality.</p> <p>Many injustices will be ended through concerted social actions.</p> <p>Increased social networking across international borders will increase the ability of these groups to undermine sovereignty.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

### **6.5.5 CLA assessment of the economic environment**

The global economic environment is being transformed at a fast pace with growing interdependence, the shift of the economic centre and globalisation as major trends. Technological innovation is also influencing changes in the economic environment. The centre of the global economy is shifting to be based on information and cultural production. Cheap communication is increasingly becoming prevalent built on inexpensive processors with high computation capabilities, which are interconnected in a pervasive network, such is currently the case with the internet. Despite the technological progress, expanding communication and growing international

economic integration, unequal economic outcomes remain a global reality. This inequality endangers progress in the long term as parts of the population might be economically marginalised while their access to power instruments might be enhanced on the other hand.

**Table 6.5: CLA assessment of the economic environment**

<b>CLA layers</b>	<b>Assessment</b>
<b>Litany</b>	The global economic system is truly interrelated and interdependent.
<b>Social systems and structures</b>	<p>Global interdependence is a reality. However, at the same time economic vulnerabilities have also increased significantly.</p> <p>Information and cultural production fuelled by easy and cheap communication is growing in significance as economic activities.</p>
<b>Worldview</b>	<p>Globalisation has increased the mutual interdependence of all national economies. With growing interdependence the world is also facing growing inequality.</p> <p>Social production and exchange could become a major economic means of production next to property-based and market-based production.</p>
<b>Myth</b>	<p>National economies will eventually be fully integrated into a global economy.</p> <p>The current global economic structure is unable to address growing global inequality.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

## 6.6 INTEGRATION OF CLA ASSESSMENT WITH MODEL'S IDENTIFIED TRENDS

The layered CLA assessments are in line with the futures model developed in this study. This model identifies three main trends, namely the dynamics of networks, especially social networks, technological innovation and the prominence of transformation, especially institutional transformation in human endeavours. It is possible to integrate the CLA assessments and identify the cross-cutting issues significant enough to bring about change. As all of these identified issues can precipitate shifts within society so immense that they cause other significant shifts. Hence, they can function as driving forces linked to the identified three main trends. In evaluating these environments the impact on global inequality is also highlighted. Although most of these driving forces can be linked to more than one of the main trends, the primary main trend has been highlighted in each case. (The result of this process is presented in Table 6.6 and is visually depicted in Figure 6.4.)

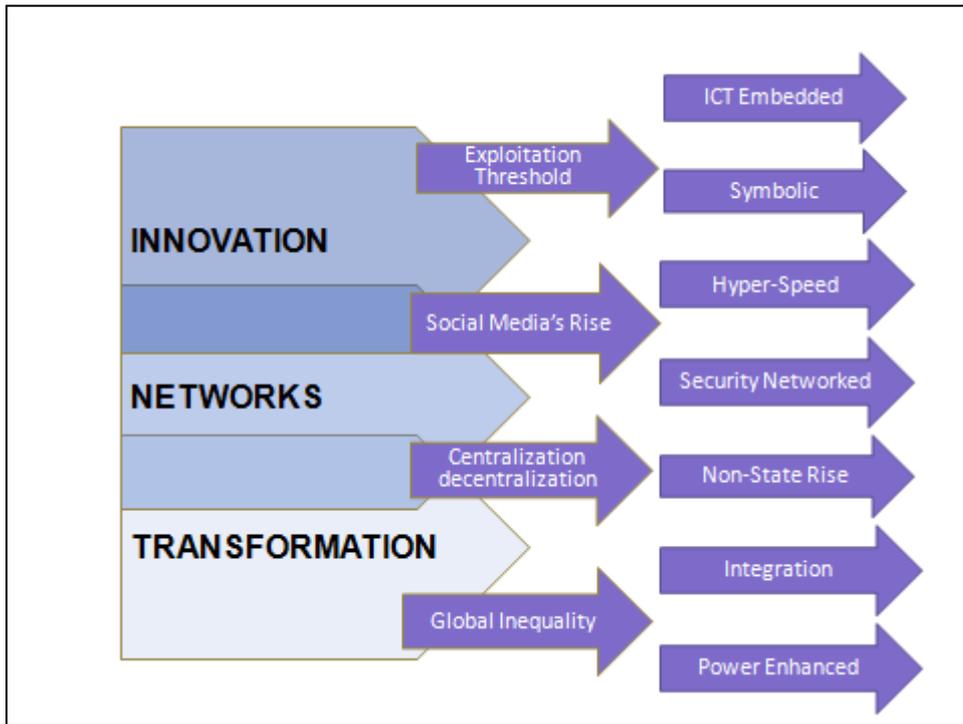
**Table 6.6: Identification and evaluation of driving forces**

<b>Driving forces</b>	<b>Category: Link to main trend</b>
Globally, the centre of <b>power</b> is shifting, <b>enhancing</b> the political, social and economic influence of individuals and sub-state entities in the world.	Primary transformation Subcategory: shift
<b>Security</b> is increasingly becoming a more encompassing, globally influenced and <b>networked</b> phenomenon.	Primary networked Subcategory: interconnection
The <b>integration</b> of systems and processes are exponential in the Information Age.	Primary transformation Subcategory: revolution
Despite the dominance of integration many human endeavours are also faced with systemic stress as challenges associated with <b>centralisation</b> and <b>decentralisation</b> are impacting on entities globally.	Primary transformation Subcategory:

	shift
<b>Symbolic</b> , information-related phenomena are increasingly impacting behaviour.	Primary innovation Subcategory: modification
The <b>speed</b> of change is increasing exponentially with global communication becoming instantaneous.	Primary innovation Subcategory: modernisation
<b>Non-state actors</b> are increasing their influence on international politics, especially in terms of national security.	Primary networked Subcategory: complexity
<b>Global inequality</b> in terms of economic, social and technological access continues to be a major global challenge.	Primary transformation Subcategory: renewal
<b>ICT</b> is <b>embedding</b> itself as a crucial part of society.	Primary innovation Subcategory: addition
<b>Social media</b> is imbedded in communication and is expected to grow in the future.	Primary networked Subcategory: system
The <b>threshold</b> required <b>to exploit</b> the advantages of information technology is relatively low and decreasing rapidly as the recursive simplicity within the ICT sector, which supports a clear trend of ever-expanding growth in access, availability and speed with a simultaneous reduction in cost and skill barriers, is increasing.	Primary innovation Subcategory: modification

Source: Own compilation.

These driving forces remain highly interdependent and influential for the creation of futures scenarios focusing on the manifestation of information warfare as national security threat. (The driving forces are illustrated in Figure 6.5.) It will, however, be necessary to scrutinise the validity of these driving forces by way of expert opinion through a Delphi study.



**Figure 6.5: Driving forces for information warfare futures**

Source: Own compilation.

## 6.7 CONCLUSION

The thematic qualitative text coding of the environmental scan output has been done to open up the text for evaluation. The summative essence-capturing categories, which have been identified as innovation, networks and transformation, are the three cross-cutting main trends identified from the environmental scan. Sub-categories have also been identified, which are useful in the development of scenarios on how information warfare will manifest as a national security threat by the 2030s.

A framework has been created for integrating theory and practise. Grounded in data, a model has been developed to produce knowledgeability that brings about insight and eventually foresight regarding information warfare futures. Modelling is a visualisation and mental tool developed to add value to the analysis of the environmental scan output.

The model is constructed from three different but related constructs, namely the futures map, environmental scanning and CLA. The data collected during the environmental scan and coded in

terms of the thematic qualitative text analysis method led to the identification of three categories and thus also three main trends. Driving forces related to the manifestation of information warfare are collated in this study from the CLA-based strategic evaluation of factors potentially influencing the future. Eleven such driving forces have been identified as issues which can precipitate shifts within society so immense that they can cause other significant shifts in context of the role of information as instrument of power.

The value of the model-derived driving forces is increased when the driving forces can be scrutinised, integrated and validated by a panel of global and local experts knowledgeable about the environments identified as relevant to the futures of information warfare.

For this purpose two Delphi studies will be conducted in the next chapter as the most appropriate method to arrive at an expert opinion and consensus on the most appropriate driving forces. This will be followed by a scenario exercise focusing on the manifestation of information warfare as a national security threat by the 2030s.

## **CHAPTER 7**

# **VERIFYING AND PRIORITISING DRIVING FORCES FOR INFORMATION WARFARE FUTURES THROUGH THE DELPHI METHOD**

### **7.1 INTRODUCTION**

The model developed in Chapter 6 assisted in identifying eleven driving forces relevant to the future manifestation of information warfare. These driving forces are central to the development of the scenarios explaining the possible manifestation of information warfare by the 2030s. The value of the model's output is increased when it is scrutinised, improved and validated by local and global experts with knowledge of the Information Age dynamics relevant in terms of the current and future manifestation of information warfare. This is achieved by using the Delphi method, which is a structured technique employed to arrive at an expert consensus opinion on the main driving forces, influencing the scenarios focused on the manifestation of information warfare as a South African national security threat by the 2030s.

Two Delphi studies are conducted in this chapter. The pilot Delphi study is completed with South African security experts as panel members. A second Delphi study is conducted with both domestic and international experts (knowledgeable in one or more TWEPS environments) participating. As illustrated in the overview of the manifestation of information war in Chapter 5, this is a global phenomenon that can hardly be evaluated outside its international context. Hence, the second Delphi study is undertaken to ensure that a more diverse group of expertise adds additional value and validates the driving forces.

The Delphi method was initially developed as a methodical, interactive forecasting technique which depends on a panel of experts. In this study, the Delphi studies are useful to authoritatively validate and identify the main driving forces used to create possible future scenarios regarding the manifestation of information warfare as a national security threat in the 2030s (Roux, 2012). This method is based on a structured and democratic approach to forecasting, using the combined wisdom of participants (Powell, 2003:381).

The Delphi methodology became known when the USA-based RAND Corporation (Research and Development Corporation) used it during the 1960s for forecasting. Since then, academics and forecasters have used it periodically for qualitative explorations into complex issues or domains. The overall purpose of Delphi studies is to facilitate formal discussion among selected experts in given environments around a specific topic. The method encourages the sharing of diverging worldviews over a few "rounds" or iterations in the hope that the views may converge into some

direction around the given topic. The Delphi has often been used in situations or environments that tend to be somewhat ambiguous, in particular when it is not possible for those experts to easily gather in one place and where interviews and surveys are neither timely nor appropriate (Wakefield & Watson, 2013:577). Delphi also prevents strong personalities from dominating the agenda and views regarding issues under investigation.

## 7.2 VALIDATION AND PRIORITISATION OF DRIVING FORCES

The identified eleven driving forces need to be validated and prioritised. At the same time, expert suggestions for improvements and additional relevant insights will also enhance the quality of the Delphi studies' output. The analysis of the driving forces will be deepened by testing them against the insights of local and global experts with relevant knowledge on one or more of the identified environmental domains. The Delphi studies are done on the one hand to verify, tweak and refine these forces derived from the environmental analysis and on the other to prioritise the driving forces with the aim to assist in identifying the two key scenario drivers.

Although a collective approach in analysing challenges might not always be the best solution, a managed approach such as the Delphi method has proved itself as highly constructive in aggregating inputs from expert and peer groups (Lanier, 2006). According to Linstone and Turoff (2002:4), the application of a Delphi study will usually be necessary when one or more of the following properties are present:

- The problem does not lend itself to precise analytical techniques but can benefit from subjective judgements on a collective basis.
- The individuals needed to contribute to the examination of a broad or complex problem have no history of adequate communication and may represent diverse backgrounds with respect to experience or expertise.
- More individuals are needed than can effectively interact in a face-to-face exchange.
- Time and cost make frequent group meetings infeasible.
- The efficiency of face-to-face meetings can be increased by a supplemental group communication process.
- Disagreements among individuals are so severe or politically unpalatable that the communication process must be refereed and/or anonymity assured.
- The heterogeneity of the participants must be preserved to assure validity of the results, i.e. avoidance of domination by quantity or by strength of personality ("bandwagon effect").

In this study, all of the above properties are valid to some extent, and the Delphi studies have proven to be an appropriate methodology for the purposes stated.

Additionally, a Delphi study is a valuable tool to ensure that contemporary developments are taken into account. This is the case, because the Delphi study facilitates a strong forecasting dynamic, the method also tends to be useful for staying abreast of the most recent technological advances.

Articles and books frequently lag behind actual research because of the time necessary for writing, editing and printing. A Delphi study, by contrast, can provide a more updated exchange of information than a literature search by drawing upon current knowledge and experiences of experts and rapidly reproducing it (Nielsen & Thangadurai, 2007:148). This is especially valid in terms of information warfare, which continues to generate daily news headlines, while technological developments ensure that ever more innovative uses of information warfare become possible.

A fundamental question regarding the importance of value adding at this stage can be asked: "Is it possible, via structured communications, to create any sort of collective human intelligence<sup>26</sup> capability?" (Linstone & Turoff, 2002:5). Such a capability is necessary for validating, prioritising, narrowing down, improving and integrating the already identified driving forces. The most appropriate method to do this for the purposes of this study is by utilising the Delphi technique (Roux, 2012).

### **7.3 BACKGROUND TO THE DELPHI METHOD**

The Delphi method originated at the RAND Corporation in the 1950s to 1960s as a systematic method for obtaining expert opinion on a variety of topics although it was initially used especially in technological forecasting (Sackman, 1974:iii). Since then it has been used extensively in social research as a qualitative research methodology. A Delphi study is a structured communication method, developed as an interactive, systematic forecasting technique that relies on a panel of experts (Linstone & Turoff, 1975:1). The method can also be described as a controlled debate (Gordon, 2003:5). The controlled debate or structured communication is created by providing feedback on individual contributions; offering some evaluation of the group views or judgement; providing some level of anonymity for the individual responses; and presenting some prospect for individuals to modify views (Linstone & Turoff, 2002:3). This structured communication is achieved through the use of questionnaires.

A Delphi study is thus rooted in the principle that evaluations (or forecasts) from individuals in structured groups are more accurate than those from unstructured groups (Rowe & Wright, 2001:124). The aim is to exploit the "collective intelligence" of knowledgeable individuals (Hiltz & Turoff, 1978:16). Rowe, Wright and Bolger (1991:235–251) stated that for Delphi to be of value, it should offer more accurate judgements or assessments than those gained either by interacting groups or individuals. Other techniques for obtaining consensus, such as meetings or committees, are generally acknowledged to be disposed to be improperly influenced by individuals. Specific problems include domination by powerful individuals, the biasing effects of seniority, personality traits as well as the reality that only one individual can speak at a time (Powell, 2003:377). While the standard that groups in general perform superior to the best member remains valid, Rowe,

---

<sup>26</sup> Linstone and Turoff (2002:5) indicated that "intelligence" in this situation also includes feelings and attitudes which are part of human actions and motivations.

Wright and Bolger (1991:238) also recognised that process loss can occur, which refers to the effect that the actions and presence of individuals in group situations may restrain the possibility of resolving conflicting and ambiguous issues while also constraining general creativity. However, the participant anonymity offered by the Delphi method and its democratic, structured approach can assist in a process gain.

A Delphi study is a virtual panel of experts gathered to arrive at an answer to a challenging problem. Thus, a Delphi study could be considered a type of virtual meeting or group decision technique, though it appears to be a complicated survey (Okoli & Pawlowski, 2004:19). Although the Delphi method has its origins in the American security community, it has since been widely accepted throughout the world in a diversity of domains including political science, business, defence, education, information technology, transportation, health care and engineering. The flexibility of this method is evident in its many research applications globally (Skulmoski, Hartman & Krahn, 2007:1).

The Delphi study is especially useful as a communication tool for generating debate. Thus, the output of a Delphi study is an informed opinion and its output should be interpreted as such (Powell, 2003:377). However, the method does offer generalisability and reliability of its results, guaranteed through the repetition of rounds for data collection and analysis, directed by the principles of anonymity and democratic participation. A Delphi study is therefore more than a form of data collection; its repetitive feedback technique expands insight, which in its whole “is more than the sum of the parts” (Day & Bobeva, 2005:104).

#### **7.4 THE DELPHI STUDY PROCESS**

In a Delphi study, experts from the required disciplines are first identified and then requested to take part in the inquiry. The identified experts then provide inputs based on questionnaires in two or more rounds. After each round, the facilitator provides a summary of the experts' inputs from the previous round without identifying the experts. The reasons and/or comments they provide for their judgments are also included. In this way the experts are encouraged to modify their earlier inputs based on the replies received from other members of the panel. It is expected that during this process, the range of the replies will become more focused and the group will move towards a consensus position. Finally, the process is stopped after a pre-defined stop criterion (e.g. achievement of consensus, stability of results or number of rounds reached) and the median or mean scores of the final round are used to determine the concluding results (Rowe & Wright, 1999:353).

A Delphi study does not (and is not intended to) generate statistically significant results, seeing that the number of participants is usually limited. Therefore, the results provided by any Delphi panel do not foresee the response of a different Delphi panel or a larger population. These results embody the synthesis of the particular group's opinion, no more, no less. The value of the Delphi method

rests with the ideas it generates, both those that evoke consensus and those that do not. The arguments for the extreme positions also represent a useful product (Gordon, 2003:5).

The foremost advantage of a Delphi study is the attainment of consensus in a particular area of uncertainty where there is a lack of empirical evidence (Powell, 2003:377). In this study, the identified driving forces of the envisaged information warfare by the 2030s provided such a focus area. The Delphi method also works well when the goal is to improve understanding of challenges and opportunities, or to develop forecasts (Skulmoski, Hartman & Krahn, 2007:1). It should, however, also be noted that outcome of a Delphi study unavoidably reflects the subjective bias, cultural attitudes and knowledge of those who formulated the outcome (Linstone & Turoff, 2002:226).

As a method of communication during a Delphi study, direct interaction between the facilitator and individual panel members can take place if the panel members are reachable. More common would be the use of electronic communication in the case where the panel members are from geographically distant places. Electronic communication allows the group to focus quickly on the major developments identified and communicate on those issues in detail. Additionally, because anonymity is used, it is compulsory for each participant to evaluate the prospects of each driving force on the basis of his or her understanding and the backing arguments presented. The predisposition to evaluate only those positions recommended by the most distinguished panellists is also eradicated as a result of anonymity (Enzer, 2006:189). The Delphi method is highly suitable for the purposes of a futurist-orientated study.

## **7.5 FRAMEWORK OF THE DELPHI STUDY**

The taxonomy of Delphi designs choices is extensive. In the design of a Delphi study, additionally to criteria set by the subject domain, the following must be taken into account (Day & Bobeva, 2005:104-105):

- Purpose of the study
- Number of rounds
- Participants
- Mode
- Anonymity
- Media
- Concurrency.

The two Delphi studies conducted on the driving forces influencing information warfare as an upcoming national security threat are conducted based on the above-mentioned criteria.

### **7.5.1 Purpose**

The purpose of a Delphi study can include activities such as the creation, building, exploration, testing and evaluation of knowledge (Day & Bobeva, 2005:104). In this research, Delphi studies are used to validate and prioritise the main driving forces which will impact the manifestation of information warfare by the 2030s. Additionally, the Delphi studies' outcomes will also provide expert direction, tweak the driving forces, generate new ideas, offer base insights and provide additional inputs for the scenario process.

### **7.5.2 Number of rounds and questionnaire**

The number of rounds in a Delphi study can vary between two and ten, but it is usually restricted to two or three rounds (Day & Bobeva, 2005:104). However, the decision regarding the number of rounds remains mainly pragmatic as it is also required to balance cost, time and possible panel member fatigue (Powell, 2003:378). As the aim is to find consensus on the eleven identified driving forces, it is calculated (based on case studies) that a maximum of three rounds will suffice in finding consensus among experts. If a sufficient degree of consensus cannot be reached, an additional round can be implemented.

Although Delphi studies initially used open-ended questionnaires, Hsu and Sandford (2007:2) noted that it is both an acceptable and common modification of the Delphi process format to use structured questionnaires which are based upon an extensive review of the literature. Kerlinger (1973) noted that the use of a modified Delphi process is appropriate if basic information on the target issue is available and usable. Information warfare media coverage has reached high levels and increasingly professionals in a variety of professions are taking note of this phenomenon. Hence, a modified Delphi process will suit the research approach followed in this thesis.

### **7.5.3 Participants and panel size**

The profile of the panel members can be defined in terms of knowledge, nationality, age, expertise, qualifications, background, position and/or occupation. These distinctions can be used to analyse both heterogeneous and homogeneous groups. Of specific importance to researchers using a Delphi study is ascertaining the expertise of the panel members as this affects the value of the outcomes (Day & Bobeva, 2005:104). The pilot Delphi study members in this investigation were homogeneous in terms of nationality, age, qualifications and occupation but heterogeneous in terms of background. The convergence was knowledge of international security issues as applied to South Africa.

The second Delphi study members were heterogeneous in terms of nationality, knowledge, age, qualifications, expertise, background, position and occupation. The convergence was knowledge applicable to the manifestation of information warfare in one of more of the TWEPS environments. In Chapter 5, the overview of the current information warfare manifestation illustrated that it has become so prevalent that incidents are reported in the international media daily. Most of the Delphi

panel members were not experts on information warfare. Instead, they were experts on contemporary security and political, economic and social issues. Therefore, as a minimum, they had sufficient knowledge about the phenomenon of information warfare and they were in a position to make an informed judgement about its current and future manifestations.

In general, Delphi studies make use of large panel sizes. Reid (1988:28), for example, referred to “panel sizes ranging from 10 to 1685” members. Experience suggests that the number of panel members will fluctuate according to the resources available and the scope of the problem. Seeing that experts are used as Delphi panel members and taking into account that the process calls for convergence of opinion, panels of approximately 10 experts are used in this study.

An expert is defined as “a person who is very knowledgeable about or skilful in a particular area” (Oxford Dictionaries, 2014). This study focused on selecting a wide range of experts, preferably knowledgeable on at least one of the TWEPS environments. An overarching field that is relevant in terms of information warfare (especially for the primary Delphi) is the security field. Jairath and Weinstein (1994:33) proposed that panel members should be experts who reflect current perceptions and knowledge, yet are comparatively neutral to the findings. Powell (2003:379) stated that heterogeneous groups, characterised by participants with extensively differing personalities and significantly diverse worldviews, produce a greater proportion of high-quality, highly satisfactory solutions than homogeneous groups.

A Delphi study does not require panel members to be representative samples for statistical purposes; therefore the quality of the expert panel is assessed on its expert representativeness rather than its numbers (Powell, 2003:378). The focus in this study was on experts who were knowledgeable about the strategic implications of information warfare as a national security threat. A variety of viewpoints that cover respectable controversy will also assist in generating interest and participation (Linstone & Turoff, 1975:15). Rowe (1994:165) supported this assertion and suggested that experts should be drawn from varied environments in order to guarantee a broad base of knowledge. Many users of the Delphi method propose that experts should be chosen for their credibility with the target audience and work in the appropriate field (Powell, 2003:379).

#### **7.5.4 Choosing the participants**

Participants in the primary Delphi, which also served as the pilot Delphi study, were chosen from the South African state agency responsible for foreign security. Senior analysts and management members with at least ten but up to thirty years of substantive security-related experience were requested to participate in the Delphi. These individuals were deemed as experts on the security challenges facing South Africa and were thus in a position to make an authoritative judgement on the main driving forces fundamental to information warfare’s manifestation as a national security threat by the 2030s. In the light of the interconnected global society and fast changing world, it would not be appropriate to only depend on such input as the only judgement on the future manifestation of information warfare. A second Delphi study was undertaken to evaluate the

judgements of the pilot Delphi study and to obtain additional strategic insights on driving forces expected to impact on the future manifestation of information warfare.

Panel members for the second Delphi study were chosen to represent a variety of experts on one or more of the TWEPS environments. Individuals both domestic and international were identified based on their expertise in relevant TWEPS environments. Individuals who were known to the researcher as well as experts who were identified based on their proven practical expertise were selected. Each respondent was chosen based on his or her potential to contribute in terms of the environments covered by the environmental study.

#### **7.5.5 Mode**

The mode used in a Delphi study refers to how the interaction is conducted – through face-to-face discussions or remote access via electronic communication (Day & Bobeva, 2005:105). Both modes were used in these Delphi studies. Remote access can also help to ensure the anonymity of the participants.

#### **7.5.6 Anonymity**

In a Delphi study, it is common practice that all participants uphold anonymity. Even after the completion of the final report the participants' identities are not revealed. The advantages of maintaining anonymity include the following: stopping individuals from dominating others by using their authority or personality, freeing participants to some extent from their personal biases, minimising the "bandwagon effect" or "halo effect", allowing participants to freely express their opinions, admitting errors by revising earlier judgements and encouraging open critique. This approach avoids the negative effects of face-to-face panel discussions and solves the common problems of group dynamics (Day & Bobeva, 2005:106).

#### **7.5.7 Media**

A wide variety of media can be used in Delphi studies. This includes physical paper and pen, phones and computerised communication. Progress in ICT is transforming society and business. The expediency of electronic communication has driven the development of the Delphi technique forward to computer-mediated studies. This translates into progress which can include support from multi-media, modelling and simulation tools, and increase new research prospects for the technique (Day & Bobeva, 2005:105).

In this study both paper-and-pen based media and electronic media were used. The pilot study used hard copy questionnaires as most of the panel members worked in the same building. The second Delphi study was done mainly via e-mail as the panel members' locations were geographically remote.

### 7.5.8 Concurrency

Most Delphi studies use a standard chronological set of rounds or real-time online conferencing. ICT options such as video conferencing allow for various concurrency modes, depending upon the character of the issue under investigation as well as the urgency of its resolution (Day & Bobeva, 2005:105). In this study, a sequential set of rounds was used.

See Table 7.1 for a summary of the taxonomy used in this study.

**Table 7.1: The Delphi design choices in the study of driving forces impacting information warfare**

<b>Criteria</b>	<b>Choice for validating and identifying information warfare driving forces</b>
Purpose of the study	Knowledge creation, prioritisation and validation of driving forces
Number of rounds	Maximum of three per Delphi study
Participants	Heterogeneous group
Mode of operation	Both remote and paper based
Anonymity of panel	Full
Communication media	Face-to-face and e-mail
Concurrency of rounds	Sequential

Source: Adapted from Day and Bobeva, 2005:105.

### 7.5.9 Evaluation criteria

Fink, Kosecoff, Chassin and Brook (1991:78) proposed a number of prerequisites to guarantee credibility in Delphi findings. These prerequisites include a lucid decision trail that defends the suitability of the method to address the issue under investigation, the choice of expert panel members, the data management processes, the identification of justifiable consensus stages, and the means of dissemination as well as implementation. These issues are extensively addressed in this chapter and in the annexures. Other validity and credibility issues include biases, rigour, trustworthiness and expertise.

Qualitative evidence also needs to be analysed in order to properly acknowledge the biases of the participants and researchers (Day & Bobeva, 2005:112). The choice of participants takes the bias challenge into consideration. In this study, the choice of experience, a long track record (10 years plus) of working in the security environment and the seniority of the individuals ensured that this bias was minimised. In addition, the participants in this study represented different genders and races, and came from divergent backgrounds – some from the apartheid structures, some from the liberation structures and some from the post-transition era. They were involved in managing national security from a South African perspective and were indeed knowledgeable about the South African national interest in terms of national security. In order to counter the South African bias in this group, the second Delphi study was done with a combination of domestic and international participants. This provided different views and opened up opportunities to expand insight into the driving forces under investigation.

One challenge associated with the analysis of qualitative evidence is the lack of instruments available to refine a significant number of unstructured, non-numerical and loaded data sets obtained through conducting Delphi studies (Day & Bobeva, 2005:112). As the Delphi studies in this study focused on prioritising the identified eleven driving forces, these Delphi studies did not generate such large data sets. Hence, it is possible to use qualitative text analysis to code the outcomes of the Delphi study and to facilitate the use of the outcome in the scenario exercise.

The questionnaire was developed by utilising a future studies model applicable to information warfare futures in which CLA and qualitative text analysis coding were central. This enhanced confidence in the primary data in addition to the standards for validity and reliability of the questionnaire. Additionally, an audit trail was created, providing a sequence of evidence through the data analysis stages (Day & Bobeva, 2005:113), both for the pilot and second Delphi studies.

The examination of the plausibility and consistency of panel members' inputs assists in assessing the rigour of the research findings and the internal validity criteria. When managing the Delphi process, continuous feedback and confirmation by panel members help to ensure that tests of quality are maintained throughout the process. The facilitator also recognised that during the implementation of the rounds important contextual changes must be detected and appropriately acknowledged (Day & Bobeva, 2005:112). The identification of the driving forces was derived from the researcher's environmental scanning, but adequate opportunity was provided for the experts to modify, add or reject any of the driving forces. These processes have been systematically documented in tables covering each driving force in each round. (See Figures 7.2 to 7.59 for panel member feedback and evaluation.)

According to Flanagan and Metzger (2008:7), credibility has two key components, namely expertise and trustworthiness, which both have objective and subjective components. Expertise is based more on subjective factors, but also includes relatively objective characteristics of the source or message (e.g. credentials, certification or information quality). Trustworthiness can also be

perceived subjectively, but can include objective measurements such as established reliability. Scientific credibility has been defined as the extent to which science in general is recognised as a source of reliable information about the world (Bocking, 2004:164).

The use of multiple participants assists in strengthening the credibility of a Delphi study. For this study, this meant comparing the results obtained from the pilot study with another study. The variations in outcomes between Delphi studies can be attributed to the ability of each person to comprehend the formulated driving forces from his or her own worldview, as well as to the different contextual settings in which the individuals function. The measure used to decrease this risk to plausibility is the inclusion of a reason for the survey as well as an explanation of the source of the driving forces. Panel members were invited to contact the researcher for further clarification.

While the duplication of outcomes from another context is the ultimate test for external validity, this is not so significant for Delphi studies. Gordon (1994:1) explained this as follows: "Because the number of respondents is usually small, Delphis do not (are not intended to) produce statistically meaningful results; in other words, the results by any panel predict the response of a larger population or even a different Delphi panel. They represent the synthesis of opinion of the particular group, no more, or less."

In the case of a Delphi study it is more constructive and appropriate to take a qualitative viewpoint by investigating the outcomes of the study for their coherence, plausibility and relevancy by "identifying the explicit limitations upon transferability of the results to other contexts" (Day & Bobeva, 2005:113).

A Delphi study permits a certain inter-subjective selection from the more or less spontaneously and intuitively expressed individual opinions. The method is based on the assumption that a forecast that can be agreed upon by the majority of those surveyed will possess a greater degree of credibility than the opinion of an individual expert. Consequently, the composition of the surveyed group will have a considerable impact on the results of the survey. Special caution is justified when it comes to the role extraneous motives might play in the formation and expression of the opinions held by the experts participating in the survey. Experts may, for instance, present a skewed view (i.e. overly optimistic) of the future prospects of work in their own fields, while a tendency towards self-fulfilling prophecies cannot be ruled out (Pillkahn, 2008:195). In the case of the two Delphi studies conducted in this study no extraneous motives could be identified. The participants did not stand to gain from the outcome of the study.

## **7.6 PILOT DELPHI STUDY**

### **7.6.1 Aim of the pilot study**

A pilot study is a research project that is conducted to allow the researcher to get a clearer idea of the investigation or to fine-tune the focus of the study. It is typically used to evaluate survey questions and to refine the questionnaire (Crossman, 2014). A pilot study is also conducted to

assist in identifying ambiguities and to improve the general administration for the follow-up Delphi study (Powell, 2003:378). However, as this pilot study involved South African national security experts, the pilot study was also the primary contributor to the content and identification of the driving forces relevant to the South African future information warfare scenarios.

### **7.6.2 Focus of the pilot study**

The pilot study was conducted taking into account all TWEPS environments included in the environmental scan. One of the outcomes of the environmental scan was that national security is an overarching issue that impacts all environments in terms of information warfare. In this regard, one of the main focus areas for conducting of a Delphi study is the national security environment in South Africa. At the same time, the study conducted in this environment also served as the Delphi pilot study. Hence, the pilot study results were fully incorporated in the overall results as participants cannot be expected to participate twice in the study.

The pilot study utilised a South African foreign security panel providing a cross-environmental perspective on the proposed driving forces. In January 2014, the relevant state entity responsible for South African foreign security related issues granted permission for the researcher to proceed with a Delphi study, provided that no participants were identified and no organisational information was revealed in the study. These provisos had no negative impact on the outcome of the pilot study as this Delphi study was not intended to provide classified information.

The Departmental Ethics Screening Committee of the University of Stellenbosch Business School (USB-DESC) reviewed the researcher's application for a Delphi Study and the research as set out in the ethics application was approved on 23 June 2014.

### **7.6.3 Participants in the pilot study**

A group of 13 senior officials working in managerial roles in the security environment were identified to participate in the Delphi Study on the key drivers central to the future manifestation of information warfare. This provided for some leeway should some of the participants not be able to participate in all the rounds. It is essential that expert panel members are able and willing to make a significant contribution.

As expertise in national security would be a requirement, the following factors were taken into account in identifying possible participants:

- At least 10 year of experience in national security core business
- Analytical and/or national security management experience
- A higher degree in national security, international relations, political science or public administration
- Representing a diversified group in terms of race and gender.

Diversity in age was not significant with most participants in the age group early 40 to late 50. This is in line with the requirement that the panel members should be experts. In this study, most of the panel members had 20 years of experience in national security related work. All participants were serving officials (senior analysts and/or management level) in a public foreign security environment. None of the individuals primarily focused on information warfare as research topic. However, from an analytical or operational viewpoint, all the participants were responsible for international, regional or thematic foreign security issues in which information warfare was becoming a growing issue.

Once the potential participants had been identified, they were individually contacted and asked for permission to become part of the pilot Delphi panel. As they were all based in Pretoria, the initial contact was personal. The following was briefly discussed: It was indicated that their expertise in the security field will be relevant to information warfare as an upcoming national security threat. It was emphasised that participation would be voluntary and that individuals were free to stop participating at any stage. Their identities would not be revealed to other members of the study or identified in the final thesis. In addition, their privacy would be respected and it was confirmed that organisational approval had been granted for their participation.

The guidelines for participation encouraged panel members to question anything but also to provide solutions, suggestions, leads and clues to possible answers. The panel members were requested to add value to the study. In the cover letter, some direction was provided but it was also carefully formulated not to limit or restrict the requested responses. As the scope must be as wide as possible for unhindered input an additional open-ended question was included to solicit wider contribution by the panel members and to obtain ideas for additional driving factors. This question requested panel members to identify any additional driving forces which would be relevant in the context of the future manifestation of information warfare. Completely off-target responses would rather be disregarded by researcher than preventing potential creative inputs. In this cover letter some insight was provided into the methodology and definitions, but it was also kept brief and basic not to unduly influence panel members.

After obtaining their verbal consent, a cover letter (see Appendix C, Table C:1 for the cover letter) and the questionnaire were provided in hard copy or, if requested, in electronic copy. Round 1 of the pilot Delphi study was conducted from 4 to 29 August 2014. Questionnaires were distributed to 13 participants and responses were received from 10. The second round was conducted from 8 January to 12 February 2015. Questionnaires were distributed to 10 participants and responses were received from eight participants.

#### **7.6.4 Structuring of the questionnaire**

The aim of the questionnaire was to obtain an expert group evaluation, validation and prioritisation of the driving forces which will influence the manifestation of information warfare as an upcoming national security threat in the 2030s. The questionnaire was designed to be as organised and as

clear as possible. It was presented in landscape table format. The layout of the questionnaire was based on the example provided by Day and Bobeva (2005:110). The driving forces influencing the future manifestation of information warfare were listed as statements from one to eleven. The formulation of the driving forces were identical, as indicated in Table 6.6, which reflected the results of the CLA assessment done on the output of the information warfare environmental scan, framed within the futures framework model developed in Chapter 6. (See Appendix B, Table B:1 for the questionnaire used in the Pilot Delphi study)

Delphi panel members were requested to measure each driving force first against its current significance and then against its futures relevancy (2030). A 10-point Likert scale was used for both current significance and futures relevancy. On the scale, 1 was coded to be the least feasible/desirable constituent while 10 was coded to be the most feasible/desirable driving force. When responding to the Likert questionnaire item, respondents were required to specify their level of agreement or disagreement on a symmetric agree-disagree scale for the series of 11 identified driving forces. Thus, the range captured the intensity of their evaluation for a given item (Burns & Burns, 2008:245).

A typical five-level Likert item scale ranges from 1st level (strongly disagree) to 2nd level (disagree), 3rd level (neither agree nor disagree), 4th level (agree) and 5th level (strongly agree). This is not sufficient for the purposes of this study. In order to allow the Delphi experts to provide a more precise evaluation of each driving force on a scale ranging from 10% to 100%, a 10-level Likert item scale was used. This provided the Delphi participants with an opportunity to measure the impact of each driving force against the two dimensions requested, namely against its current significance and then against its potential relevancy in the 2030s.

The driving forces will serve as ordering data input for the Delphi Study. Ordering data can be described as data in which an ordering or ranking of responses is possible but no measure of distance is possible (Allen & Seaman, 2007). Ordinal thus refers to quantities that have a natural ordering potential. With ordinal data it is impossible to state with certainty whether the intervals between each value are equal. On a 10-point scale, the difference between 9 and 10 is not necessarily the same difference as the difference between 6 and 7.

It is widely recognised that the types of data as well as the class of problems that a researcher is likely to encounter vary greatly with the field of research. Consequently, methods that are useful in one area or discipline may be of little use or interest to research in another area. In the physical sciences, for example, the overwhelming proportion of the data is essentially quantitative although possibly measured on an arbitrary scale. In the social sciences, qualitative data is more common. These qualitative measurements, whether subjective or objective, usually take values in a limited set of categories which may be an ordinal scale (McCullagh, 1980:109).

Next to each driving force space is provided for the panel members to make comments, suggest changes, raise arguments and ask questions. To allow the panel members to make overall

comments and to identify additional driving forces, the questionnaire ends by requesting the participants to "... identify any additional driving forces which would be relevant in the context of the future manifestation of information warfare".

The questionnaire was designed to present clear, unambiguous and concise statements, together with understandable instructions for the participants. During the pilot study some participants were also requested to provide general feedback on the clarity and format of the questionnaire. It has been observed that an easy-to-complete and aesthetically pleasing questionnaire positively influences a panel member's decision whether or not to take part in the Delphi study (Day & Bobeva, 2005:110). The questionnaire should also be designed to take no more than 30 minutes to complete (Okoli & Pawlowski, 2004:23).

The initial contributions from the panel members were collected in the form of answers to the questions and their comments on these answers. The researcher as facilitator controlled the interactions among the participants by processing the information and filtering out irrelevant content. Individually drafted second-round questionnaires were provided to the participants in which the comments on the analysed driving forces were consolidated, and the individual and group scores were provided.

More detailed descriptions of all elements of the Delphi study are provided in the round-by-round discussions below. Results are analysed according to the research paradigm's qualitative coding (Skulmoski, Hartman & Krahn, 2007:4). In this regard, qualitative text analysis was used as explained in 6.2 coding of the environmental scan output.

### **7.6.5 Evaluation of Delphi Study Pilot Round 1**

The aim of the first round of the Delphi study was to add value to the evaluation in terms of the information warfare futures model which included the results of the environmental scan and subsequent CLA study, leading to the identification of 11 driving forces relevant to information warfare as an upcoming national security threat. In processing each driving force it was coded and the category / subcategory stated while a scale for measuring the driving force was included. This assisted in the evaluation of the driving forces and informed the scenario-processes.

The Delphi results were verified (continuously through the Delphi) and the extent to which the results can be generalised was also investigated (Skulmoski, Hartman & Krahn, 2007:5). The questionnaire was enhanced by integrating and assimilating information. This was done primarily through the qualitative analysis of the results which in turn provided the foundation on which to create the second questionnaire (Powell, 2003:378).

This process of value adding by a divergent expert group (represented by the Delphi group) entailed the following:

- Validating the driving forces as applicable
- Reformulating driving forces according to responses

- Casting doubt on any driving force and/or identifying any contrary interpretation
- Identifying implications and adding insight into the future impact of the driving forces
- Identifying possible wild cards which could fundamentally influence future outcomes
- Identifying new ideas that have not been focused on during the environmental study.

All responses (comments, suggested changes, arguments and questions) were collated on a single spreadsheet and the median Likert score was calculated for both the current and future impact of each driving force. Supplementary input on identifying any additional driving forces which would be relevant in the context of the future manifestation of information warfare was also listed.

Based on the feedback some reformulations of driving forces were deemed to be appropriate for Round 2. The reformulations served to clarify the issues and not to change the essence of the driving force. One driving force was replaced by another based on the feedback.

**Table 7.2: Evaluation of Driving Force 1 (first-round pilot Delphi)**

<b>Driving Force 1</b>	“Globally the centre of power is shifting, enhancing the political, social and economic influence of individuals and sub-state’s entities in the world.”		
<b>Collective Likert score (current significance)</b>	6.3	<b>Collective Likert score (futures relevancy)</b>	7.2
<b>Comments from panel members</b>	<p>“States as sovereignty bound actors are resisting this trend. The centre of power shift will not be too important given the short timeframe to 2030.</p> <p>Sentence is too broad and there are two parts of which the impact is different: 1) Centre of power shifting has implications for balance of power among states which could be a driving force.</p> <p>Not sure what you mean by sub-state entities. If you want to say that individuals will become driving force then put it as such separately.</p> <p>What was traditionally considered the centre of power is shifting. However, aware of that traditional power brokers will change the rules of the game to redefine power and with it new definition of what the centre of power is.”</p>		
<b>Evaluation</b>	The feedback received indicated that the meaning was not clear as two issues were addressed, namely shifting power and the		

	influence of individuals and sub-state entities in the world. Driving Force 7 was already referring to the role of sub-state entities. Based on these arguments a new formulation (see below) for this driving force was created for Round 2 and subsequent questionnaires. This will highlight a specific aspect of the shifting of power referred to in the original formulation. The new formulation will by implication include both state power and power associated with the other environments, addressing the concerns expressed about this driving force.
<b>Decision on formulation of Driving Force 1</b>	Change formulation. The new formulation: “The centre of power is shifting from the traditional developed countries to the developing countries.”

Source: Round 1 of Delphi Pilot Study.

Based on qualitative text analysis, this driving force falls in the category “Transformation”, sub-category “Shift”, in which the specific dimensions can be measured on a weak-strong axis as well as a static-dynamic axis.

**Table 7.3: Dimensions of the category “Shifting Power”**

Category	Sub-category	Specific dimension
Transformation	Shift	Weak – Strong Static – Dynamic

Source: Coded based on Kuckartz, 2014:25.

**Table 7.4: Evaluation of Driving Force 2 (first-round pilot Delphi)**

<b>Driving Force 2</b>	“Security is increasingly becoming a more encompassing, globally influenced and networked phenomenon.”		
<b>Collective Likert score (current significance)</b>	6.7	<b>Collective Likert score (futures relevancy)</b>	8.2
<b>Comments from</b>	“Increased security will make information warfare more difficult		

<b>panel members</b>	<p>than in the past. Most internet users are probably more security aware.</p> <p>Peace and security issues are discussed at forums such as the BRICS, previously only an economic forum.</p> <p>I would scrap networked.</p> <p>No people will relinquish entirely their security to an outside force as it is primal to human existence, hence the 9 in terms of future relevance.</p> <p>Security is not defined to assist in understanding the use of the “term” and “sphere”. Increasingly, indications suggest that advanced conflict will be characterised by struggle over information systems impacting on both physical and substantial security.</p> <p>Particularly in Africa where states do not seem to have the resources to deal with their security challenges, making them dependant on big powers so the status quo remains.”</p>
<b>Evaluation</b>	<p>The comment that security is not defined to assist in understanding the use of the “term” and “sphere” is valid. The reference to the expected increase in struggle over information systems also highlights both the physical and non-physical elements of security. This also stresses the increasing complexity of security if the digital and technological advances are taken into account. The comment to scrap networked can be disregarded as this is the core concept of this driving force. The shift to network security is also confirmed by some of the panel members’ comments. The comment that increased security will make information warfare more difficult than in the past can be disregarded as increased security results in even more innovative efforts to counter it (Booz Allen Hamilton Inc, 2012).</p>
<b>Decision on formulation of Driving Force 2</b>	<p>Change formulation.</p> <p>New formulation: “Security in a networked environment will increase in complexity as its physical and non-physical elements increase.”</p>

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category “Networked”, sub-category “Interconnection”, in which the specific dimensions can be measured on a low-high axis.

**Table 7.5: Dimensions of the category “Networked Security”**

Category	Sub-category	Specific dimension
Networked	Interconnection	Low level of manifestation – high level of manifestation

Source: Coded based on Kuckartz, 2014:25.

**Table 7.6: Evaluation of Driving Force 3 (first-round pilot Delphi)**

<b>Driving Force 3</b>	“Integration of systems, processes are exponential in the Information Age.”		
<b>Collective Likert score (current significance)</b>	6.4	<b>Collective Likert score (futures relevancy)</b>	8.6
<b>Comments from panel members</b>	<p>“The dominance of integration is not necessarily ensured; systemic stresses may increase as centripetal and centrifugal forces clash.</p> <p>The more integration also means more difficulty to conduct information warfare in the sense that own systems could be accidentally harmed.</p> <p>But also more dangerous.</p> <p>Because all forms of struggle over control and dominance of information are components of one struggle essentially.</p> <p>True, however, this might in itself present a major future security challenge.”</p>		
<b>Evaluation</b>	The comment that the focus should be on the clash of centripetal and centrifugal forces clarified the impact of this driving force. By only focusing on the integration aspect, the driving force does not truly cover the complexity observed in the broader environment.		
<b>Decision on</b>	Change formulation.		

<b>formulation of Driving Force 3</b>	New formulation: “Systemic stresses from clashing centripetal and centrifugal forces will increase exponentially.”
---------------------------------------	--

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category “Transformation”, sub-category “Revolution”, in which the specific dimensions can be measured on a high-low axis.

**Table 7.7: Dimensions of the category “Clashing Centripetal and Centrifugal Forces”**

Category	Sub-category	Specific dimension
Transformation	Revolution	High Level – Low Level

Source: Coded based on Kuckartz, 2014:25.

**Table 7.8: Driving Force 4 (first-round pilot Delphi)**

<b>Driving Force 4</b>	“Despite the dominance of integration many human endeavours are also faced with systemic stress as challenges associated with centralisation and decentralisation are impacting on entities globally.”		
<b>Collective Likert score (current significance)</b>	6.2	<b>Collective Likert score (futures relevancy)</b>	6.3
<b>Comments from panel members</b>	<p>“The main role-players are not expected to have a problem in overcoming such challenges.</p> <p>Complex.</p> <p>Clarify challenges.</p> <p>Do not consider this as an important issue. It is only relevant in lower systematic challenges and not a global phenomenon.</p> <p>New formulation: Integration of systems, processes are exponential in the Information Age.”</p>		
<b>Evaluation</b>	The new formulation of Driving Force 3 essentially captures this idea. It can thus be removed and replaced by a driving force recommended in the panel member’s feedback.		

	The request for additional driving forces resulted in a panel member suggesting that as interstate wars decreased, information warfare provides an opportunity to fill that void. This idea can be formulated in a driving force which could replace Driving Force 4 which has been removed based on feedback during Round 1.
<b>Decision on formulation of Driving Force 4</b>	Will be replaced by a new driving force. New Driving Force 4: "Information warfare will become an easy alternative and safe option for power projection."

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category "Transformation", sub-category "Renewal", in which the specific dimensions can be measured on a low intensity to high intensity axis.

**Table 7.9: Dimensions of the category "Alternative Power Projection Instrument"**

Category	Sub-category	Specific dimension
Transformation	Renewal	Low intensity – High intensity

Source: Coded based on Kuckartz, 2014:25.

**Table 7.10: Driving Force 5 (first-round pilot Delphi)**

<b>Driving Force 5</b>	"Symbolic, information-related phenomena are increasingly impacting behaviour."		
<b>Collective Likert score (current significance)</b>	6.2	<b>Collective Likert score (futures relevancy)</b>	7.3
<b>Comments from panel members</b>	<p>"Perception is now reality!</p> <p>Yes, symbols will play a bigger role to simplify messages and to overcome information overload.</p> <p>Very much evident in the social protests over the last couple of years.</p>		

	<p>Provide example of symbolic information. Not sure what you refer to.</p> <p>It is primal instinct for humans to respond to symbolism; hence, it would be very difficult for us to evolve sufficiently for it to have limited relevance.</p> <p>Psychological warfare works better with the element of surprise as it was the case during World War I and World War II.</p> <p>Example would assist to strengthen this question.”</p>
<b>Evaluation</b>	The significance of the symbolic in terms of the manifestation of information warfare was accepted by panel members. However, the need for a definition to put the concept into perspective was called for.
<b>Decision on formulation of Driving Force 5</b>	<p>Keep formulation, define symbolic:</p> <p>“Symbolic, information-related phenomena are increasingly impacting behaviour.”</p> <p>“Symbolic refers to representations (media or social media) which become reality.”</p>

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category “Innovation”, sub-category “Modification”, in which the specific dimensions can be measured on a low-level to high-level axis.

**Table 7.11: Dimensions of the category “Symbolic”**

Category	Sub-category	Specific dimension
Innovation	Modification	Low level – High level

Source: Coded based on Kuckartz, 2014:25.

**Table 7.12: Driving Force 6 (first-round pilot Delphi)**

<b>Driving Force 6</b>	“The speed of change is increasing exponentially with global communication becoming instantaneous.”		
<b>Collective Likert score (current)</b>	7.4 (second)	<b>Collective Likert score (futures)</b>	9.3 (highest)

<b>significance)</b>	<b>highest)</b>	<b>relevancy)</b>	
<b>Comments from panel members</b>	<p>“Once again, the system may get to a point where any more speed would lead to a breakdown.</p> <p>Yes, once information is out there, it is and will become more difficult to counter it.</p> <p>Probably most important characteristic together with 2 and 3.</p> <p>Change and technology are inextricable.</p> <p>This will increase even more particularly in Africa who is still lagging behind.”</p>		
<b>Evaluation</b>	<p>This driving force is regarded as particularly important both for its current as well as future significance. The formulation is not grammatically correct and needs to be amended slightly.</p>		
<b>Decision on formulation of Driving Force 6</b>	<p>New formulation:</p> <p>“The speed of change is increasing exponentially with global communication becoming instantaneous.”</p>		

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category “Innovation”, sub-category “Modernisation”, in which the specific dimensions can be measured on a low level to a high level of manifestation axis.

**Table 7.13: Dimensions of the category “Hyper-Speed”**

<b>Category</b>	<b>Sub-category</b>	<b>Specific dimension</b>
Innovation	Modernisation	Low level of manifestation – High level of manifestation

Source: Coded based on Kuckartz, 2014:25.

**Table 7.14: Driving Force 7 (first-round pilot Delphi)**

<b>Driving Force 7</b>	“Non-state actors increasing their influence on international politics but especially related to national security.”		
<b>Collective Likert</b>	6	<b>Collective Likert</b>	7.5

score (current significance)	score (futures relevancy)
<b>Comments from panel members</b>	<p>“Same challenges of complexity confront non-state actors. Especially where non-state actors are proxies for main role-players in information warfare.</p> <p>While it cannot be disputed, trends also point to the continued survival of the nation state and information warfare (I could argue) would be primarily contested by states, not other entities.</p> <p>Probably not only in politics.</p> <p>The character and role of those in power will definitely adapt and change in the future.</p> <p>The phenomena of non-state actors is overstated. It is an influential but not determining factor in international politics.”</p>
<b>Evaluation</b>	<p>Although states remain the most important actors in the global system, non-state actors in today’s world have increasing influence and power in international relations (Joey, 2011:4). The increasing influence of these actors over the past decades indicates that it remains likely that this will continue. Although it might be true that in some cases the influence of these actors might be overstated, it can be expected that their future influence cannot be discounted – as supported by the views of most panel members.</p>
<b>Decision on formulation of Driving Force 7</b>	<p>Keep formulation:</p> <p>“Non-state actors increasing their influence on international politics but especially related to national security.”</p>

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category “Networked”, sub-category “Complexity”, in which the specific dimensions can be measured on a low level of manifestation to a high level of manifestation axis.

**Table 7.15: Dimensions of the category “Rise of the Non-State Actor”**

Category	Sub-category	Specific dimension

Networked	Complexity	Low Level of manifestation – High level of manifestation
-----------	------------	---

Source: Coded based on Kuckartz, 2014:25.

**Table 7.16: Driving Force 8 (first-round pilot Delphi)**

<b>Driving Force 8</b>	“Global inequality in terms of economic, social and technological access continues to be a major global challenge.”		
<b>Collective Likert score (current significance)</b>	6.7	<b>Collective Likert score (futures relevancy)</b>	7.4 (second highest)
<b>Comments from panel members</b>	<p>“The inequality of access will decrease.</p> <p>Those who cannot keep up will become the “victims” of information warfare.</p> <p>This will be key.</p> <p>Global inequality will grow as resources get scarce in the future.</p> <p>As we see the emergence of the so-called Third World and the shift of global centre of power this challenge will diminish.”</p>		
<b>Evaluation</b>	<p>Although most panel members agreed that inequality is significant and will continue to grow, some dissenting views indicated that it might decrease. In terms of its futures relevancy it is indicated as the second most significant driving force. While it is true that around the world economic growth in many countries is positive, deep challenges remain, including poverty, environmental degradation, persistent unemployment, political instability, violence and conflict. These problems are often closely related to inequality (Mohammed, 2013).</p>		
<b>Decision on formulation of Driving Force 8</b>	<p>Keep formulation:</p> <p>“Global inequality in terms of economic, social and technological access continues to be a major global challenge.”</p>		

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category “Transformation”, sub-category “Global Inequality”, in which the specific dimensions can be measured on a low level of manifestation to a high level of manifestation axis.

**Table 7.17: Dimensions of the category “Global Inequality”**

Category	Sub-category	Specific dimension
Transformation	Global Inequality	High Level – Low Level

Source: Coded based on Kuckartz, 2014:25.

**Table 7.18: Driving Force 9 (first-round pilot Delphi)**

<b>Driving Force 9</b>	“ICT is embedding itself as a crucial part of society.”		
<b>Collective Likert score (current significance)</b>	7.7 (highest)	<b>Collective Likert score (futures relevancy)</b>	9.2 (second highest)
<b>Comments from panel members</b>	<p>“Mostly in the developed world within existing systems – the future manifestation of ICT in developing countries/societies not clear.</p> <p>I expect it to be absolute by 2030.</p> <p>ICT will determine national defence strength and vulnerabilities.”</p>		
<b>Evaluation</b>	This driving force has been regarded as highly significant by the panel members. The issue of the role of ICT in the developing world has also been raised.		
<b>Decision on formulation of Driving Force 9</b>	<p>Keep formulation:</p> <p>“ICT is embedding itself as a crucial part of society.”</p>		

Source: Round 1 of Delphi pilot study

Based on qualitative text analysis, this driving force falls in the category “Innovation”, sub-category “Addition”, in which the specific dimensions can be measured on a low level of manifestation to high level of manifestation axis

**Table 7.19: Dimensions of the category “Embedding of ICT”**

Category	Sub-category	Specific dimension
Innovation	Addition	Low level of manifestation – High level of manifestation

Source: Coded based on Kuckartz, 2014:25.

**Table 7.20: Driving Force 10 (first-round pilot Delphi)**

<b>Driving Force 10</b>	“Social media is a significant part of communication and this is expected to grow in the future.”		
<b>Collective Likert score (current significance)</b>	7.4	<b>Collective Likert score (futures relevancy)</b>	9.3 (highest)
<b>Comments from panel members</b>	<p>“This is a major national security threat.</p> <p>But what is social media used for? To scan for information or to socialise.</p> <p>It will be the dominant force by 2030.</p> <p>Social media is changing the entire society, i.e. interest groups which span traditional boundaries.”</p>		
<b>Evaluation</b>	In general, panel members regarded social media as a significant factor related to the manifestation of information warfare. The future significance in this regard is acknowledged with this driving force attaining the top position.		
<b>Decision on formulation of Driving Force 10</b>	<p>Keep formulation:</p> <p>“Social media is a significant part of communication and this is expected to grow in the future.”</p>		

Source: Round 1 of Delphi pilot study

Based on qualitative text analysis, this driving force falls in the category “Networked”, sub-category “System”, in which the specific dimensions can be measured on a low level of penetration to a high level of penetration axis.

**Table 7.21: Dimensions of the category “Rise of Social Media”**

Category	Sub-category	Specific dimension
Networked	System	Low level penetration – High level of penetration

Source: Coded based on Kuckartz, 2014:25.

**Table 7.22: Driving Force 11 (first-round pilot Delphi)**

<b>Driving Force 11</b>	“The threshold required to exploit the advantages of information technology is relatively low and decreasing rapidly as the recursive simplicity within the ICT sector, which supports a clear trend of ever-expanding growth in access, availability, and speed with a simultaneous reduction in cost and skill barriers.”		
<b>Collective Likert score (current significance)</b>	7	<b>Collective Likert score (futures relevancy)</b>	8.8
<b>Comments from panel members</b>	<p>“Very much so.</p> <p>Sentence is long and there are sections that one agrees with and others which can be disputed. I do not see the “recursive simplicity” within ICT sector nor the “reduction” in “skill barriers”.</p> <p>I do not think that we currently have the exposure to rate the extent to which we will use, be reliant on and be controlled by IT in the future. It will be a central part of everything we do.</p> <p>Continuous search for vulnerability to exploit weaknesses in systems and defence systems.</p> <p>This will illustrate fundamental difficulties in coming to terms with information warfare.</p> <p>It brought about a revolution in military affairs.</p> <p>True, however, this is true for the North but not so for the developing South, particularly Africa.”</p>		

<b>Evaluation</b>	The formulation of the driving force is too complex and needs to be formulated in a more direct manner. It is also controversial and remains uncertain if this is the case in especially the developing world. This needs to be investigated further as the Delphi study continues.
<b>Decision on formulation of Driving Force 11</b>	New formulation: "The threshold required to exploit the advantages of information technology is relatively low and decreasing rapidly."

Source: Round 1 of Delphi pilot study.

Based on qualitative text analysis, this driving force falls in the category "Innovation", sub-category "Modification", in which the specific dimensions can be measured on a low level of manifestation to a high level of manifestation axis.

**Table 7.23: Dimensions of the category "Decreasing Threshold"**

<b>Category</b>	<b>Sub-category</b>	<b>Specific dimension</b>
Innovation	Modification	High levels – Low levels

Source: Coded based on Kuckartz, 2014:25.

**Table 7.24: Additional driving forces as suggested by the pilot Delphi panel members**

<b>Panel members' responses to: Identify any additional driving forces which would be relevant in the context of the future manifestation of information warfare.</b>	<p>"The main ones listed here are correct.</p> <p>Internet governance? Global institutions to monitor and govern the internet?</p> <p>Traditional warfare is on the decline: The broad trend regarding traditional interstate warfare is on a decline. The reasons are complex but a key aspect is growing rational state behaviour based on strong historical evidence related to the devastating economic/human consequences of interstate wars, and in addition, a more mature and coordinated international system of conflict prevention and management. Interstate competition, however, is stronger than ever as resources continue to shrink, and as such information warfare increasingly becomes a handy alternative in relation to dealing with and managing adversaries.</p> <p>Within the context of the short timeframe to 2030 not much can be added,</p>
---	--

	however, I would have loved to include a “singularity event” (especially by 2048) into the equation as a driving force. The forecasted “singularity” of 2048 will impact information warfare dramatically because it would be “uncontrollable”.
<b>Evaluation</b>	<p>Driving Force 4 is replaced by a driving force formulated as: “Information warfare will become an easy alternative and safe option for power projection.”</p> <p>Another noteworthy suggestion in terms of identifying driving forces is the issue of a Black Swan<sup>27</sup> related event such as a “singularity event” (especially by 2048) added to the equation as a driving force. The forecasted “singularity of 2048” will impact information warfare dramatically because it would be “uncontrollable”.</p> <p>The idea of a Black Swan event will be relevant in terms of the approach to building the future scenarios.</p>

All eleven driving forces were measured against two dimensions by the Delphi panel members. The driving forces were firstly measured in terms of their current significance. Driving Force 9 (“ICT is embedding itself as a crucial part of society.”) with an average score of 7.7 is the highest. The second highest average score of 7.4 is for Driving Force 6 (“The speed of change is increasing exponentially with global communication becoming instantaneous.”) and Driving Force 10 (“Social media is a significant part of communication and this is expected to grow in the future.”).

Measured against its futures relevancy (2030s), Driving Force 6 (“The speed of change is increasing exponentially with global communication becoming instantaneous.”) and Driving Force 10 (“Social media is a significant part of communication and this is expected to grow in the future.”) with average scores of 9.3 are the highest. The second highest is Driving Force 9 (“ICT is embedding itself as a crucial part of society.”) with an average score of 9.2.

#### **7.6.6 Evaluation of Delphi study pilot Round 2**

Individual questionnaires based on the feedback provided were prepared for all the participants. The individual Likert score as well as the aggregate Likert score are provided for each driving force. The panel members’ own comments, if any, are also provided as well as the comments of all other participants with the aim to provide more insight into the interpretation of all the driving forces. (See Appendix D, Table D:1 for an example of a Round 2 questionnaire.)

---

<sup>27</sup> Taleb (2007:xvii-xviii) described a Black Swan as an event with the following three attributes. “First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme

The cover letter for the second-round Delphi (See Appendix E, Table E:1 for letter) covered the following: Panel members were thanked for participating in the first round of the Delphi study aimed at identifying the most significant contemporary driving forces which will impact the manifestation of information warfare by the 2030s. Feedback and ratings have been received from all panel members. Based on these some changes were made to the formulation of the driving forces. The panel members' responses to the first-round questionnaire are included for easy reference. The average score for each dimension is listed as well as the score the panel member provided. The letter indicated that it would be appreciated if the panel member could again consider each driving force and make a judgement on the score the member provided in the context of the collective average Likert score of the Delphi group as a whole. The comments from the other Delphi participants are also included in the questionnaire. The panel member is told that his or her rating can stay the same or move closer or further away from the average rating. Any additional comments will also be appreciated. Eight panel members out of 10 returned the completed questionnaire in the second round of the pilot Delphi survey.

**Table 7.25: Evaluation of Driving Force 1 (second-round Delphi pilot)**

<b>Driving Force 1</b>	"The centre of power is shifting from the traditional developed countries to the developing countries."					
<b>Collective Likert score (current significance)</b>	5.1	<b>Collective Likert score (Round 1)</b>	6.3	<b>Collective Likert score change</b>	-1.2	
<b>Collective Likert score (futures relevancy)</b>	6.1	<b>Collective Likert score (Round 1)</b>	7.2	<b>Collective Likert score change</b>	-1.1	
<b>Additional comments from panel members</b>	<p>"I prefer the formulation used in Round 1 it is more accurate.</p> <p>Maybe the centre of power is shifting from traditional developing countries but who constitute the latter group of developing countries. This is also constantly shifting.</p> <p>Developed countries are actively seeking ways to dominate drivers of the new Information Age."</p>					
<b>Evaluation</b>	The original formulation of the fist driving force was: "Globally the centre of power is shifting, enhancing the political, social and					

	<p>economic influence of individuals and sub-state entities in the world.” The formulation was changed because it included an element already incorporated in Driving Force 7 which is referring to the role of sub-state entities. Therefore, although the previous formulated driving force might be more comprehensive for the purpose of differentiating between the power shift and sub-state entities, the current formulation is maintained. It is also acknowledged that this shifting power trend remains highly dynamic and constantly changing in terms of actors. For this reason, this driving force should remain strategic in focus.</p>
<b>Decision on final formulation of Driving Force 1</b>	<p>Keep formulation:          “The centre of power is shifting from the traditional developed countries to the developing countries.”</p>

Source: Round 2 of Delphi pilot study.

**Table 7.26: Evaluation of Driving Force 2 (second-round Delphi pilot)**

<b>Driving Force 2</b>	“Security in a networked environment will increase in complexity as its physical and non-physical elements increase.”					
<b>Collective Likert score (current significance)</b>	5.4	<b>Collective Likert score (Round 1)</b>	6.7	<b>Collective Likert score change</b>	-1.3	
<b>Collective Likert score (futures relevancy)</b>	6.4	<b>Collective Likert score (Round 1)</b>	8.2	<b>Collective Likert score change</b>	-1.8	
<b>Additional comments from panel members</b>	<p>“Maybe more accurate to say ... ‘physical and non-physical elements become more tightly interwoven’.</p> <p>The reformulation has changed the meaning of the question. In the first formulation the focus was on complexity. Now the focus is on networked.</p> <p>Due to networked character cyber threat to increase.”</p>					
<b>Evaluation</b>	The original formulation of Driving Force 2 was: “Security is increasingly becoming a more encompassing, globally influenced and networked phenomenon.” Although there was					

	indeed a shift of focus in the first formulation of the second version in terms of the network aspect, it did not fundamentally change the meaning of the driving force. The collective Likert score change for the second round is also in line with the changes in the other driving forces. The suggestion of a slight reformulation will, however, add value in explaining the driving force more accurately.
<b>Decision on final formulation of Driving Force 2</b>	Minor reformulation as suggested: “Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.”

Source: Round 2 of Delphi pilot study.

**Table 7.27: Evaluation of Driving Force 3 (second-round Delphi pilot)**

<b>Driving Force 3</b>	“Systemic stresses from clashing centripetal and centrifugal forces will increase exponentially.”					
<b>Collective Likert score (current significance)</b>	4.9	<b>Collective Likert score (Round 1)</b>	6.4	<b>Collective Likert score change</b>	-1.5	
<b>Collective Likert score (futures relevancy)</b>	6.5	<b>Collective Likert score (Round 1)</b>	8.6	<b>Collective Likert score change</b>	-2.1	
<b>Additional comments from panel members</b>	“Equilibrium between the two forces will keep the system stresses constant and there will not be an exponential increase of any significance.”					
<b>Evaluation</b>	It is not necessarily the case that clashing centripetal and centrifugal forces will keep the system stresses constant. These types of clashes could have significant but unquantifiable consequences regarding information warfare. However, the new formulation did result in the highest decrease (with Driving Force 6) in its collective Likert score in terms of its futures relevancy by panel members. This is a driving force that needs to be					

	highlighted for further investigation in the next Delphi study.
<b>Decision on final formulation of Driving Force 2</b>	Keep formulation provisionally: “Systemic stresses from clashing centripetal and centrifugal forces will increase exponentially.”

Source: Round 2 of Delphi pilot study.

**Table 7.28: Evaluation of Driving Force 4 (second-round Delphi pilot)**

<b>Driving Force 4</b>	“Information warfare will become an easy alternative and safe option for power projection.”				
<b>Collective Likert score (current significance)</b>	5	<b>Collective Likert score (Round 1)</b>	n/a	<b>Collective Likert score change</b>	None
<b>Collective Likert score (futures relevancy)</b>	6.3	<b>Collective Likert score (Round 1)</b>	n/a	<b>Collective Likert score change</b>	None
<b>Additional comments from panel members</b>	<p>“Yes, currently it is easier and safer but complexity of information warfare will increase and make it more difficult and dangerous to project such power.</p> <p>Agree fully with it becoming an alternative option for power projection. May not necessarily be an easier option (requires a set of skills). ‘Safer’ is also debatable. More safe than nuclear weapons but still exposes a country to a huge risk (especially in the current techno-dominant society).</p> <p>Suggestion: ‘easy alternative and safe option’ should rather be ‘of growing importance’ because information warfare will be built in among others.”</p>				
<b>Evaluation</b>	Feedback indicated that information warfare could be regarded as a growing option for power projection. However, the descriptions “easier option” and “safer” are more controversial. The suggestion to rather refer to the growing importance of information warfare as an alternative option for power will enhance the gist of the driving force.				
<b>Decision on final formulation of Driving</b>	Minor reformulation as suggested: “Information warfare will become a growing option for power projection.”				

<b>Force 4</b>	
----------------	--

Source: Round 2 of Delphi pilot study.

**Table 7.29: Evaluation of Driving Force 5 (second-round Delphi pilot)**

<b>Driving Force 5</b>	<p>“Symbolic, information-related phenomena are increasingly impacting behaviour.</p> <p>Symbolic refers to representations (in the media and social media) which reflect perceived reality.”</p>				
<b>Collective Likert score (current significance)</b>	5.2	<b>Collective Likert score (Round 1)</b>	6.2	<b>Collective Likert score change</b>	-1
<b>Collective Likert score (futures relevancy)</b>	5.9	<b>Collective Likert score (Round 1)</b>	7.3	<b>Collective Likert score change</b>	-1.4
<b>Additional comments from panel members</b>	<p>“Clarification of ‘symbolic’ helps and invalidates some of the comments (from Round 1). The clarification also reaffirms my initial score.</p> <p>The Islamic State (IS) is successfully using psychological warfare to radicalise societies. This trend is likely to increase over time.</p> <p>Social media activities of IS and hacking of the USA Military’s Central Command (CENTCOM).”</p>				
<b>Evaluation</b>	<p>The description of symbolic assisted to clear some concerns expressed during Round 1 regarding this driving force.</p>				
<b>Decision on final formulation of Driving Force 5</b>	<p>Keep formulation:</p> <p>“Symbolic, information-related phenomena are increasingly impacting behaviour.</p> <p>Symbolic refers to representations (in the media and social media) which reflect perceived reality.”</p>				

Source: Round 2 of Delphi pilot study.

**Table 7.30: Evaluation of Driving Force 6 (second-round Delphi pilot)**

<b>Driving Force 6</b>	“The speed of change is increasing exponentially with global
------------------------	--

	communication becoming instantaneous.”					
<b>Collective Likert score (current significance)</b>	6 (second highest)	<b>Collective Likert score (Round 1)</b>	7.4	<b>Collective Likert score change</b>	-1.4	
<b>Collective Likert score (futures relevancy)</b>	7.2 (second highest)	<b>Collective Likert score (Round 1)</b>	9.3	<b>Collective Likert score change</b>	-2.1	
<b>Additional comments from panel members</b>	None					
<b>Evaluation</b>	This driving force is regarded as the second most significant driving force in terms of its current as well as future importance. In terms of its futures relevancy it did receive the highest decrease (with Driving Force 6) in its collective Likert score.					
<b>Decision on final formulation of Driving Force 6</b>	Keep formulation: “The speed of change is increasing exponentially with global communication becoming instantaneous.”					

Source: Round 2 of Delphi pilot study.

**Table 7.31: Evaluation of Driving Force 7 (second-round Delphi pilot)**

<b>Driving Force 7</b>	“Non-state actors increasing their influence on international politics but especially related to national security.”					
<b>Collective Likert score (current significance)</b>	5.1	<b>Collective Likert score (Round 1)</b>	6	<b>Collective Likert score change</b>	-0.9	
<b>Collective Likert score (futures relevancy)</b>	6.2	<b>Collective Likert score (Round 1)</b>	7.5	<b>Collective Likert score change</b>	-1.3	
<b>Additional comments</b>	“Non-state actors’ access to the means of information warfare makes					

<b>from panel members</b>	them influential, and will be more so in the future as access to better technology empowers them.  The Islamic State's utilisation of technology."
<b>Evaluation</b>	The role of non-state actors in information warfare is acknowledged by panel members. Contemporary uses of information warfare by non-state actors are mentioned.
<b>Decision on final formulation of Driving Force 7</b>	Keep formulation:  "Non-state actors increasing their influence on international politics but especially related to national security."

Source: Round 2 of Delphi pilot study.

**Table 7.32: Evaluation of Driving Force 8 (second-round Delphi pilot)**

<b>Driving Force 8</b>	"Global inequality in terms of economic, social and technological access continues to be a major global challenge."					
<b>Collective Likert score (current significance)</b>	4.9	<b>Collective Likert score (Round 1)</b>	6.7	<b>Collective Likert score change</b>	-1.8	
<b>Collective Likert score (futures relevancy)</b>	5.8	<b>Collective Likert score (Round 1)</b>	7.4	<b>Collective Likert score change</b>	-1.6	
<b>Additional comments from panel members</b>	None					
<b>Evaluation</b>	No consenting views on the relevance of inequality were expressed by panel members.					
<b>Decision on final formulation of Driving Force 8</b>	Keep formulation:  "Global inequality in terms of economic, social and technological access continues to be a major global challenge."					

Source: Round 2 of Delphi pilot study.

**Table 7.33: Evaluation of Driving Force 9 (second-round Delphi pilot)**

<b>Driving Force 9</b>	“Information communication technology (ICT) is embedding itself as a crucial part of society.”					
<b>Collective Likert score (current significance)</b>	6.1 (highest)	<b>Collective Likert score (Round 1)</b>	7.7	<b>Collective Likert score change</b>	-1.6	
<b>Collective Likert score (futures relevancy)</b>	7.4 (highest)	<b>Collective Likert score (Round 1)</b>	9.2	<b>Collective Likert score change</b>	-1.8	
<b>Additional comments from panel members</b>	Counter measures, collective action and multi-lateral structures will play a crucial role to strengthen defence.					
<b>Evaluation</b>	This driving force has been regarded as the most significant driving force by the panel members, both in terms of its current significance and its futures relevance. A global regulatory framework is required urgently; otherwise the weak and poor will either be excluded or exploited.					
<b>Decision on final formulation of Driving Force 9</b>	Keep formulation: “Information communication technology (ICT) is embedding itself as a crucial part of society.”					

Source: Round 2 of Delphi pilot study.

**Table 7.34: Evaluation of Driving Force 10 (second-round Delphi pilot)**

<b>Driving Force 10</b>	“Social media is a significant part of communication and this is expected to grow in the future.”					
<b>Collective Likert score (current significance)</b>	6 (highest)	<b>Collective Likert score (Round 1)</b>	7.4	<b>Collective Likert score change</b>	-1.4	

<b>Collective Likert score (futures relevancy)</b>	7.4 (highest)	<b>Collective Likert score (Round 1)</b>	9.2	<b>Collective Likert score change</b>	-1.8
<b>Additional comments from panel members</b>	<p>“Can be a tool for information warfare. Will unite the driving forces mentioned in two, three and four.”</p>				
<b>Evaluation</b>	<p>The use of social media for information warfare purposes can manifest in many formats. The futures relevancy of social media is especially regarded as a significant information warfare driving force.</p>				
<b>Decision on final formulation of Driving Force 10</b>	<p>Keep formulation: “Social media is a significant part of communication and this is expected to grow in the future.”</p>				

Source: Round 2 of Delphi pilot study.

**Table 7.35: Evaluation of Driving Force 11 (second-round Delphi pilot)**

<b>Driving Force 11</b>	“The threshold required to exploit the advantages of information technology is relatively low and decreasing rapidly.”				
<b>Collective Likert score (current significance)</b>	5.6	<b>Collective Likert score (Round 1)</b>	7	<b>Collective Likert score change</b>	-1.4
<b>Collective Likert score (futures relevancy)</b>	6.8	<b>Collective Likert score (Round 1)</b>	8	<b>Collective Likert score change</b>	-1.2
<b>Additional comments from panel members</b>	<p>“New formulation is debatable and ties in with the point on global inequality. This point is true for developed and not developing countries.”</p>				
<b>Evaluation</b>	<p>The formulation of the driving force increasingly seems to be relevant in developed countries but not necessarily in developing countries. Although user-friendly software could be deployed by relatively unskilled individuals for purposes of information warfare, the high-level development and applications are definitely restricted to high-skill and advanced training levels. The veracity of the driving force as currently</p>				

	formulated is suspect. Driving Force 8 does cover the implications of global inequality.
<b>Decision on final formulation of Driving Force 11</b>	Remove this driving force from the next Delphi study.

Source: Round 2 of Delphi pilot study.

**Table 7.36: Additional comments by the pilot Delphi panel members for Round 2**

<b>Panel members' responses to: Identify any additional driving forces which would be relevant in the context of the future manifestation of information warfare.</b>	<p>"Information warfare is just another type of 'traditional' warfare. The destruction to civilisation could even be worse, even though the human suffering might not be as gruesome as in the past, the suffering will be more long term and continuous.</p> <p>I disagree that traditional warfare is on the decline. Especially intra-state warfare. Consider current examples of the Ukraine, Libya, Sudan and the Central African Republic.</p> <p>Question the notion that traditional warfare is on the decline. There are a growing number of conflicts in the developing world."</p>
<b>Evaluation</b>	<p>No specific proposals were made for additional driving forces. The arguments against the notion of the decline of conflict are not correct when a long-term view is taken on the frequency of conflict in the world. Although conflict continues, the world is currently much more peaceful than in the past. Statistics reveal dramatic reductions in conflict deaths, racism, rape and murder. The number of people killed in battle, calculated per 100 000 of the population, has dropped 1000-fold over the centuries as civilisation has evolved (Pinker, 2011:53).</p>

Source: Round 2 of Delphi pilot study.

During Round 2 of the pilot Delphi study eleven driving forces were measured against two dimensions by the Delphi panel members, namely against their current significance and against their futures relevancy. Driving Force 9 ("ICT is embedding itself as a crucial part of society.") with an average score of 6.1 was the highest. The second highest average score of 6 was for Driving Force 6 ("The speed of change is increasing exponentially with global communication becoming instantaneous.") and Driving Force 10 ("Social media is a significant part of communication and this is expected to grow in the future."). This was consistent with Round 1 of the pilot Delphi study.

Measured against its futures relevancy (2030s), Driving Force 9 (“ICT is embedding itself as a crucial part of society.”) and Driving Force 10 (“Social media is a significant part of communication and this is expected to grow in the future.”) with an average score of 7.4 were the highest. The second highest was Driving Force 6 (“The speed of change is increasing exponentially with global communication becoming instantaneous.”) with an average score of 7.2. This reflected a slight change from Round 1 in the positions of driving forces with Driving Force 6 and Driving Force 9 switching positions. (See Appendix F and Appendix G for the pilot Delphi study’s score sheets.)

The average scores on all driving forces were revealed to all participants. Collectively, the participants moderated their scores on all the driving forces on both the current and futures dimensions. With the panel design focusing on South African national security experts, it is easier to attain consensus because the panel members were deliberately selected for their homogeneity in professional focus (Okoli & Pawlowski, 2004:25). In general, no significant changes were made in terms of the individual prioritisation (except for moderating scores). However, the group did move towards stability and consensus.

It is necessary to distinguish between the two concepts “consensus/agreement” and “stability” in Delphi studies. Consensus measurement should be considered a valuable component of data analysis and interpretation in Delphi research. In most Delphi studies, “... consensus is assumed to have been achieved when a certain percentage of the votes fall within a prescribed range – for example, when the interquartile range (IQR) is no larger than two units on a ten-unit scale” (Scheibe, Skutsch & Schofer, 1975:271). In descriptive statistics, the IQR, also called the midspread or middle fifty, is a measure of statistical dispersion, being equal to the difference between the upper and lower quartiles (Upton & Cook, 1996:55). Consensus has been achieved in Round 2 of the pilot Delphi study.

However, Dajani, Sincoff and Talley (1979:83) stated that consensus is meaningless if group stability has not been reached beforehand; group stability is thus considered the necessary criterion. Stability is defined as “the consistency of responses between successive rounds of a study” (Dajani, Sincoff & Talle, 1979:84). In the case of stability, the results of two different Delphi rounds are not statistically different for a certain projection (Von der Gracht, 2012:1527). The model did assist to provide reasonably accurate driving forces with only one driving force change and one removed as result of feedback from the Delphi panel. A third round would not be necessary as consensus and stability within the pilot Delphi study has been reached.

## **7.7 SECOND DELPHI STUDY**

### **7.7.1 Aim of the second Delphi study**

In the pilot study, the Delphi questionnaire was tested and expert assistance was used to modify the top ten driving forces determining the manifestation of information warfare futures in South Africa in the 2030s. However, as information warfare is a global phenomenon transcending

national borders, a second Delphi study was undertaken making use of an expert panel of domestic and international panel members from the broader environment impacting on information warfare. The second Delphi panel aimed to provide additional insights into the future manifestation of information warfare as a national security threat. Additionally, the priority driving forces were refined to serve as the driving forces determining information warfare futures in South Africa for the 2030s.

### 7.7.2 Focus of the second Delphi study

The pilot study used expertise in the South African security field as focal point for all relevant environments in which information warfare manifests. The second Delphi study focused more strategically on domestic and international experts knowledgeable about one or more of the Technological, War/Conflict, Economical, Political and Social (TWEPS) macro environments.

### 7.7.3 Participants in the second Delphi study

A group of 21 individuals was approached to take part in the second Delphi study. Eleven agreed to participation, representing expertise in all the TWEPS macro environments. (See Table 7.37 for list of participants.) The participants included a wide variety of individuals working in TWEPS macro environments, all with tertiary qualifications. Two individuals worked in the cyber-security environment; the others in one or more TWEPS-related environments.

**Table 7.37: List of participants in the second Delphi study**

<b>Panel member</b>	<b>Expertise</b>	<b>TWEPS coverage</b>
Panellist 01	South African business process consultant and expert. Thirty years of business experience. Expert in strategic management. Master's degree in Futures Studies.	Economic environment
Panellist 02	South African high-level technical expert in information management and IT field. Master's degree in Futures Studies.	Technological environment
Panellist 03	Prominent Singapore professional futurist. Ten years of experience in social and urban development projects.	Social environment
Panellist 05	British management expert with law enforcement background, PhD candidate.	War/conflict environment

Panellist 06	Canadian ICT expert. PhD candidate.	Technological environment
Panellist 14	American computer security specialist. PhD candidate	Technological environment
Panellist 15	South African academic, international relations. PhD in International Relations.	Political environment
Panellist 16	Zimbabwean financial expert. PhD in Business Administration.	Economic and social environment
Panellist 17	Russian ICT security expert.	Technological environment
Panellist 18	Senior South African diplomat.	Political environment
Panellist 19	Senior South African diplomat.	Political environment

Source: Own compilation based on matrix framework suggested by Gordon (1994:6).

Despite identifying a more representative group of individuals representing all TWEPS macro environments, the participating group had overrepresented the technological environment and underrepresented the war and conflict environment. This does not represent a challenge to the validity of the study as the aim of the second Delphi study was "...to provide additional insights into the future manifestation of information warfare as a national security threat." The pilot Delphi was the "... the primary contributor to the content and identification of the driving forces relevant to the South African future information warfare scenarios."

Round 1 of the second Delphi study was conducted from 3 February to 11 August 2015. Requests for participation were forwarded to 21 individuals of which 11 agreed to participate. The second round was conducted from 3 September to 23 September 2015. Questionnaires were distributed to 11 participants and responses were received from nine participants.

#### 7.7.4 Questionnaire

The questionnaire has been developed and refined during Round 1 and Round 2 of the pilot Delphi study. As with the pilot study, the second Delphi panel members were requested to measure each driving force first against its current significance and then against its futures relevancy (2030s). Again, a 10-point Likert scale was used, where 1 coded the least feasible/desirable constituent and 10 for the most feasible/desirable driving force. When responding to the Likert questionnaire items, respondents were required to specify their level of agreement or disagreement on a symmetric agree-disagree scale for the series of the ten identified driving forces.

### 7.7.5 Evaluation of the second Delphi study Round 1

The process followed in the pilot Delphi study was replicated in the first-round questionnaire of the second Delphi study. The evaluation of the individual driving forces are presented in table format. See Table 7.38 to Table 7.59 for an evaluation of the driving forces in Round 1 and Round 2.

**Table 7.38: Evaluation of Driving Force 1 (first-round second Delphi)**

<b>Driving Force 1</b>	“The centre of power is shifting from the traditional developed countries to the developing countries.”		
<b>Collective Likert score (current significance)</b>	5.5	<b>Collective Likert score (futures relevancy)</b>	6.8
<b>Comments from panel members</b>	<p>“Yes. But I think we’re in the very early stages of this shift and, if that is so, then the tensions between the two worlds could be high as the developing tries to assert power it does not yet have and the other finds it increasingly difficult to exert yesteryear influence. However, 2030 may be too close for this to be a very important factor.</p> <p>Only some developing countries - in mainly Asia - have and will have the necessary technological advances currently and in the near future.</p> <p>The definition of power is unclear here. Moreover, the statement contains a state-centric bias.”</p>		
<b>Evaluation</b>	<p>Realists postulated that any political unit (such as a state) will act in such a way as to maximise its power, which is defined mainly in terms of the security of its territory (Edwards, 1969:69). Political power can be seen as a psychological relationship between those who exercise it and those over whom it is exercised. Those who exercise power gain control by actions which have an impact on the minds of those over whom it is exercised. The impact derives from three sources, according to Morgenthau (1973:28), namely “the expectation of benefits, the fear of disadvantages, and the respect or love for men and institutions”. Power may be exerted through orders, threats, the authority or charisma of a person or of an office, or a combination of any of these. Nye (2011:xv) stated “...that two great power shifts are occurring in this century: a power transition among states and a power diffusion away from all states to nonstate (sic) actors”.</p>		

<b>Decision on formulation of Driving Force 1</b>	Keep formulation: “The centre of power is shifting from the traditional developed countries to the developing countries.”
---	--

Source: Round 1 of second Delphi study.

**Table 7.39: Evaluation of Driving Force 2 (first-round second Delphi)**

<b>Driving Force 2</b>	“Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.”		
<b>Collective Likert score (current significance)</b>	6.5	<b>Collective Likert score (futures relevancy)</b>	8.9
<b>Comments from panel members</b>	“I think that this cannot be seriously challenged. The complexity of the networked world presents opportunities for criminals and other ne'er-do-wells. In the absence of a cataclysm, this will increase and offer even more opportunities.  The definition of security is unclear here.”		
<b>Evaluation</b>	Understanding of security to be included as suggested by one panel member.		
<b>Decision on formulation of Driving Force 2</b>	Keep formulation: “Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.  Security refers to being protected or safe from harm.”		

Source: Round 1 of second Delphi study.

**Table 7.40: Evaluation of Driving Force 3 (first-round second Delphi)**

<b>Driving Force 3</b>	“Systemic stresses from clashing centripetal and centrifugal forces will increase exponentially.”		
<b>Collective Likert score (current significance)</b>	5.2	<b>Collective Likert score (futures relevancy)</b>	6.8

<b>Comments from panel members</b>	<p>“Include a definition of ‘centripetal’ and ‘centrifugal’ forces. I interpreted it as opposing forces.</p> <p>I was slightly unclear about this point but I think I understand it. The convergence in some matters seems to be counterbalanced by a balkanisation. On the principle that IW gives power to smaller players with a grievance – I see this point as similar to 4, 7 and 11.</p> <p>Do not really understand the question.</p> <p>I am unsure what these centripetal/centrifugal forces are.</p> <p>The definition of forces is unclear here.</p> <p>This could be constant over time, i.e. the ever-present forces of change – so I wouldn’t regard it as a peculiar driving force.</p> <p>Question is somewhat confusing and 5 is therefore given for both.”</p>
<b>Evaluation</b>	Feedback strongly indicates that the formulation of this driving force is not sufficiently clear.
<b>Decision on formulation of Driving Force 3</b>	<p>Reformulation based on comments received.</p> <p>“An increase in integration and polarisation will contribute to systemic stresses.”</p>

Source: Round 1 of second Delphi study.

**Table 7.41: Driving Force 4 (first-round second Delphi)**

<b>Driving Force 4</b>	“Information warfare will become a growing option for power projection.”		
<b>Collective Likert score (current significance)</b>	6.5	<b>Collective Likert score (futures relevancy)</b>	8.9
<b>Comments from panel members</b>	<p>“I think that this is the most powerful driver of its increase today but I believe that countermeasures will mature and in due course, other things will finally supplant it.</p> <p>Reference to information – rather than cyber – warfare is unclear.”</p>		
<b>Evaluation</b>	Disagree with remark that driving force should refer to cyber warfare and not information warfare. Information warfare is a more encompassing term than cyber warfare which is a constituent element thereof. The		

	definition proposed for information warfare encompasses three forms of manifestation of information warfare, namely netwar, psychological warfare and cyber warfare.
<b>Decision on formulation of Driving Force 4</b>	Keep formulation: “Information warfare will become a growing option for power projection.”

Source: Round 1 of second Delphi study.

**Table 7.42: Driving Force 5 (first-round second Delphi)**

<b>Driving Force 5</b>	<p>“Symbolic, information-related phenomena are increasingly impacting behaviour.</p> <p>Symbolic refers to representations (in the media and social media) which reflect perceived reality.”</p>		
<b>Collective Likert score (current significance)</b>	6.4	<b>Collective Likert score (futures relevancy)</b>	8
<b>Comments from panel members</b>	<p>“This is more subtle and a fascinating point which possibly could be the subject of a PhD on its own. I think that there can be no contest that the point is true and it is seen in recent ISIS-related matters (and I am sure lots of other things).</p> <p>Do not really think it is important.</p> <p>I’m unsure what behaviour refers to here. Behaviour of the general public?</p> <p>Venturing into the realm of symbolism requires elaboration on the importance of political rituals.”</p>		
<b>Evaluation</b>	<p>Behaviour refers to the way in which people conduct themselves with reference to others and the world in general. Society has increasingly moved from being dominated by the “mode of production” to one controlled by the “code of production”. The objective has shifted from exploitation and profit to domination by the signs and systems that produce them (Ritzer &amp; Goodman, 2004:607-608). The symbolic is integrated into the conduct and utilisation of information war.</p>		

<b>Decision on formulation of Driving Force 5</b>	<p>Keep formulation:</p> <p>“Symbolic, information-related phenomena are increasingly impacting behaviour.</p> <p>Symbolic refers to representations (in the media and social media) which reflect perceived reality.”</p>
---	--

Source: Round 1 of second Delphi study.

**Table 7.43: Driving Force 6 (first-round second Delphi)**

<b>Driving Force 6</b>	“The speed of change is increasing exponentially with global communication becoming instantaneous.”		
<b>Collective Likert score (current significance)</b>	6.5	<b>Collective Likert score (futures relevancy)</b>	8.6
<b>Comments from panel members</b>	<p>“Security vulnerability discovery (as a main driving force behind cyber attacks) isn’t so much a factor of the speed of communication, but the integrity of software.</p> <p>Change is not defined here.”</p>		
<b>Evaluation</b>	<p>The comment on “integrity of software” refers to the cyber aspect, while the definition of information warfare also addresses power-related influence on a cognitive continuum for which speed is a relevant issue.</p> <p>Change should be defined, as one panel member suggested.</p>		
<b>Decision on formulation of Driving Force 6</b>	<p>Keep formulation but add a definition of change:</p> <p>“The speed of change is increasing exponentially with global communication becoming instantaneous.</p> <p>Change refers to the act or process of transforming which results in a change in form, appearance, nature, or character.”</p>		

Source: Round 1 of second Delphi study.

**Table 7.44: Driving Force 7 (first-round second Delphi)**

<b>Driving Force 7</b>	“Non-state actors increasing their influence on international politics but especially related to national security.”		
<b>Collective Likert score (current significance)</b>	6.8	<b>Collective Likert score (futures relevancy)</b>	8.5
<b>Comments from panel members</b>	<p>“I saw some link between this point and number 4. Again, the recent events in Iraq come to mind. The USA government also because involved in the recent cyber attack on Sony.</p> <p>Does the statement assume that non-state actors are influential in international politics but not influential in international security?”</p>		
<b>Evaluation</b>	The focus should be on global/national security and this should be reflected in the formulation. Non-state actors are influential in both international politics and international security (Nye, 2011:xv). The focus in this study is more related to the security aspect.		
<b>Decision on formulation of Driving Force 7</b>	<p>Minor reformulation based on feedback received.</p> <p>“Non-state actors are increasing their influence related to global security.”</p>		

Source: Round 1 of second Delphi study.

**Table 7.45: Driving Force 8 (first-round second Delphi)**

<b>Driving Force 8</b>	“Global inequality in terms of economic, social and technological access continues to be a major global challenge.”		
<b>Collective Likert score (current significance)</b>	6.8	<b>Collective Likert score (futures relevancy)</b>	7.9
<b>Comments from panel members</b>	<p>“My problem with this was whether I thought global inequality was going to increase – not whether it was a driver.</p> <p>I think inequality will decrease.</p> <p>The difference in economic/social/technological gains as a</p>		

	<p>means of polarising nations may contribute to the increase of information warfare.</p> <p>Statement vague. Global inequality continues to be a major global challenge. But: the qualifier (“in terms of economic, social and technological access”) should be rephrased.</p> <p>Global and intra-regional inequality in terms of economic, social and technological access continues to be a major global challenge.”</p>
<b>Evaluation</b>	<p>Although inequality might decrease, this seems highly unlikely on the short to medium term as various current indicators confirm that global inequality remains a major problem (Ghosh, 2013). Thus, a driver reflecting the influence of inequality would be appropriate. Formulation suggestions by a panel member did enhance the meaning of the driver and were therefore accommodated in a reformulated driver.</p>
<b>Decision on formulation of Driving Force 8</b>	<p>Reformulation based on comments received:</p> <p>“Global and intra-regional inequalities are stimulating conflict potential.”</p>

Source: Round 1 of second Delphi study.

**Table 7.46: Driving Force 9 (first-round second Delphi)**

<b>Driving Force 9</b>	“Information communication technology (ICT) is embedding itself as a crucial part of society.”		
<b>Collective Likert score (current significance)</b>	8.1 (highest)	<b>Collective Likert score (futures relevancy)</b>	9.1 (highest)
<b>Comments from panel members</b>	<p>The present-day significance is that the shift is still ongoing, from isolation and separation to highly integrated global connections. Eventually, in the mid-term future, it will be a forgone expectation that everything is interconnected and integrated, like the roads we have to getting anywhere. As a subject, ICT as it gets enhanced and integrated, will become less of a concern, just as our road infrastructure which is crucial, but not something we</p>		

	<p>think about. Over time, advancements become trivialised and decline in importance as subjects of discourse.</p> <p>I think this is undeniable in the absence of some catastrophic change – but catastrophic change does sometimes happen.</p> <p>Increased ubiquity implies increased opportunity for IW.</p> <p>Not all technology is related to communication.</p>
<b>Evaluation</b>	<p>Collectively, this driving force has been scored the highest in terms of its current as well as futurist influence. Although the remark that not all technology is related to communication is true, the focus in this study remains on the communication aspect and influence of technologies. However, even technologies not previously associated with communication are being connected by the expected exponential rise of the Internet of Things (IoT) (McKendrick, 2015).</p>
<b>Decision on formulation of Driving Force 9</b>	<p>Keep formulation:</p> <p>“Information communication technology (ICT) is embedding itself as a crucial part of society.”</p>

Source: Round 1 of second Delphi study.

**Table 7.47: Driving Force 10 (first-round second Delphi)**

<b>Driving Force 10</b>	“Social media is a significant part of communication and this is expected to grow in the future.”		
<b>Collective Likert score (current significance)</b>	7.4 (second highest)	<b>Collective Likert score (futures relevancy)</b>	9 (second highest)
<b>Comments from panel members</b>	<p>“Also undeniable. 15-year-olds now will be 30 in 2030 and in positions of influence.</p> <p>I think social media has reached its peak.</p> <p>On a nation state conflict level, protection of classified information is prioritised over social media-related information.”</p>		
<b>Evaluation</b>	<p>Collectively, this driving force has been scored the second highest in terms of its current as well as futurist influence. Social</p>		

	media technologies have prompted radically new ways of interacting, with literally hundreds of different social media platforms created (Richard, Rohm & Crittenden, 2011:266).
<b>Decision on formulation of Driving Force 10</b>	Keep formulation: “Social media is a significant part of communication and this is expected to grow in the future.”

Source: Round 1 of second Delphi study.

**Table 7.48: Additional driving forces as suggested by the Delphi panel members**

<b>Panel members' response to: Identify any additional driving forces which would be relevant in the context of the future manifestation of information warfare.</b>	<p>The World Economic Forum identified a number of trends – such as hyper-connectivity – in its latest Risk Report. It also referred to cyber-security as one of the 10 main risks.</p> <p>Information can be defined as many things, including the commands and algorithms that drive machines. As the world progresses to a commerce-driven economy over the next few decades and we see mass automation where our cars and aeroplanes function autonomously, information warfare of the future will be about gaining access information to the machines, programmes and systems for the purpose of manipulation for sabotage; it is a real threat that if the road transportation system is hacked and hijacked in the future, the very vehicles that transport us and our inventory will become weapons used against us. That includes passenger planes. Network technology allows for the remote hijacking and abuse of machines. In a commerce model of business, sabotage means the disappearance of accounts, money and information critical to the continuation or recovery of business. Information warfare enables nations to cripple other nations without deploying a single soldier.</p> <p>Some of the above seem to be about asymmetric conflicts and terrorism without saying so. The possibility of non-governmental groups being terrorist groups focuses the mind. Is the world still moving away from divisions around ideology and towards divisions on culture? If so, this could be a driver. The embedded nature of IT is making us increasingly vulnerable, also to terrorism. Once upon a time terrorists could cause disruption and fear by means of bomb scares. Now they simply need to threaten a network.</p>
--	---

	<ul style="list-style-type: none"> <li>• Access to and production of basic human needs, such as water and food</li> <li>• Religious fanaticism</li> <li>• Cyber security</li> <li>• Energy (electricity) required to drive technology</li> <li>• Importance of rare earth metals and minerals as conductors</li> <li>• Chinese dominance of this market.</li> </ul>
<b>Evaluation</b>	<p>The inputs on the future manifestation of technology and terrorism are used in the formulation of scenarios in Chapter 8.</p> <p>The five suggested driving forces are tactical in nature and implicit in the already identified driving forces.</p>

The second Delphi panel members measured all ten driving forces against their current and future significance. Driving Force 9 (“ICT is embedding itself as a crucial part of society.”) with an average score of 8.1 was the highest. The second highest average score 7.4 was allocated to Driving Force 10 (“Social media is a significant part of communication and this is expected to grow in the future.”).

Measured against its futures relevancy (2030), Driving Force 6 (“The speed of change is increasing exponentially with global communication becoming instantaneous.”) and Driving Force 10 (“Social media is a significant part of communication and this is expected to grow in the future.”) with average scores of 9.3 were the highest. The second highest was Driving Force 9 (“ICT is embedding itself as a crucial part of society.”) with an average score of 9.2.

#### **7.7.6 Evaluation of the second Delphi study Round 2**

The second round of questionnaires was prepared according to the exact procedures used in the second round of the pilot Delphi study. The questionnaires were distributed to 11 panel members of which nine completed the questionnaires.

**Table 7.49: Evaluation of Driving Force 1 (second-round second Delphi)**

<b>Driving Force 1</b>	“The centre of power is shifting from the traditional developed countries to the developing countries.”
------------------------	---

<b>Collective score (current significance)</b>	<b>Likert (current)</b>	5	<b>Collective score (Round 1)</b>	<b>Likert (Round 1)</b>	5.5	<b>Collective score change</b>	<b>Likert change</b>	-0.5
<b>Collective score relevancy)</b>	<b>Likert (futures)</b>	6.7	<b>Collective score (Round 1)</b>	<b>Likert (Round 1)</b>	6.8	<b>Collective score change</b>	<b>Likert change</b>	-0.1
<b>Additional comments from panel members</b>	<p>"I think a shift in power is inevitable.</p> <p>I have adjusted my thinking just slightly in the light of the other interesting comments and certainly there is an interesting change in the last year which may challenge the thinking about 'countries'. The growth and influence of the Islamic State supports the ideas put forward in 'Clash of Civilisations' (Samuel P. Huntington) and might question the importance of countries in 2030.</p> <p>Given the current turmoil in the financial markets, and specifically the fact that developing countries' currencies have been hit particularly hard, I am of the opinion that it will take a very long time before power significantly shifts towards developing countries. Expectations were a bit inflated."</p>							
<b>Evaluation</b>	<p>Although it is acknowledged that the pace of this shift might differ depending on global events such as the global economic crisis of 2008 and China's stock exchange fall of 2015, the trend will continue. World Trade Organization (WTO) Director-General Lamy (2012) stated that "... the rising weight of influence of emerging economies has shifted the balance of power. This clearly implies a number of transitions to which we have not yet adjusted as classic Westphalia concepts of sovereignty are being challenged by the realities of interdependence."</p>							
<b>Decision on final formulation of Driving Force 1</b>	<p>Keep formulation:</p> <p>"The centre of power is shifting from the traditional developed countries to the developing countries."</p>							

Source: Round 2 of second Delphi study.

**Table 7.50: Evaluation of Driving Force 2 (second-round second Delphi)**

<b>Driving Force 2</b>	<p>“Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.</p> <p>Definition of security is included as suggested in previous round: Security refers to being protected or safe from harm.”</p>					
<b>Collective Likert score (current significance)</b>	6.7	<b>Collective Likert score (Round 1)</b>	6.5	<b>Collective Likert score change</b>	+0.2	
<b>Collective Likert score (futures relevancy)</b>	8.8	<b>Collective Likert score (Round 1)</b>	8.9	<b>Collective Likert score change</b>	-0.1	
<b>Additional comments from panel members</b>	<p>“The Internet of Things, in particular, will enable access to process control / automation / operational technologies which could cause all sorts of havoc.</p> <p>I have not moved my view here. States currently seem to have problems protecting themselves from cyber-attack. I have no doubt the technology will become more complex and the opportunities presented to those who wish to do harm will be clear.”</p>					
<b>Evaluation</b>	The significance of this driving force, especially in terms of its futures relevancy, is acknowledged by panel members.					
<b>Decision on final formulation of Driving Force 2</b>	<p>Keep formulation:</p> <p>“Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.</p> <p>Definition of security is included as suggested in previous round: Security refers to being protected or safe from harm.”</p>					

Source: Round 2 of second Delphi study.

**Table 7.51: Evaluation of Driving Force 3 (second-round second Delphi)**

<b>Driving Force 3</b>	“An increase in integration and polarisation will contribute to systemic stresses.”				
<b>Collective Likert score (current significance)</b>	4.6	<b>Collective Likert score (Round 1)</b>	5.2	<b>Collective Likert score change</b>	-1.4
<b>Collective Likert score (futures relevancy)</b>	6	<b>Collective Likert score (Round 1)</b>	6.8	<b>Collective Likert score change</b>	-0.8
<b>Additional comments from panel members</b>	<p>“The migrant crisis in Europe is an example of where too much integration (e.g. Schengen area) is causing tension.</p> <p>I have kept my position here for three reasons:</p> <ul style="list-style-type: none"> <li>• Polarisation appears to be increasing (see Q1) and add on trends in Russia and North Korea.</li> <li>• Aspects of integration are also increasing (see Q2).</li> <li>• So, opportunities and motivations are increasing.</li> </ul> <p>Possibly, I should increase my ‘future’ score to 9!</p> <p>Initially, my scores (for both) were quite far from the collective score. After consideration, I agree that the statement is more significant currently, but feel that it still warrants a higher score for “future relevancy”. We are currently witnessing attempts at integration (e.g. the African Union (AU) and its Regional Economic Communities (RECs); Shanghai Cooperation Organisation (SCO); the Trans-Pacific Partnership (TPP)), but non-state actors or groups are playing a much more significant role in causing polarisation. This trend in my opinion will accelerate during the coming decades due to cultural, religious and ideological reasons and which will subsequently lead to an increase in systemic stresses.”</p>				
<b>Evaluation</b>	During Round 1 some concerns were raised regarding the formulation of this driving force. Consensus now exists on the current formulation. Scores on this issue were slightly lower for both current and future relevancy.				

<b>Decision on final formulation of Driving Force 2</b>	Keep formulation: “An increase in integration and polarisation will contribute to systemic stresses.”
---	--

Source: Round 2 of second Delphi study.

**Table 7.52: Evaluation of Driving Force 4 (second-round second Delphi)**

<b>Driving Force 4</b>	“Information warfare will become a growing option for power projection.”					
<b>Collective Likert score (current significance)</b>	6.1	<b>Collective Likert score (Round 1)</b>	6.5	<b>Collective Likert score change</b>	-0.4	
<b>Collective Likert score (futures relevancy)</b>	8.8	<b>Collective Likert score (Round 1)</b>	8.9	<b>Collective Likert score change</b>	-0.1	
<b>Additional comments from panel members</b>	<p>“Improper use of AI alone is a major risk. In addition, the Internet of Things as mentioned above opens up systems. With larger populations, more serious competition for resources is inevitable. Organisations and countries will increasingly obtain competitive intelligence to understand competitors’ weak spots and to increase their chances to be the first mover.</p> <p>I still think this is the most important driver in relation to the opportunities it gives and the potential damage which can be caused. Developed countries now exist on the basis of their management of information – which is huge.”</p>					
<b>Evaluation</b>	The significance of this driving force, especially in terms of its futures relevancy, is acknowledged by panel members.					
<b>Decision on final formulation of Driving Force 4</b>	Keep formulation: “Information warfare will become a growing option for power projection.”					

Source: Round 2 of second Delphi study.

**Table 7.53: Evaluation of Driving Force 5 (second-round second Delphi)**

<b>Driving Force 5</b>	<p>“Symbolic, information-related phenomena are increasingly impacting behaviour.</p> <p>Symbolic refers to representations (in the media and social media) which reflect perceived reality.”</p>					
<b>Collective Likert score (current significance)</b>	7	<b>Collective Likert score (Round 1)</b>	6.4	<b>Collective Likert score change</b>	+0.6	
<b>Collective Likert score (futures relevancy)</b>	8.3	<b>Collective Likert score (Round 1)</b>	8	<b>Collective Likert score change</b>	+0.3	
<b>Additional comments from panel members</b>	<p>“Exactly how behaviour will change over the next 15 years is unclear. However, if you consider how behaviour has changed over the last 20 years since the WWW became generally available (e.g. social media, easy access to maps, making holiday bookings, online bullying, internet banking, Netflix, dating sites, online ordering), much more change in behaviour can be expected.</p> <p>I find the word ‘increasing’ here the difficult one to judge. This has always been true (consider the impact of flags in medieval battles, or just communities). Is the amount of information available today even more impactful (sic) on behaviour? Possibly. The world seems to be moving away from rationality and the scientific model which the enlightenment brought. Scary!</p> <p>Yes. I think we are seeing this with the Syrian refugee crisis.”</p>					
<b>Evaluation</b>	<p>The increasing impact of symbolic, information-related phenomena is directly related to the growing interconnectedness of the world. The opportunities for the symbolic to influence the world will escalate significantly in the future.</p>					
<b>Decision on final formulation of</b>	<p>Keep formulation:</p> <p>“Symbolic, information-related phenomena are increasingly</p>					

<b>Driving Force 5</b>	<p>impacting behaviour.</p> <p>Symbolic refers to representations (in the media and social media) which reflect perceived reality.”</p>
------------------------	---

Source: Round 2 of second Delphi study.

**Table 7.54: Evaluation of Driving Force 6 (second-round second Delphi)**

<b>Driving Force 6</b>	“The speed of change is increasing exponentially with global communication becoming instantaneous.”					
<b>Collective Likert score (current significance)</b>	7.1	<b>Collective Likert score (Round 1)</b>	6.5	<b>Collective Likert score change</b>	+0.6	
<b>Collective Likert score (futures relevancy)</b>	8.8	<b>Collective Likert score (Round 1)</b>	8.6	<b>Collective Likert score change</b>	+0.2	
<b>Additional comments from panel members</b>	<p>“Technology is increasingly driving change. New emerging technologies such as AI will start having drastic (good and bad) implications in the next 15 years.</p> <p>I stand by my scores here. It is impossible to question the driver. It is a fact. To what extent will this influence IW? Significantly. This is one of the contributors to instability and therefore opportunity to destabilise.”</p>					
<b>Evaluation</b>	The significance of this driving force especially in terms of its futures relevancy is acknowledged by panel members.					
<b>Decision on final formulation of Driving Force 6</b>	<p>Keep formulation:</p> <p>“The speed of change is increasing exponentially with global communication becoming instantaneous.”</p>					

Source: Round 2 of second Delphi study.

**Table 7.55: Evaluation of Driving Force 7 (second-round second Delphi)**

<b>Driving Force 7</b>	“Non-state actors are increasing their influence related to global security.”
------------------------	---

<b>Collective Likert score (current significance)</b>	7	<b>Collective Likert score (Round 1)</b>	6.8	<b>Collective Likert score change</b>	+0.2
<b>Collective Likert score (futures relevancy)</b>	8.6	<b>Collective Likert score (Round 1)</b>	8.5	<b>Collective Likert score change</b>	+0.1
<b>Additional comments from panel members</b>	<p>“IS is an example of a virtual state spanning across multiple geographical areas.</p> <p>I also see a link back to Q1 here. Can it be questioned that the power of non-state actors can be huge – especially in terms of the symbols they can create for us (which influence our behaviour). No-one in Britain can dismiss the power of NewsCorp in parliamentary elections. Why is George Osbourne currently in China? I bet he is accompanied by major business leaders. Is it really doubted the extent to which oil companies influence international policy?”</p>				
<b>Evaluation</b>	The significance of this driving force especially in terms of its futures relevancy is acknowledged by panel members.				
<b>Decision on final formulation of Driving Force 7</b>	<p>Keep formulation:</p> <p>“Non-state actors are increasing their influence related to global security.”</p>				

Source: Round 2 of second Delphi study.

**Table 7.56: Evaluation of Driving Force 8 (second-round second Delphi)**

<b>Driving Force 8</b>	“Global and intra-regional inequalities are stimulating conflict potential.”				
<b>Collective Likert score (current significance)</b>	7.1	<b>Collective Likert score (Round 1)</b>	6.8	<b>Collective Likert score change</b>	+0.3
<b>Collective Likert score (futures relevancy)</b>	8.3	<b>Collective Likert score (Round 1)</b>	7.9	<b>Collective Likert score change</b>	+0.4
<b>Additional comments</b>	“The migrant crisis in Europe is an example were migrants move from				

<b>from panel members</b>	<p>conflict-ridden areas to mainland Europe. In the process new conflict emerges between European countries around spreading the migrants equally. As competition for basic resources (e.g. water) increases, new migration challenges and other conflicts will emerge.</p> <p>I am feeling a bit entrenched in my views – but since commenting in the first round I am more convinced that inequalities will increase.”</p>
<b>Evaluation</b>	Consensus is that inequality will be a challenge even in terms of the future manifestation of information warfare.
<b>Decision on final formulation of Driving Force 8</b>	<p>Keep formulation:</p> <p>“Global and intra-regional inequalities are stimulating conflict potential.”</p>

Source: Round 2 of second Delphi study.

**Table 7.57: Evaluation of Driving Force 9 (second-round second Delphi)**

<b>Driving Force 9</b>	“Information communication technology (ICT) is embedding itself as a crucial part of society.”					
<b>Collective Likert score (current significance)</b>	8.3 (highest)	<b>Collective Likert score (Round 1)</b>	8.1	<b>Collective Likert score change</b>	+0.2	
<b>Collective Likert score (futures relevancy)</b>	8.9 (highest)	<b>Collective Likert score (Round 1)</b>	9.1	<b>Collective Likert score change</b>	-0.4	
<b>Additional comments from panel members</b>	<p>“Artificial Intelligence, together with the Internet of Things and automation in particular will have a major impact on society. In addition, people get their news from non-traditional platforms such as Facebook, Twitter, LinkedIn, etc. Also, more and more real-world aspects are encoded as symbols (e.g. genetics) which can then be manipulated in various ways. The convergence of AI, genetics, neuro-sciences, robotics, and nano-technologies will provide interesting opportunities and challenges.</p> <p>I think the semantic internet, Internet of Things, and big data will</p>					

	increase this trend.”
<b>Evaluation</b>	This driving force is regarded the highest in terms of both the current significance and the futures relevancy.
<b>Decision on final formulation of Driving Force 9</b>	Keep formulation: “Information communication technology (ICT) is embedding itself as a crucial part of society.”

Source: Round 2 of second Delphi study

**Table 7.58: Evaluation of Driving Force 10 (second-round second Delphi)**

<b>Driving Force 10</b>	“Social media is a significant part of communication and this is expected to grow in the future.”					
<b>Collective Likert score (current significance)</b>	7.6 (Second highest)	<b>Collective Likert score (Round 1)</b>	7.4	<b>Collective Likert score change</b>	+0.2	
<b>Collective Likert score (futures relevancy)</b>	8.8 (Second highest)	<b>Collective Likert score (Round 1)</b>	9	<b>Collective Likert score change</b>	-0.2	
<b>Additional comments from panel members</b>	<p>“Whether it will dumb down or increase average intelligence is a sensitive discussion point. Like all technologies, it has good uses and bad uses. Many risks exist as well. It will also provide a platform for people with similar agendas and causes to organise themselves very quickly.</p> <p>The popularity of social media continues to grow and its influence has become more important than more formal methods of communication. Who would have believed that the UK government now commonly releases policy decision using Twitter? So this adds. And will continue to add to the embeddedness and complexity of information networks.”</p>					
<b>Evaluation</b>	This driving force is regarded the second highest in terms of both the current significance and the futures relevancy.					
<b>Decision on final formulation of</b>	Keep formulation:					

<b>Driving Force 10</b>	“Social media is a significant part of communication and this is expected to grow in the future.”
-------------------------	---

Source: Round 2 of second Delphi study.

**Table 7.59: Additional comments by the second Delphi panel members for Round 2**

<b>Panel members’ response to: Identify any additional driving forces which would be relevant in the context of the future manifestation of information warfare.</b>	<p>Infrastructures, etc. are of particular concern to me. Terrorists can cause havoc by control systems.</p> <p>Uncontrolled AI systems can also inflict pain on financial markets, etc.</p> <p>Increasing polarisation between the haves and the have-nots will pose interesting challenges globally with the potential to destabilise economies should it spill over into drastic actions (e.g. sabotage) by unhappy parties. With social media groups with specific agendas can organise themselves very quickly.</p> <p>I think there will be a convergence of the semantic internet, Internet of Things, and big data which will cause increasing dramatic change.</p>
<b>Evaluation</b>	The additional comments of panel members serve as inputs for the final formulation of scenarios in Chapter 8.

Source: Round 2 of second Delphi study.

During Round 2 of the second Delphi study Delphi panel members measured ten driving forces against two dimensions, namely against current and futures significance. Driving Force 9 (“ICT is embedding itself as a crucial part of society.”) with an average score of 8.3 was the highest. The second highest average score was for Driving Force 10 (“Social media is a significant part of communication and this is expected to grow in the future.”) with an average score of 7.6. This outcome is consistent with Round 1 of the second Delphi study.

Measured against its futures relevancy (2030s), Driving Force 9 (“ICT is embedding itself as a crucial part of society.”) with an average score of 8.9 is the highest. The second highest average score, namely 8.8, was for Driving Force 10 (“Social media is a significant part of communication and this is expected to grow in the future.”). This outcome is consistent with Round 1 of the second Delphi study. (See Appendix H and Appendix I for the second Delphi study’s score sheets.)

During the second round the changes in positions have been marginal. The outcome reached consensus as well as stability. Hence, a third round was not necessary.

## 7.8 FINAL DRIVING FORCES

The two Delphi studies refined and validated the ten most significant drivers influencing the manifestation of information warfare as a national security threat in the 2030s. In this regard, see Table 7.60 for the final list.

**Table 7.60: Final driving forces**

<b>Driving forces</b>	<b>Category: Link to main trend</b>
The centre of <b>power</b> is <b>shifting</b> from the traditional developed countries to the developing countries.	Primary transformation Subcategory: shift
<b>Security</b> in a <b>networked</b> environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.	Primary networked Subcategory: interconnection
An increase in <b>integration</b> and <b>polarisation</b> will contribute to systemic stresses.	Primary transformation Subcategory: revolution
Information warfare will become a growing option for <b>power projection</b> .	Primary transformation Subcategory: renewal
<b>Symbolic, information-related phenomena</b> are increasingly impacting behaviour.	Primary technology Subcategory: modification
The <b>speed of change</b> is increasing exponentially with global communication becoming instantaneous. <b>(third highest prioritised driving force)</b>	Primary technology Subcategory: modernisation
<b>Non-state actors</b> are increasing their influence related to global security.	Primary networked Subcategory: complexity
Global and intra-regional <b>inequalities</b> are stimulating conflict potential.	Primary transformation Subcategory: renewal

Information communication technology (ICT) is <b>embedding</b> itself as a crucial part of society. <b>(highest prioritised driving force)</b>	Primary technology Subcategory: addition
<b>Social media</b> is a significant part of communication and this is expected to grow in the future. <b>(second highest prioritised driving force)</b>	Primary networked Subcategory: system

Source: Own compilation as modified by Delphi studies.

## 7.9 CONCLUSION

The two Delphi studies conducted used the expertise of South African security specialists and a diverse panel of experts on the TWEPS environments to identify the ten main drivers which will create possible scenarios for the manifestation of information warfare as a national security threat by the 2030s. The Delphi studies validated and prioritised the driving forces and assisted in this regard to triangulate previous findings in the study. The highest prioritised driving force was identified as: "Information communication technology (ICT) is embedding itself as a crucial part of society". Findings from the two Delphi studies are used to inform and enrich the more normative process of developing scenarios in the next chapter, by providing defensible grounds upon which to "build" four possible scenarios reflecting the manifestation of information warfare in South Africa by the 2030s.

## CHAPTER 8

### 2030 SCENARIOS FOR INFORMATION WARFARE AS NATIONAL SECURITY THREAT

#### 8.1 INTRODUCTION

The validated driving forces underlying the future manifestation of information warfare still do not provide a depiction of the possible manifestation of information warfare by the 2030s. In this chapter, four such plausible scenarios are formulated.

Van der Heijden (2005:1) stated that the ultimate purpose of scenarios is to create more adaptable organisations, which firstly recognise change and uncertainty, and secondly use it creatively to their advantage. In this study, however, the purpose is to proceed beyond these limited aims of adding only value to a single organization. Inayatullah (2005d:156) explained the full spectrum of scenario outcomes as being possible (irrespective of the laws of the universe), plausible (more realistic, structural considerations), probable (given historical trends and quantitative data) and preferred (what participants desire, the vision of the organisation). The purpose of this study is to create plausible scenarios within which to evaluate the manifestation of how information warfare could develop as a national security threat in South Africa by the 2030s.

This more expansive use of scenarios is not unique and it has been used for strategic purposes in the past. An example of this was the positive role that the outcomes of scenario exercises played in the political transition in South Africa. The communication of scenarios developed by Anglo American, Nedcor/Old Mutual and Mont Fleur during the late 1980s and early 1990s, for example, played a significant role in convincing decision makers to choose the high road to a negotiated settlement and not the low road to demise (Van Vuuren, 2011:227).

The scenario process is underpinned by the assumption that central determinants or elements of the future are already existent in the contemporary real world. As a futures methodology, the scenario process can be used to access and expose these futures. It is possible to extrapolate from key drivers of the future and apply both qualitative and quantitative methods to investigate them in order to be able to wisely reflect and discuss what may someday happen in a more informed manner (Fourie, 2007: 97).

While it can be said that innovation boosting new thinking should be central to the process of creating the scenarios (Lindgren & Bandhold, 2003:25), a critical success factor for useful scenarios remains foresight, which includes the anticipation of events, discontinuities and trends, as well as the so-called “wild card” (Loveridge, 2009:148).

Scenarios offer the prospect of embracing uncertainty in thinking. They represent thought experiments, facilitating trends and events that would not otherwise have become known. Thus scenarios are not predictions. However, as a framework, a scenario must include a plausible possible future state of affairs, prospects, actors and boundaries, all of which will be enveloped by the broader environment (Loveridge, 2009:150). Schwartz (1991:38) concurred that scenarios are not about predicting, but rather about perceiving futures in the present.

Thinking shaped by scenarios assist in understanding the logic of developments, clarifying key players, key factors and driving forces as well as humanity’s own potential to exert an influence on the future (Lindgren & Bandhold, 2003:25). Scenarios draw pathways from the present to several different outcomes, thus providing analysts with the advantage of considering a full series of events between the present and the future (Cronje, 2014:39).

Some regard scenarios as being basically learning oriented. It is seen as “... more of an art form than an activity with a well-established theoretical base” (Loveridge, 2009:148). Schwartz (1991:114) stated that scenario creation is not a reductionist process; instead it is an art, as in storytelling. While this is the case, a substantive amount of work has also been done on especially the methodological aspects of scenario exercises, both in the academic and practical fields, making it possible to benefit from such scenarios. Recent writings agree that good scenario work is both analytical (rational) and conceptual (generative). It is possible to apply all forms of logic in scenario work namely inductive, deductive and abductive logic. Scenario work is both an art and a science (Ogilvy, 2005:331).

Some background on the development of scenarios, the definition of scenarios, the identification of the uses thereof, and an explanation of the nature of the scenario exercise will be of value before the scenario methodology can be implemented in this study.

## **8.2 BACKGROUND TO THE DEVELOPMENT OF SCENARIOS**

In order to understand the potential value of scenarios, it is useful to briefly examine the historic development of the scenario method. The first use of the scenario method dated back to the actions of RAND Corporation during and after World War II. Subsequently, it was further evolved by the Hudson Institute, especially by Herman Kahn after he resigned from RAND. Kahn

developed this method, calling it a “future-now” way of thinking (Lindgren & Bandhold, 2003:36). Kahn adopted the term “scenario”, a Hollywood concept which refers to a detailed outline of a future movie that was fictional, reinforcing his contention that scenarios do not make accurate predictions, but rather develop stories to explore the future (Van der Heijden, 2005: 3).

The rise of the scenario method was related to the collapse of the usual extrapolative planning because of the mounting uncertainties most entities “faced during the Cold War years and particularly from the mid-1960s onward” (Loveridge, 2009: 147). As the two superpowers, the USA and Soviet Union, were in a nuclear standoff, strategic planning failures in such an environment could evidently have had catastrophic consequences (Cronje, 2014:31-32).

Originally, scenario analysis was fundamentally an addition of the traditional “predict-and-control” approach to planning. The most notable change was that a single-line forecast was substituted by a probabilistic assessment of alternative futures, resulting in a “most likely” projection. This did not provide sufficient progress over other forecasting approaches and by the end of the 1960s, the defects in this approach were widely known. The scenario-based method used in this study has at its core a completely different central idea, namely not relying on probability but on causality (Van der Heijden, 2005: 3). As such, it provides for the intuitive need to expand knowledge and understanding.

In the 1970s the scenario method reached beyond the Hudson Institute and RAND. Companies like Royal Dutch Shell as well as consultants such as Batelle and SRI International adopted scenarios as part of their strategy methodologies. Consequently scenario planning became more closely related to business strategy. Shell is also acknowledged as the first company to use scenarios widely as a strategy method in the corporate setting. Kees van der Heijden, Pierre Wack and Arie de Gues were some of the famous scenario experts of that time (Lindgren & Bandhold, 2003:36-37).

The method used by Wack and his team in Shell’s group planning department was to examine rigorously forces driving change in the sectors or markets under investigation. Thereafter the team would, for a given set of assumptions, formulate a small number of different, internally logical stories (scenarios) as to how these forces could play themselves out. These stories were aimed at assisting managers to understand the ways in which the future would not be the same as the past and also to prepare them, through their enhanced grasp of the context in which they were working, to take better and informed decisions as the future actually unfolded (Segal, 2007:5-6). The scenario method was also used outside the business environment in policy and academic environments.

During the 1970s a number of national entities in the West were financed to study the future. Several of these entities utilised scenario planning as an essential futures examination method. However, this “scenario planning era” was short lived, as a result of the oil crises and recession in the mid and late 1970s. During the 1980s renewed interest in how planning happens led to various futures-orientated entities developing scenario planning methods. The changes of the 1990s as well as the renewed awareness in managing uncertainty through scenario planning and thinking have resulted in the further refinement of scenario methodologies. The scenario method still plays a major role in multi-national entities and has become a standard method used by most consultancy firms and companies over the last decade (Lindgren & Bandhold, 2003:36-37).

### **8.3 USE OF SCENARIOS IN SOUTH AFRICA**

Scenario planning with the aim to influence policy-makers and shape public opinions has played a significant role in South Africa’s history. This was particularly the case during the unstable political transition years of the 1990s. The High Road/Low Road scenarios were created by Anglo American in the late 1980s and early 1990s and were the original but conceivably the most well-known of these South African examples. An Anglo American team including Pierre Wack produced these scenarios for the company’s internal use, but then also released the scenarios for public consumption. These scenarios ignited noteworthy debate about the future course of the political and economic development of the country (Cronje, 2013:111). The Anglo American scenarios in particular made some contribution to thinking during the immediate pre-transition and early transition period in South Africa. Segal (2007:17) stated that this contribution must be regarded as one of the positive factors that encouraged the government to finally embark on the political transition in South Africa.

Senior government officials were already familiar with the Anglo American scenarios because structured approaches to thinking about the future had been initiated by the military and the security services in the late 1970s. However, their work remained tightly held within the entities undertaking it and was not shared across government as a whole. During the early 1980s a new approach to future thinking was initiated in the State Security Council (SSC), which continued for a decade. This was done across many departments and involved outside experts including Philip Spies, the doyen of South Africa’s futurists and then director of the Institute for Futures Research (IFR) at Stellenbosch University (SU), and Clem Sunter, the “father” of scenario planning in South Africa. The overall purpose was to encourage strategic thinking about the future, and scenarios were seen as an essential input to this end (Segal, 2007:17).

The Anglo American High Road/Low Road scenarios (presented from 1986 to 1990) captured the imagination of corporates, professionals and other circles to an extent that had not been seen

previously. It became a useful and perhaps even necessary platform on which the later Nedcor/Old Mutual and Mont Fleur exercises could build (Segal, 2007:19). During 1990 the Nedcor/Old Mutual scenarios, which involved Pierre Wack, were developed and communicated to both domestic and foreign role-players involved in South Africa's economic and political transition at that time (Segal, 2007:36). The presentations, which ran from 1991 to the middle of 1992, had an aggregated audience of around 45 000 South Africans (Segal, 2007:37). Three scenarios were produced, which presented the risk of "a disengaged civil society falling victim to an interventionist state" (Cronje, 2013:111).

The Mont Fleur scenarios differed from the other two projects in several significant respects. It was a project essentially of civil society and not of the corporate sector. From the outset, it was also well connected politically with the African National Congress (ANC – the later ruling party) in particular. It adopted a methodology dependent on facilitating debate and finding common ground among diverse perspectives, rather than being research-based (Segal, 2007:45). From August 1992, the results were presented to the most influential economic and political role-players in South Africa's transition process (Segal, 2007:47).

The Anglo American, Nedcor and Mont Fleur scenarios accentuated the perils of a South Africa not reaching a negotiated settlement, strengthened efforts to reach a negotiated settlement and implemented a transition to democracy (Cronje, 2013:111).

#### **8.4 DEFINING SCENARIOS**

A variety of definitions describe scenarios created through a scenario method. A scenario is a technique of organising many assertions about the future; however, it is not a single forecast or prediction. It represents a plausible description of what might occur. A scenario is a narrative that links an account of a particular future to illustrate existence in a sequence of causal links which highlight the influence of consequences and decisions. Scenarios thus describe events and trends as they could evolve (Glenn, 2003:4). A scenario can therefore also be viewed as a narrative of an alternative setting in which current decisions may be played out (Ogilvy & Schwartz, 1998:2). A scenario presents descriptions of plausible futures (Lindgren & Bandhold, 2003:22).

Additionally, scenarios can fulfil the above-mentioned roles in envisaging plausible possible futures by taking account of bedrock certainties, things that may or may not happen, and complete uncertainties (Howkins & Valantin, 1997). Scenarios are like hypotheses of different futures purposely designed to highlight the opportunities and risks involved in specific strategic issues (Ogilvy & Schwartz, 1998:2). Scenarios hold value for future studies as they can assist individuals

to explore what the future might look like and the likely challenges to be faced in these futures (Global Business Environment, 2003:8).

All of above provides a broad view of what scenarios are and the contribution they can make. For the purposes of this study the conclusions of Cronje (2013:98) are used in this regard: "... as plausible extrapolations of the future, scenarios are descriptions of how trends already evident in a system may combine over time. Scenarios, as a concept, can therefore be defined as: A set of diverse but equally plausible descriptions of future events for the same system."

In Chapter 3 it was stated that despite the interconnectedness of past, present and future, any definitive study of the future requires an open-minded futurist approach to gain insight into the dynamics between the past, present and future. Such an approach may lead to foresight. In terms of the scenario output, it will also be necessary to identify the types of futures likely to be experienced.

## **8.5 FOUR TYPES OF FUTURES**

According to Courtney (2001:21-33), four types of futures or diverse options are distinguished from one another by their comparative uncertainty. The four forms Courtney (2001:21) identified are:

1. A clear, single view of the future
2. A limited set of possible future outcomes, one of which will occur
3. A range of possible future outcomes
4. A limitless range of possible future outcomes.

In the case of a clear, single future, uncertainty does not have much of an impact as the range of possible outcomes is narrow. The future is not necessarily perfectly predictable but at least it is predictable enough for a primary strategy of choice to conform to all plausible outcomes (Cronje, 2014:28). Taking into account the time frame and complexities influencing information warfare, a clear, single view of the future is not possible.

Alternate futures become possible when it is achievable to identify a narrow set of possible outcomes. Courtney (2001:25) identified potential regulatory, legislative or judicial changes as sources of this level of uncertainty. Although regulation is one aspect of the manifestation of information warfare, the nature of the phenomenon as illustrated in the environmental scan is such that it would prove to be highly unlikely to be constrained by legislation and regulation.

In the case where the future is more uncertain than a single alternate future, a range of possible future outcomes might be identified. In such a situation the identification of a shortlist of possible

outcomes is not possible. Rather, it is essential to develop an expansive series of plausible outcomes (Courtney, 2001:31). Information warfare futures serve as an example in this regard.

Where a limitless range of possible future outcomes exist, uncertainty is increased. In such a case it is of value to rather categorise the different variants or kinds of futures according to their relative uncertainty (Cronje, 2014:29). Courtney (2001:32) regarded Level 4 situations as rare and stated that they tend to degrade over time to lower levels of uncertainty. The impact of major social or economic discontinuities, for example, result in such a future, which makes it difficult to even identify a series of possible future outcomes.

The pace and nature of change are additional factors impacting on scenarios. Ralston and Wilson (2006:11) stated that the character of change itself has been adjusted. Change is becoming more rapid as well as complex. Furthermore, the development time for new products and new systems has been radically compressed from their original invention to their diffusion through society. Innovations in the sectors of nanotechnology, biomedical advances, nuclear power and information technology "... will have a more pervasive influence on human life than any other previous technologies in human history". This is also an issue that was highlighted in all the environments during the environmental scan in Chapter 5.

As a third or fourth variant future, the manifestation of information warfare is thus not easy to forecast. That future must still be shaped. This will be based on a diverse set of factors, including how technology impacts on the system, the way the role-players in the system interrelate with each other over the next decade, how that interaction impacts on the balance of negative and positive feedback entering the system, and how the regulating authorities react in trying to promote positive over negative feedback (Cronje, 2013:102). All of these interactions and events creating the information warfare future must still take place. Consequently, this future "... is too uncertain to be forecast to a single point in time, but must rather be presented as a spectrum of equally plausible future possibilities" (Cronje, 2013:102).

## **8.6 APPROACHES TO SCENARIOS**

Two fundamentally diverse approaches can be used to determine the basic premises of scenarios. The methods are inductive and deductive. The inductive method is not as structured as the deductive method. It relies mainly on patience to continue with deliberations until consensus is reached. The general logical principles are derived from particular facts or instances. In contrast, the deductive approach uses uncomplicated procedures of prioritisation to conduct a two-by-two scenario matrix based on the two key driving forces (Schwartz & Ogilvy, 1998:61-62).

It is also possible to distinguish between analytical versus intuitive scenario approaches. Analytical scenario approaches use formal models or simulations to develop both broad alternative scenarios and their details. In contrast, intuitive scenario approaches centre more on qualitative visions of the future that reflect the “mental maps” of the scenario developers. They, too, may have considerable analytical detail, but intuition plays a greater role in their initial development. In practice, most scenario work involves both approaches (Ralston & Wilson, 2006:22). In this study, deductive and analytical scenario approaches (with elements of the intuitive scenario approach) are followed.

## 8.7 IDENTIFYING DIFFERENT PURPOSES FOR SCENARIOS

Based on years of experience in using scenario methodology in various projects, Lindgren and Bandhold (2003:24-26) identified four basic purposes for the scenario method. (See Figure 8.1 for a graphical presentation in this regard.) The four purposes identified are related to planning and feature crafting new direction (in which innovation is central), identifying prerequisites for change (in which learning is central), appraising current direction (in which evaluation is central) and planning future action (in which strategic planning is central). Thinking within a scenario structure assists in understanding the logic of developments; clarifying key players, key factors, and key driving forces, and provides the potential to exert an influence on future outcomes. Scenarios are powerful in challenging existing assumptions and paradigms.



**Figure 8.1: Different purposes and different focuses for scenarios**

Source: Lindgren and Bandhold, 2003:25).

The practical value of scenario building for especially decision-makers and planners is emphasised in most of the literature on scenario building as practical methodology. As illustrated earlier, the Anglo American, Nedcor and Mont Fleur scenario exercises played a positive role in the transition of South Africa to a democratic state. This demonstrates what Schwartz (1991:3-4) identified as some of the main uses of scenarios. The South African examples allowed their users to think about the effects that policies will have in the future rather than be concerned about immediate political expediency within an extremely uncertain world. It also allowed a significant number of individuals to appreciate the long-term repercussions of decisions made in the 1990s during uncertain times in South Africa (Cronje, 2013:112). Schwartz (1991:4) referred to the utilisation of scenarios for reasons ranging from assistance in personal decision-making to assistance in corporate decision-making. He also remarked that scenarios sometimes make it possible to address concerns about complicated decisions that would otherwise be “missed or ignored”.

### **8.7.1 Purpose of scenario method in this study**

In this study, the main purpose of using scenario building was to evaluate possible futures of information warfare. Hence, four plausible possible exploratory scenarios focused on information warfare as a national security threat in the 2030s were identified. This was done by highlighting the risks, taking note of uncertainties and using mainly qualitative inputs derived from an environmental analysis, an information warfare model (inclusive of CLA) and the Delphi process. Descriptive or exploratory scenarios portray trends and events as they could develop, based on different conjectures on how these trends and events may influence the future (Glenn, 2003:4).

## **8.8 SCENARIOS AS MENTAL MODELS**

Scenarios serve as mental models by providing an additional or alternative approach to analyse, reveal and reconstruct a specific issue (Chermack, 2003:33). Mental models provide the lenses through which the world is viewed and incorporate values, biases and beliefs about how the world functions (Forrester, 1973:14). Senge (1990:8) defined mental models as “...deeply ingrained assumptions, generalizations, or even pictures or images that influence how we understand the world and how we take action. Very often, we are not consciously aware of our mental models or the effects they have on our behaviour.”

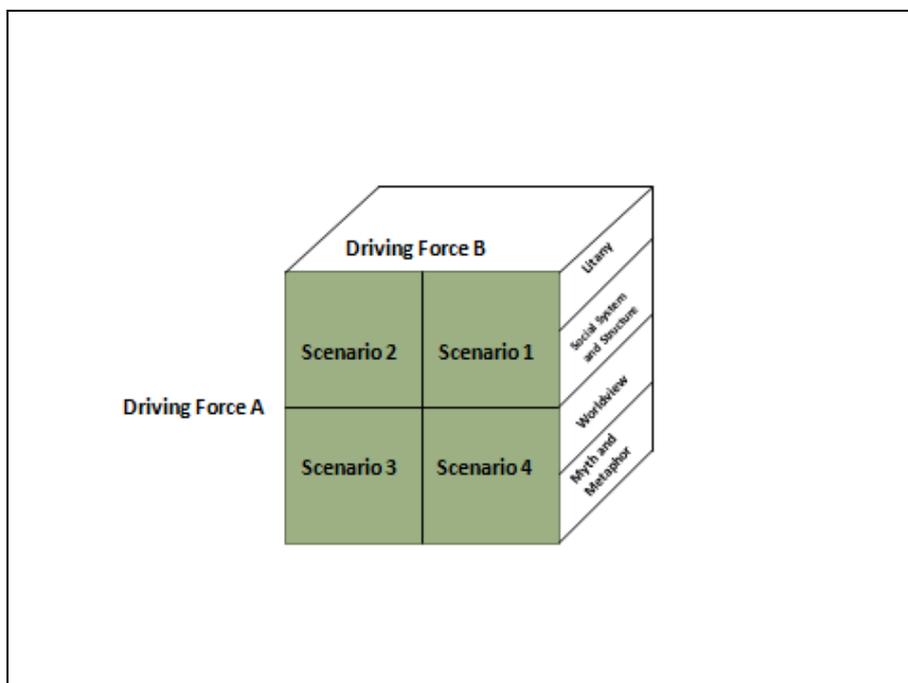
Although scenarios are future-orientated mental models that form mind representations that direct activities in the actual world, all mental models are restricted by their partiality (Loveridge, 2009:151). Two options are available to manage the existing mental models' impact on scenario building. The one option is to acknowledge existing mental models and process their role in the

outcomes. The creator or creators of the scenario thus need to be explicit about assumptions regarding their worldviews. These assumptions constitute the mental models in use. Mental models can therefore be revealed by examining the underlying assumptions about the manner in which a process or domain of knowledge works, exists and operates (Chermack, 2003:37).

Another option could be to insist on the deferral of existing mental models so that speculative ones can be developed in the context of the unknown future (Loveridge, 2009:151). In many thought experiments this is done by suspending current mental models. The extent to which this can be done will determine the creation of scenarios that can modify perceptions to a different dimension (Loveridge, 2009:151). Neither of these two options provides an ideal solution. However, the facilitators or creators of scenarios should be alert to this challenge and communicate whether rigid mental models impact on the process.

In Chapter 3 it is stated that a futures map is a generic design of the various futures and a symbolic representation of what might unfold or be comprehended by human interventions in the material world (Malaska & Virtanen, 2009:69). As a futures map is therefore the all-inclusive description of the outcomes of a futures research process, it will encompass the scenarios envisaged for the manifestation of information warfare in South Africa by the 2030s. The approach in this study is to use the model created in Chapter 6 (see Figure 6.3 for the graphical representation) as the framework for the creation of scenarios. The scenarios are created within the mapping horizon of this model.

The dominating structure for scenario building is to identify two driving forces that are considered together in a scenario matrix. This will result in four different scenarios, which will be developed within the four spaces created (Lindgren & Bandhold, 2003:66). (See Figure 8.2 for a graphical representation of this.)



**Figure 8.2: Scenario matrix which constitutes four different scenarios based on two main driving forces**

Source: Lindgren and Bandhold, 2003:67, modified with own studies model applicable to information warfare futures.

To add depth and breadth to the scenarios, the layered CLA approach was followed. CLA was identified in Chapter 3 as a tool to categorise different views of and concerns about the future, and then used in Chapter 6 to identify the driving forces. Using CLA to develop the scenarios assists with deconstruction and increasing the depth of the scenarios developed (Inayatullah, Minkkinen & Heinonen, 2015).

The scenarios should be more than an authoritative narrative as they should also identify the salient points which still could be acted on. Individuals using scenarios should feel that the scenarios have touched their deepest, most radical concerns. They should then be willing to test their future decisions against each scenario. Scenarios should always connect to realistic choices and ultimately to decisions and action (Howkins & Valantin, 1997). Compared to a simple hypothesis, a scenario is a complete, carefully thought out and highly consistent picture. Scenarios help one to grasp and limit one's own uncertainty as well as to detect the limits of a plausible future. The success of the method depends on the understanding of the result and if applicable, the associated course of action (Pillkahn, 2008:228).

In the process of creating scenarios it is vital to find two driving forces that, combined with each other, will provide four substantially different scenarios that can actually assist to provide insight into possible and probable futures. After identifying and selecting a number of drivers to facilitate change, these drivers can be combined through qualitative processing (Lindgren & Bandhold, 2003:67). Following the identification and exploration of the driving forces, it is important to uncover the "predetermined elements" and the "critical uncertainties" (Schwartz, 1991:113).

Successful mental models within scenarios will need to focus on two aspects according to Ringland (2006:4):

- The ability to anticipate real-world behaviour (which in some cases may be unexpected) through investigating the constraints or changes in the external environment, or the relationships between driving forces.
- The creation of a mental model which allows the user to look for early confirming or disconfirming indications.

## **8.9 KEY ASPECTS OF SCENARIOS**

### **8.9.1 Boundary setting**

Synthesis within mental frameworks assists to establish scenarios of value, of which boundary setting is the first (Loveridge, 2009:151). In this study, the broad macro environment has been set out in Chapter 3 as the Technological, War/Conflict, Economical, Political and Social (TWEPS) hexagon.

The role of the observer within the scenario environment is also of significance. It is not true that the observer is in some way external to the system. The observer becomes part of the system by the very act of observing. Boundary setting on this level is also done subjectively from inside the system. The mental and cultural worldviews of the participant(s) are thus carried along during the scenario exercise (Loveridge, 2009:152).

Exploring the assumptions that the participant(s) currently hold about the future provide insight to act more effectively in the present (Global Business Environment, 2003:12). It can assist in recognising when assumptions are being challenged by events and knowing how to respond appropriately. The interplay between the context in which the phenomenon occurs and the developed scenarios need to be critically evaluated to identify potential inconsistencies. In this process the issue of the boundaries of the scenario exercise as a whole as well as the individual scenarios created should be taken into consideration.

The outcome of the environmental study done in Chapter 5 stressed the rhizoid network nature which strengthen the threat posed by information warfare to national security. Three trends have also been identified, which are common to all environments evaluated in the scan. These are the rise of networks (especially social networks), rapid innovation (especially in the spread of technology), and transformation (as a constant reality affecting nearly all social entities). These trends reinforce the notion that a globalised, interconnected future (in terms of the threats posed by information warfare) will probably confront South Africa. The boundaries for the possible future scenarios will thus be global and not only limited to the domestic situation.

### **8.9.2 Managing uncertainties**

Although scenarios offer the prospect to include and embrace uncertainty in thinking, the nature of uncertainty in terms of the scenario method needs to be clarified. It must be acknowledged that there are no tools to explain how today becomes tomorrow. However, it is important to clarify that

uncertainty in this context is not knowing what tomorrow will be like. Uncertainty is not knowing which events, trends, issues and decisions will constitute tomorrow (Marsh, 1998: 44).

The deductive approach to scenario building is used in this study. Scenarios provide a way to cope with uncertainties by creating the space to develop insights. Often, during the grounding phase, a number of drivers can be identified that have a significant impact on the central subject but that are not easy to predict. It thus remains uncertain what the true impact of these drivers will be (Lindgren & Bandhold, 2003:22). In complex systems, which have evolving properties, the deductive approach can assist in overcoming the risks intrinsic to such evolving properties. The scenario method has the potential to support efforts to overcome the conjecture and disagreements that accompany work to create foresight in uncertain systems (Cronje, 2013:98).

In this study, the technique used to contain uncertainty in terms of the driving forces was the Delphi studies conducted to identify, verify and prioritise these driving forces. The Delphi studies provided a credible outcome based on the clear decision trail that defends the appropriateness of the method to address the problem selected, choice of expert panel, data collection procedures, identification of justifiable consensus levels and means of dissemination and implementation.

Some of these drivers are so uncertain that they could be called “wild cards”. Such wild cards could of course have significant impact on the central subject, but their predictability is so small that they cannot be meaningfully used as a basis for scenarios (Lindgren & Bandhold, 2003:22). While scenarios are something one plans for, wild cards are things that one plans against. Wild cards are surprises that have the power to completely change the situation as well as the outcome of the scenario. Wild cards include:

- Complete discontinuous events
- Discontinuities that might be anticipated but which have significant unintended consequences
- Catalytic developments so different in scale or degree that they are different in kind (Schwartz & Ogilvy, 1998:74).

## **8.10 STRENGTHS AND WEAKNESSES OF THE SCENARIO METHODOLOGY**

The scenario method is a powerful instrument for several reasons. This includes its ability to overcome complexity, to focus on a wide range of options, to empower participants, to create a coherent future vision and to integrate capacities in order to create innovative views.

Lindgren and Bandhold (2003: 28-29) mentioned that the scenario method is a brain-compatible arrangement as scenario thinking matches the way the brain works. According to them, the

narrative format used for scenarios (stories and images) makes them memorable without difficulty. Visualisation assists in ensuring that scenarios can be regarded as believable. Scenarios remain one of the simplest means to deliver complex information to the scenario audience and to construct future possibilities which appear more authentic (Glenn, 2003:16). The strength of this method can also be ascribed to its inherent ability to overcome the complexity dilemma facing any forecasting (Cronje, 2014: 35).

The future of complex systems is plural rather than singular (Cronje, 2014: 35). In this regard the scenario method helps to develop outcomes that are viable over the wide range of possible futures. Scenario-based planning has the potential to meet this strategic challenge (Glenn, 2003:16). There is, for example, no systematic external environmental scanning capability permitting long-term contingency planning in most entities. Forward thinking creates a “decision context” in which unpleasant surprises can be minimised. It means that crises can be kept to a minimum (but of course, never eliminated entirely). As the stakes mount globally, so it becomes increasingly important to invest human and material resources in all forms of forward thinking (Slaughter, 2005a).

The development of scenarios is an intense process that includes speculation, reflection, discussion, rejection, comparison and analysis, to name but a few of the related activities. Scientific methods and logic alone are not enough. Knowledge, creativity, fantasy, powers of imagination and experience are fundamentally important to shape the future. It would be more suitable to describe the activity behind the development of provocative, refreshing and challenging scenarios as an art rather than as a science (Pillkahn, 2008:227-228).

The process of developing scenarios with individuals who have a stake in the future assists them to strengthen anticipatory consciousness. Plans can change as transformation continues to gain momentum. The scenario creation process itself can fundamentally change the way those partaking in the process think about the future. A balanced evaluation of the range of strategies that may be required can be developed. The process changes the participants’ perceptions and evaluations of trends and the full range of events that may occur in reality. As an alternative to each possibility is a potential threat to an inflexible plan, these trends and events tend to be evaluated as sign posts, indicating pathways along the way to anticipated and alternative futures (Glenn, 2003:16).

A weakness of scenarios is that critics of this method sometimes argue that scenario planning is not very useful if it presents a significant number of plausible but different extrapolations of the future (Cronje, 2013:107). According to Cronje (2013:107), this criticism can be answered in one of two ways. Firstly, it must be remembered that certainty is an illusion when dealing with the

emergent characteristics of complex systems over the long term. This cannot ever be achieved as the future of such systems is still to be determined. Over time, relatively minor amendments in the present conditions of such a system may result in momentous changes in the future. Secondly, critics can be reminded that scenarios are not forecasts. Unlike forecasts, the value of scenarios does not depend on whether they are correct. Instead, what scenarios endeavour to present is "... a number of different descriptions of how the future may evolve based on how key events in the time leading up to the scenario interact with each other and how that interaction changes". These central interactions and events develop into "a roadmap to the future."

Non-participants might regard scenarios as the "official set of possible futures" and therefore limiting or controlling their thinking to an extent. Scenarios have the capacity to influence the consumer in subtle ways because of the creator's assumptions about cause and effect (Glenn, 2003:16). Therefore, the purpose and limitations of scenarios should be explicitly stated.

### **8.11 THE PROCESS OF DEVELOPING SCENARIOS**

While it can be stated that a scenario-based exercise is a practitioner's art (Van der Heijden, 2005:155), the approach should be carefully structured. However, the real key is not so much about perfecting a particular method, but rather about satisfying the conditions, namely diversity, decentralisation and independence (Surowiecki, 2004:22).

In general, the development of scenarios is a group activity. Chermack (2011:218-219) stated that the right team's involvement is important for the success of a scenario project as team members can provide valuable information about the history, issues, context and politics of the case being investigated. He also suggested that such a team should be cross-functional and multi-levelled. Ideally, a diverse group of individuals should be used to assist in developing the content of scenarios. However, this study followed a process in which group input was integrated into whole scenario creation process backed by an extensive literature review. The key driving forces were identified through processes involving an environmental scan, qualitative text analysis, model inclusive of CLA, Delphi studies and an impact analysis. Although the author was the primary developer of the four scenarios, he extensively consulted and brainstormed with a diverse range of individuals to obtain input and guidance and undertook an extensive literature survey on scenarios. Additionally, the author also used a range of inputs obtained from two Delphi studies. These procedures ensured that the diversity, decentralisation and independence criteria were fulfilled in terms of the scenario process.

Steps have been identified to build a scenario. Based on the insights of Schwartz (1991) and Cronje (2014:45-52), the following steps were used in implementing the scenario study:

### **8.11.1 Establish the aim of scenario creation**

The outcome of the scenario exercise is the compilation of four possible future scenarios highlighting the impact of information warfare as a South African national security threat in the 2030s. Cronje (2014:51) described scenarios as follows: “The scenarios in the four quadrants of the scenario matrix are outlines, or wire frames, of four possible futures, based on the interplay of the two most important and most uncertain trends.”

### **8.11.2 Define the key concepts**

In Chapter 4, information warfare was defined as actions focused on destabilising or manipulating the core information networks of a state or entity in society with the aim to influence the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state. In Chapter 4, the components of information warfare – namely netwar, psychological operations and cyber warfare – were also defined. National security refers to all government-sanctioned actions and measures driven by the application of national will.<sup>28</sup> National security measures are taken with the aim to create an environment in which the country’s population, state structures, territorial integrity, interests and sovereignty are protected.

### **8.11.3 Analyse the environment**

In Chapter 5, the environment scan was completed focusing on the TWEPS macro-environmental hexagon within which information warfare is manifesting. Transformation, networking and the impact of innovation in all the environments investigated were highlighted as central trends in the manifestation of information warfare currently as well as in the future.

### **8.11.4 Evaluate the driving forces**

In Chapter 6, the key driving forces critical for the manifestation of information warfare as a national security threat by the 2030s were identified. This was done by using a model which assists in creating futurist insight into the manifestation of information warfare as a future national security threat. The model uses qualitative text analysis and a layered mode of evaluating the environment

---

<sup>24</sup> In this context, national will refers to the “paradoxical trinity” as formulated by Von Clausewitz (see Figure 4.2).

in the search for the driving forces. (Table 6.6 in Chapter 6 presents the driving forces identified by way of the mentioned information warfare futures model.)

The two Delphi studies conducted in Chapter 7 verified the final ten main driving forces. (Table 7.60 in Chapter 7 presents the final driving forces.)

#### **8.11.5 Identify the two key drivers**

The two Delphi studies identified three driving forces as the most significant, namely ICT Embedding, Social Media and the Speed of Change. These three drivers, however, are related and do not provide the required content contrast to create four distinct scenarios. Based on the outcome of the Delphi Studies, the ICT Embedding driver (“Information communication technology (ICT) is embedding itself as a crucial part of society”) is used as the one key driver for purposes of compiling the scenarios.

In Chapter 7 qualitative text analysis was used on this driving force, which falls in the category “Innovation”, subcategory “addition”, in which the specific dimensions can be measured on a low level of manifestation to a high level of manifestation axis. The low level axis does not necessarily imply that ICT embedding should be at a lower level than is currently the case, but implies a future where the level of ICT embedding is the same as currently without taking advantage of the growth potential that currently exists. The causes of low levels of ICT embedding include economic, social or political setbacks or even technology implementation obstacles caused by policy and regulation. The high level axis refers to the situation where ICT embedding reaches exponential levels, implying the linking of most manufactured items in society to an ICT network.

Cross-impact analysis provides a method which could be used to identify the second key driving force. This technique can be used to measure the influence of all drivers. This is done by juxtaposing the individual driving forces in order to identify their respective mutual interrelationships. The central question during this whole process is: “How do the different driving forces behave in relation to each other?” Impact analysis is consequently used as a means to systematically identify interactions and dynamics. The driving forces are listed in a matrix of columns and rows, in both cases in the same order of succession. In this way, each factor is juxtaposed with each of the others. For each pair of driving forces, the question is then asked: “To what extent does a direct relationship take effect between these driving forces?” To quantify the influence, the following scale is used: 0 = No influence; 1 = Weak relationship; 2 = Medium relationship; 3 = Strong relationship. All combinations are evaluated while the centre diagonal of the matrix remains empty. It is then possible to calculate the sums of the lines and columns, which serve as a measure of the degree of networked interrelationships.

The “line sum” of any driving force represents the so-called “Active Sum” (AS) and indicates how strongly that driving force affects other factors. The “column sum” of a driving force, on the other hand, represents the so-called “Passive Sum” (PS) which shows how strongly that factor is influenced by other factors (Kosow & Gassner, 2008: 51-52). (See Table 8.1 and Table 8.2 for the influence matrix, legend and outcome of the driving forces.)

**Table 8.1: Influence matrix for driving forces**

	DF:1	DF:2	DF:3	DF:4	DF:5	DF:6	DF:7	DF:8	DF:9	DF:10
DF:1	xxx	1	1	1	1	1	1	1	1	1
DF:2	1	xxx	2	3	1	2	1	2	0	1
DF:3	1	2	xxx	3	2	3	3	3	1	2
DF:4	1	2	3	xxx	2	0	3	3	1	2
DF:5	1	1	1	2	xxx	1	3	2	1	2
DF:6	1	3	3	2	2	xxx	2	3	3	3
DF:7	1	3	2	2	2	0	xxx	1	1	1
DF:8	1	1	1	1	3	0	3	xxx	1	1
DF:9	2	3	3	3	2	3	2	3	xxx	3
DF:10	1	2	1	2	3	1	3	1	1	xxx

Own compilation based on Kosow and Gassner, 2008: 51.<sup>29</sup>

**Table 8.2: Legend and outcome of the influence matrix for driving forces**

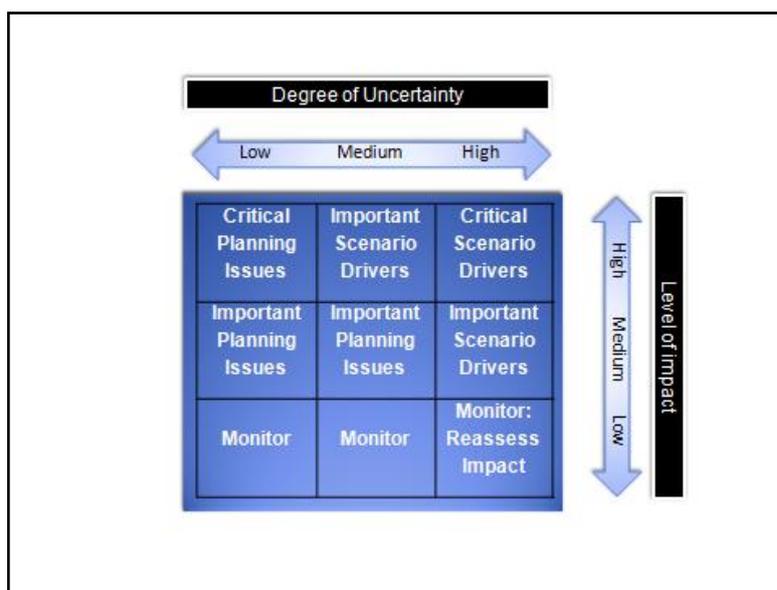
Designation	Driving force	Active Sum (AS)	Passive Sum (PS)
DF:1	The centre of <b>power</b> is <b>shifting</b> from the traditional developed countries to the developing countries.	9	10
DF:2	<b>Security</b> in a <b>networked</b> environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.	13	18
DF:3	An increase in <b>integration</b> and <b>polarisation</b> will contribute to systemic stresses.	20	17

<sup>29</sup> The cross-impact analysis was done on 24 August 2015 by the author and Professor André Roux during a brainstorming session in Cape Town. In processing each driving force it was coded, the category and subcategory stated and then measured against the stated scale. The criteria for the scale were agreed during the brainstorming session as judging the level to which the driving force under consideration is being connected but also influencing the driving force it was measured against. The cross-impact analysis has assisted in the evaluation of the driving forces and informed the scenario-processes.

<b>DF:4</b>	Information warfare will become a growing option for <b>power projection</b> .	<b>17</b>	<b>19</b>
<b>DF:5</b>	<b>Symbolic, information-related phenomena</b> are increasingly impacting behaviour.	<b>14</b>	<b>18</b>
<b>DF:6</b>	The <b>speed of change</b> is increasing exponentially with global communication becoming instantaneous.	<b>22</b>	<b>11</b>
<b>DF:7</b>	<b>Non-state actors</b> are increasing their influence related to global security.	<b>13</b>	<b>21</b>
<b>DF:8</b>	Global and intra-regional <b>inequalities</b> are stimulating conflict potential.	<b>12</b>	<b>19</b>
<b>DF:9</b>	Information communication technology ( <b>ICT</b> ) is <b>embedding</b> itself as a crucial part of society.	<b>24</b>	<b>10</b>
<b>DF:10</b>	<b>Social media</b> is a significant part of communication and this is expected to grow in the future.	<b>15</b>	<b>16</b>

The priority outcomes of the three most significant drivers based on their Active Sums are ICT Embedding, Speed of Change and Integration/Polarisation. The third driving force is formulated as follows: “An increase in **integration** and **polarisation** will contribute to systemic stresses.” This driver is a possible candidate for a second key driver. Using qualitative text analysis on the driving force, this driving force falls in the category “Transformation”, subcategory “Revolution”, in which the specific dimensions can be measured on a high level of integration to a low level of integration axis (thus high level of polarisation).

The level of impact of all driving forces is measured by way of cross-impact analysis. An issue which has not yet been addressed in the analysis is the certainty or uncertainty of the driving forces. In this regard, an impact-uncertainty matrix can be useful as it systematically evaluates the certainty-uncertainty dimension of the driving forces (see Figure 8.3). The high-medium-low scoring system allows for each driving force to be positioned on a matrix (Wilson 1998:89).



**Figure 8.3: Illustrative impact-uncertainty matrix**

Source: Wilson, 1998:89.

The rating of the impact of each driver was done during the cross-impact analysis. An evaluation of the degree of uncertainty in terms of pace, direction and the actuality of its future course is useful (Wilson 1998:88-89). The outcome of an evaluation based on the analytical insights gained during the environmental scan, qualitative text analysis, model development, CLA and Delphi studies led to the identification of four driving forces classified as critical scenario drivers, namely Integration/Polarisation, Speed of Change, ICT Embedding and Social media. (See Table 8.3 for the full outcome of the impact-uncertainty matrix for driving forces.)

**Table 8.3: Legend and outcome of the impact-uncertainty matrix for driving forces**

Designation	Driving force	Impact-uncertainty matrix outcome
DF:1	The centre of <b>power</b> is <b>shifting</b> from the traditional developed countries to the developing countries.	<b>Important Planning Issue</b>
DF:2	<b>Security</b> in a <b>networked</b> environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.	<b>Important Scenario Driver</b>
DF:3	An increase in <b>integration</b> and <b>polarisation</b> will contribute to systemic stresses.	<b>Critical Scenario Driver</b>
DF:4	Information warfare will become a growing option for <b>power projection</b> .	<b>Important Scenario Driver</b>
DF:5	<b>Symbolic, information-related phenomena</b> are increasingly impacting behaviour.	<b>Important Scenario Driver</b>

<b>DF:6</b>	The <b>speed of change</b> is increasing exponentially with global communication becoming instantaneous.	<b>Critical Scenario Driver</b>
<b>DF:7</b>	<b>Non-state actors</b> are increasing their influence related to global security.	<b>Important Scenario Driver</b>
<b>DF:8</b>	Global and intra-regional <b>inequalities</b> are stimulating conflict potential.	<b>Important Scenario Driver</b>
<b>DF:9</b>	Information communication technology ( <b>ICT</b> ) is <b>embedding</b> itself as a crucial part of society.	<b>Critical Scenario Driver</b>
<b>DF:10</b>	<b>Social media</b> is a significant part of communication and this is expected to grow in the future.	<b>Critical Scenario Driver</b>

The integration-polarisation driving forces thus present a viable second main driving force for the creation of scenarios. The ICT embedded driving force and integration-polarisation driving force will provide four possible and feasible scenarios. (See Table 8.4 for the two key drivers creating the four scenarios.)

**Table 8.4: Final two driving forces for information warfare scenarios**

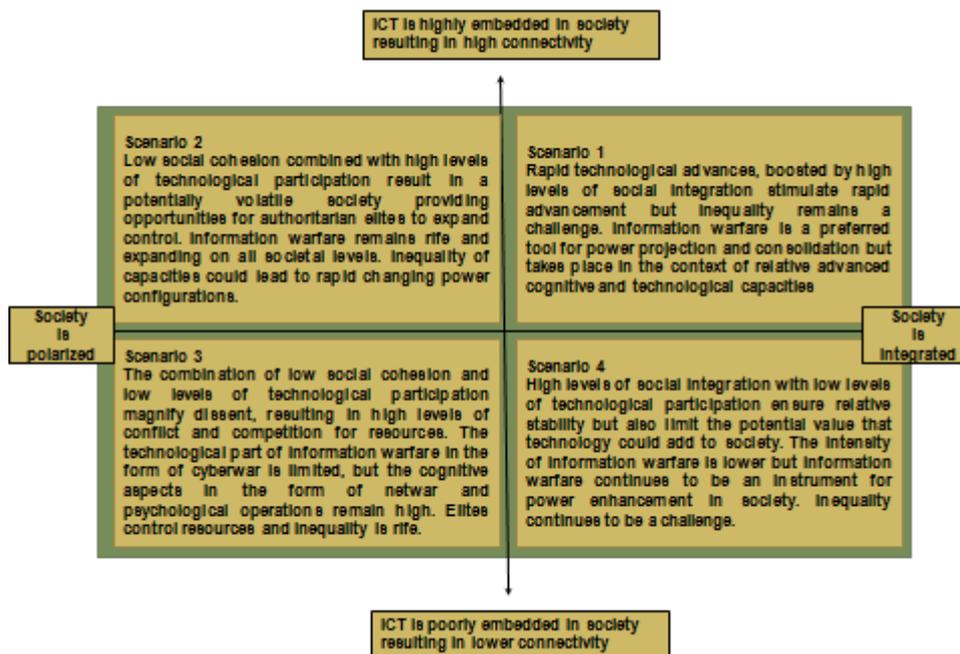
<b>Driving force</b>	<b>Specific dimension</b>
An increase in <b>integration</b> and <b>polarisation</b> will contribute to systemic stresses.	Low level of integration to high level of integration.
Information communication technology ( <b>ICT</b> ) is <b>embedding</b> itself as a crucial part of society.	Low level of ICT embedding to high level of embedding.

#### 8.11.6 Produce a basic scenario matrix

The horizontal axis of the scenario matrix embodies a spectrum measuring the level at which information communication technology (ICT) is embedding itself as a crucial part of society. The upper side of this spectrum represents an environment in which ICT is highly embedded in society resulting in high connectivity. The lower side of the axis embodies an environment in which ICT is poorly embedded in society resulting in lower connectivity. The key horizontal axis driver provides a continuum on which social technology participation by the society members are evaluated from low to high.

The vertical axis represents a spectrum measuring the level at which integration and polarisation will contribute to societal systemic stresses. The right-hand side of this axis represents an environment where society experiences high levels of integration. The left-hand side of this axis

represents an environment where society experiences high levels of polarisation. The key vertical axis driver evaluates the level of social cohesion within society between the two opposites of highly polarised to highly integrated. (See Figure 8.4 for an illustration of the scenario matrix defining the scenario possibilities.)



**Figure 8.4: Information warfare 2030s scenario matrix**

The four quadrants of the matrix each reveal a scenario for a possible future within which information warfare could manifest as a national security threat set in the 2030s. As information warfare is so ingrained in society and as it is difficult to restrict it only to South Africa the broad summary of scenarios represents a global perspective. The later full explanation of the scenarios is focussed on the South African case. The scenarios are based on how the identified ten driving forces may combine over the next decade and a half. It must be emphasised that the purpose at first is mainly structural to identify a diversity of possible scenarios based on how the most uncertain and important driving forces for the manifestation of information warfare interact over time. More detailed descriptions of these scenarios, down to the CLA levels, are presented later in the chapter.

Scenario 1 represents a technology-driven cooperative society in which information warfare is present and relevant on all levels and in all forms. Scenario 2 is a divided society in which technology empowers and entitles individuals. Information warfare is widespread and a significant part of the struggle for resources between entities and individuals. Scenario 3 represents a

polarised but also a relative technologically disconnected society in which netwar and psychological operations dimensions from information warfare are rife. Scenario 4 represents a society in which high levels of social integration with low levels of technological participation ensure relative stability. The intensity of the information warfare is lower but netwar and psychological operations continue to be instruments for power enhancement in society.

#### 8.11.7 Provide a rationale for the scenario names

This study has adopted metaphors from African traditional religion and myth for the identified scenarios with the aim to advance creative thinking about the content of the scenarios and setting it within a South Africa / Africa milieu.

Shango is from Yoruba tradition in Nigeria. As an earth deity he was once a mortal man, the king of Oyo, who transformed himself into an immortal. According to tradition, during his life he breathed tongues of fire. He then ascended into the sky by climbing a golden chain and became the god of thunder and lightning. He is also god of justice, punishing thieves and liars (Jordan, 2004:282).

**Shango Rejuvenated** illustrates a scenario in which a high level of ICT embeddedness and high levels of integration boost assimilation, cooperation and technological advancement but also provide the ideal staging area for the use of information warfare as power projection method.

Gaunab is malevolent god of darkness from the Khoi culture in Namibia. This deity is the chief adversary of the creator god Tsunigoab. He was engaged in a primordial struggle for supremacy during which Tsunigoab was wounded but eventually triumphed, consigning Gaunab to the so-called "dark heaven" (Jordan, 2004:102-103). **Gaunab Rising** does not necessarily reflect the rise of authoritarian societies but rather highlights the possible consequences of international, regional and even national polarisation in an environment in which high levels of ICT embeddedness will enhance the capabilities of the role-players involved.

Inkanyamba is a Zulu Storm god from South Africa. The deity is specifically responsible for tornados and perceived as a huge snake coiling down from heaven to earth (Jordan, 2004:139).

**Inkanyamba Reduced** reflects a polarised environment in which the embeddedness of ICT remains at a low level. Although the technological element of information warfare such as cyberwar could be constrained, high levels of potential conflict are experienced.

Tsunigoab is the creator god in the Khoi tradition in Namibia. Tsunigoab walks with a limp, because of an injury sustained in a primordial battle with his arch rival Gaunab, the god of darkness, who was eventually driven away to live in the dark heaven. Tsunigoab is invoked at dawn each day (Jordan, 2004:323). **Tsunigoab Revived** reflects a scenario in which a high level

of social, political and economic integration is achieved but this is not supported by a high level of ICT embeddedness in society overall, resulting in general stability but difficulty in maximising technological opportunities in society.

#### **8.11.8 Produce the scenarios**

The scenarios developed are stories about possible futures. Scenarios offer multiple creative pathways into a future that is basically unknown. While constrained by the rules of the game and driven by key uncertainties, they endeavour to evoke awareness and emotion in the narrative. Each scenario has a simple, vivid theme which is logically consistent, but differs from the other scenarios in the set. It provides a compelling title which ideally enters the common vocabulary of the target audience (Ilbury & Sunter, 2003:87). The outlines identified above are now turned into fully fledged scenarios focused on four possible manifestations within the TWEPS environments, namely the information warfare / national security, technology, economic, political and social environments. In order to enhance the layered view of each scenario, a CLA analysis is also done for each scenario. The scenario descriptions provided some of the litany insight into the possible scenarios. The other CLA layers are presented in Table 8.4 to Table 8.7.

#### **8.12 SCENARIO 1: “SHANGO REJUVENATED”**

The first scenario is one in which technological progress takes place in an increasingly cooperative and networked global society. This scenario is formed in the quadrant where both the two main driving forces – ICT embeddedness and societal integration – are high. This provides for a highly technological driven South African society in which the consumer and business demand for technological solutions are elevated. Information warfare is seen as a common but also practical and useful instrument for the projection of power by many entities within South Africa. In South Africa the government and other prominent local and international role-players are forcing commercial values on the country, creating a largely homogeneous landscape, with main stream diversity decreasing and some sub-cultures forced to the margins. Information warfare is regarded by many domestic but also foreign role-players as a legitimate method for dissent and conflict. The government but even larger corporate entities invest significant resources into both defensive and offensive capabilities.

##### **8.12.1 Information warfare and national security manifestation**

The high levels of social cohesion play a role in limiting both international as well as domestic conflict and war. However, competition, especially competition leading to conflict, remains common. Because of the high level of ICT embeddedness in South African society, information

warfare remains a useful as well as viable instrument of influence and power projection. The South African state continues to survive challenges against its legitimacy. However, powerful non-state entities such as corporations and ideological or religious groups continue to challenge the sovereignty of the South African state.

As interconnected high technology and especially the digital economy are central to stability and wealth creation in South Africa, society is highly vulnerable to information warfare. It also occurs on all levels and in all of its manifestations as cyberwar, netwar and psychological operations. Information warfare is regarded as a major national security issue in South Africa. It is also being developed by the government and other entities as offensive power projection tools. At the same time counter measures against threats are highly specialised and evolving fast. Networked security is seen in South Africa as of major significance and substantial resources are invested in this.

The relevance of information warfare is strengthened by the systemic nature of conflict because of the high levels of ICT embeddedness. Conflict is highly complex with growing interaction between technological change, system development and operational innovation. Within South Africa the deployment of autonomous weapons and security systems are common. Asymmetric action forms part of conflict in South Africa but is somewhat restrained because of high levels of global integration and the focus on multi-level defensive capabilities.

South Africa's multi-lateral security cooperation is strengthened and assists in the overall maintenance of order in the international system. South Africa is exposed to less inter-state conflict while the occurrence of intra-state conflict within the country is increasing in which information warfare will increasingly become the method of choice for dissent. The added value of high level anonymity provided by technology, especially with cyberwar, is also exploited by non-government institutions and the government alike. Globally the borders between military and civilian conflict weakens partly because of the proliferation of power projection opportunities brought about by information warfare options. This leads to the expansion of a technological arms race between governments and non-government groups. Despite the information warfare related challenges in general, a balance of power within South Africa as well as between South Africa and foreign competitors in terms of this phenomenon exists as counter measures are largely in place or are developed quickly.

Terrorism presents a threat in South Africa but increases in the non-physical (information warfare) part thereof. Crime and terrorism are increasingly also in South Africa been combated by way of algorithms and big data. In South Africa crime and terrorism groups use advanced technology that is basically matched by the advanced technology of the government entities opposing them. The high levels of integration in South Africa will also result in the expansion of the reach and

innovativeness of disruptive and terrorist means. The Centre of Gravity (COG) for power projection in South Africa will be strongly centred in intangibles such as the general population's morale.

### **8.12.2 Technology manifestation**

Large-scale integration of technologies takes place in South Africa economic activities as well as in daily life. This spans the globe and extends even into developing countries and communities, although at a slower pace. While both the globalising and fragmenting consequences of technology are present in South Africa, the emphasis is on the integration-related aspects. Digital networking is pervasive in South Africa. Big data is also exploited in South Africa for predictive purposes to streamline efficiency, innovation and productivity. Artificial intelligence (AI) plays a significant part in the lives of the population and the economy in general. Robotics expands beyond manufacturing in South Africa and becomes prevalent in the service sector with huge consequences for employment. Nanotechnology becomes a significant part of economic activity finding applications in most sectors.

The internet and mobile networks in South Africa are compatible and unified, while the IoT develops at full potential to link the majority of manufacturing, service and general infrastructure to the internet. South Africa is fully linked to the global ICT networks. The internet or its successor is vibrantly expanding into all realms of human life in South Africa. Technology becomes a major driver in South Africa which activates advances in education, but some inequalities continue to challenge full education for everyone. Dark Net or Deep Web grows exponentially and is a resource for South Africans for both positive and negative uses. Inequality is still an issue of concern in South Africa but technological leaps ensure continued development even in the poorer regions. Despite the high level of social cohesion South Africa remains technologically highly vulnerable to the use of information warfare as instrument for power projection and/or disruption.

### **8.12.3 Economic manifestation**

The South African economy is highly networked but significantly influenced by interdependence, automation, collaboration, integration and globalisation as major trends. Commercial values are appreciated with South African elites strongly pushing for continued innovation and global cooperation. Technological advances – especially in the fields of digital integration, IoT, AI and nanotechnology – have a significant impact on South African and global economic activity. This adds to a manufacturing revolution where additive manufacturing (3D printing) becomes common and widespread, with devastating consequences for countries and regions currently dependent on basic manufacturing. South African governmental regulation and policies are poised to promote national and global sustainable equality and stability but will face challenges in this regard partially

because it would be vulnerable to information warfare or an incapability to effectively address the ingrained problems facing the world. If not managed inclusively and effectively, these developments could have a significant negative impact on equality and consequently stability in South Africa. A potentially growing divide between the haves and the have-nots will leave many individuals in South Africa and the developing world in dire poverty.

Furthermore, the collective outcome of trends such as growing automation, digitalisation, stagnant wages, the rise of AI and globalisation potentially contributes to unemployment becoming a momentous challenge in South Africa. However, opportunities are provided by inexpensive communication technologies constructed on inexpensive processors with high computation capabilities, interconnected in a pervasive global network, for some South African marginalised individuals and communities to become part of the mainstream economy. Manipulation of symbols is expected to grow as a part of South Africa's economy. Production that is radically decentralised and nonmarket-orientated emerges at the core, rather than the periphery, especially in the more advanced economies. Focussed efforts within South Africa increase the use of alternative energy sources in South Africa, especially renewable sources, although climate changes still require long-term global efforts to address these challenges.

#### **8.12.4 Political manifestation**

Globally opposing centres of power exist but a high level of cooperation between prominent actors in the world ensures strategic stability. A shift in the balance of power in the global system occurs where collective security is becoming increasingly significant and where non-compliant states are isolated. On the strategic level, fixation on geo-political priorities shifts towards global geo-economic challenges. Multi-lateralism is vibrant and South Africa is an active participant as the levels of global cooperation is high. Processes to build legitimate global and national political entities continue to assist in ensuring stability. Dictatorships will be less viable, with democratic to benevolent authoritarian governments more successful in ensuring legitimacy. In South Africa democracy will be operational but challenges from non-state entities continuing. Because of pervasive connectivity as well as extremely high penetration of social media, the South African citizens' input on governance-related issues is high. Trends towards the implementation of multi-party democracy in many developing states strengthen local and global good governance. However, the enhanced technological capacity of governments is also a significant negative influence for non-connected minority interests in some parts of the world including in South Africa. Non-state actors capable of mobilising support are in a position to also challenge the government in South Africa. E-governance is being implemented in South Africa and spreads exponentially across the world. Big data assist both government and commercial interests in South Africa to high regulate the social order in the country. The media is owned by a few corporations in South Africa

and mostly represents the ruling elite. Diverse alternative South African and global media exists which disseminates more independent news online.

### 8.12.5 Social manifestation

As it is a highly interconnected and integrated world, social participation is high also in South Africa on many issues deemed significant in people's lives. The world of high connectivity empowers the individual to an unprecedented level in human history. This is the case because of the functioning of a pervasive knowledge network to which South Africa is fully connected. Despite this there are still limits to what marginalised individuals and groups are able to accomplish. The media is largely digital but controlled by few big players in South Africa but also globally. Independent voices are vocal but find it difficult to influence and establish traction outside the mainstream memes. However, social media and social networking are pervasive in South Africa and a key factor in managing communication as well as individual and group aspirations in society. Social openness and transparency are in general high which makes control over social media interaction by the South African government much more difficult. In South Africa as in the rest of the world social media provides a wide range of entities with significant leverage, while also ensuring that psychological operations could be used as power projection instrument through social media.

### 8.12.6 CLA evaluation of scenario "Shango Rejuvenated"

**Table 8.5: CLA assessment of the scenario "Shango Rejuvenated"**

CLA layers	Assessment
<b>Social systems and structures</b>	<p>Technology's legitimacy and usefulness are generally accepted and promoted as the main conduit of addressing the strategic challenges in society. These challenges include poverty, inequality, crime and corruption.</p> <p>Despite high levels of integration, the variety and potential ease of the deployment of information warfare ensures that it will be a significant national security risk. ICT embeddedness and innovative technology are making it possible to target higher-level decision-making entities and the management systems of opponents.</p> <p>The value of information warfare as instrument of power and finances is appreciated and fully exploited by especially the political and economic elite in society.</p>

	<p>Militaries/security entities are significant spenders on information warfare related capabilities as well as high-technology solutions in terms of drones, deep learning technology, nanotechnology, miniaturisation, swarm options, automated systems and human enhancing technologies.</p> <p>Mega-corporations pursue the multitude of opportunities to expand consumerism and fast-track the life cycles of digital gadgets to extremely profitable levels, suffocating competition and limiting the opportunities of small businesses.</p> <p>Media ownership provides opportunities to mega-corporations (and governments) to stifle freedom of speech.</p> <p>Technology provides opportunities for communication but alternative messages get drowned in the commercial market place.</p>
<b>Worldview</b>	<p>In the light of high ICT embeddedness and high levels of integration, technology is viewed as central to prosperity and progress.</p> <p>Popular views of the economy relate to integration and cooperation, and globalisation remains central to prosperity. Elites remain in a power position to manipulate this to their advantage.</p> <p>The value of social production and exchange as well as the symbolic drives innovation and growth prospects.</p> <p>Multilateral politics is appreciated for assisting to strengthen the expanding political, economic and social integration.</p>
<b>Myth</b>	<p>“Technology can overcome all problems” is the myth underlying the “Shango Rejuvenated” scenario.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

### 8.13 SCENARIO 2: “GAUNAB RISING”

The second scenario is one in which technological progress takes place in an increasingly polarised society. This scenario is formed in the quadrant where the two main driving forces –

ICT embedding and polarisation – are high. While technological progress and technological interconnectedness are high, the potential thereof cannot be realised because of divisions in society. This scenario represents a divisive world with increasing competition between societies mobilised on the grounds of status, nationality, religion and class, providing opportunities for authoritarian elites to expand control. Information warfare remains rife and its use is expanding on all societal levels. Inequality of capacities could lead to rapidly changing power configurations.

### **8.13.1 Information warfare and national security manifestation**

The nation state is paramount, but non-state entities organised on religious, ideological and national grounds do present a growing threat to national security. Full-blown information conflicts and wars are common with a mix of kinetic and non-kinetic elements. In this regard virtual cyber-based groups such as Anonymous (or its future successors) pose a major national security threat. Non-state actors regard information warfare as a primary tool to promote and advance their political agendas.

In South Africa information warfare thus poses a significant national security risk and growing ICT embeddedness ensures that states are highly vulnerable, especially to cyberwar. The level of potential hostility in South Africa ensures that all methods for promoting interests in a fairly hostile environment are used. Both terrorism and cybercrime are serious local and global threats. Information warfare is regarded as a legitimate instrument of power projection by both the elite and the dissatisfied in South Africa. The ruling elite in South Africa manipulate and force the rest of the population into submission with whatever means at their disposal. However, the marginalised are also turning to information warfare as a practical tool to pursue their interests. Conflict becomes highly complex and common with growing interaction between technological change, system development and operational innovation. Asymmetric war and conflict options are an ingrained part of conflict and war globally.

The broader global environment experiences an increase in inter-state and intra-state conflict. The threat of nuclear war will be significant as the non-proliferation system is increasingly eroded. The start of a Second Cold War is a potential risk, especially if authoritarian states expand their assertive stands and military capabilities. This leads to an escalation of an arms race with high-technology weapons and even weapons of mass destruction (WMD). Private armies (mercenaries) are significant role-players in these conflicts. Drone warfare is rife and used by many governments and even non-government role-players. The Centre of Gravity (COG) for power projection is strongly centred in hard power and control but intangibles such as the general population morale continue to be important for ruling elites.

### 8.13.2 Technology manifestation

The levels of trust between government and the civil society in South Africa are low despite high levels of technological development and embeddedness of ICT in society. The potential for cooperation supported by high levels of technological participation is actively hindered by hostility in the form of disruptive policies and low levels of trust between opposing elites. Alternative systems and even separate cyber infrastructures are created in South Africa and globally, resulting in the development of physical and cyber enclaves for the elites. This leads to a fragmented mobile network and internet, which have serious negative consequences for the further development of technology. Fragmentation can occur inside South Africa as well as with connectivity outside the country. IoT technologies function in South Africa but do not reach their full potential because global entities are reluctant to cooperate and agree on common standards.

The government and elites actively endeavour to control digital networking and to keep it largely restrictive. However, the Deep Web provides alternatives without control being an absolute. Ultra-regulated digital and physical fortresses are maintained in South Africa, while outside of these a general “free for all” reigns (despite efforts to regulate it). Big data is not exploited to its maximum potential, curbing the effectiveness of future technological innovation. Big data is, however, exploited by the government and corporates to expand control over the population. Robotics expands beyond manufacturing but with limited global cooperation, it is not such an enormous threat to jobs in South Africa. Nanotechnology becomes a part of economic activity in South Africa finding applications in many sectors, including the defence sector. Globally the pressure to deploy nanotechnology for military purposes is high, increasing the security and safety risks of these technologies substantially. The defence sector is growing in South Africa with military spending increasing. Technology is a driver in the South African economy but lack of global cooperation inhibits its potential influence. Inequality is still a global issue. However, the hope that technological leaps will help to overcome this inequality does not gain much traction in South Africa and elsewhere.

### 8.13.3 Economic manifestation

Despite high levels of technology participation, the South African economy is constrained by decisions which place interdependence, collaboration and globalisation under pressure. Globally large-scale economic competition takes place rather than cooperation, especially across the international divides. High levels of polarisation result in obstacles being created which limits the integration of the global economy. This creates a new multi-polar world with a dramatic increase in the diversity of cultures, religions, worldviews, economies, political regimes and legal systems but within a polarised framework. In general, the economy is not so vulnerable to information warfare,

but the South African economy faces many other challenges. Elites are successful in creating enclaves of haves while the have-nots remain marginalised. Tariff barriers and other trade impediments hamper global trade.

Globally, the middle classes are under pressure while many individuals in the developing world continue to live in dire poverty. This also manifests in South Africa. The global economy has no incentives for the promotion of sustainable equality and stability, worsening the already polarised environment. Cheap communication technologies are available and in use in South Africa but the economic value remains constrained. Global trade and cooperation are constrained by government/corporate impediments and controls. The manipulation of symbols is not a significant part of the South African economy. The main source of energy will be fossil fuels although alternative energy sources are extensively used in parts of the world.

#### **8.13.4 Political manifestation**

Technological participation is not reflected on the political level as opposing centres of power are rising, resulting in conflict rather than cooperation. Globalisation is stunted. Large-scale political competition is the norm and also manifests in South Africa. Conflict increases domestically as well as internationally. Strategic geo-political priorities remain prominent while conflict in addressing geo-economic challenges increases. Multi-lateralism is under pressure, resulting in poor collective action on issues such as climate change, non-proliferation of WMD, arms control, free trade and the creation of global norms on shared global policy challenges. A shift in the balance of power in the global system takes place where the balance of power is becoming increasingly significant and backed up by “hard power”.

Information warfare is regarded as a significant instrument for power projection. The nation state is strengthened but increasingly in conflict with other entities. The state will not be the only actor with significant power projection capabilities, and a power balance between state and non-state entities exists in some parts of the world. In South Africa non-state role-players prove to be seriously disruptive and influence national security negatively. In South Africa there are dominant digital political actors of which the government is not necessarily the most significant. Efforts to implement e-governance, especially in the developing world including South Africa, are struggling. Setbacks will occur for multi-party democracy in many developing states while global good governance decreases in parts of the world. It is difficult to build legitimate global and national political entities. Independent media continues to exist in South Africa but its influence on political processes is limited.

### 8.13.5 Social manifestation

While the South African society is interconnected, it is prone to conflict because of high levels of polarisation. The potential for a pervasive knowledge network is high in South Africa but it is not functioning optimally. Social participation in South Africa is high but disruptive and controlled. The government and corporate entities in South Africa increase efforts to control media and social media. In the developing world this control is mostly for political reasons while in the developed world it is mostly for commercial reasons. Control of social media interaction by the government is much more difficult but provides other entities in South Africa with significant leverage. Social media and social networking are largely fragmented. In general, social openness is low. Mass protests and rioting in many parts of the world including South Africa are common. Global migration is a major issue and some countries take harsh measures against migration. Psychological operations are used by many entities and undermine media freedom.

### 8.13.6 CLA evaluation of scenario “Gaub Rising”

**Table 8.6: CLA assessment of the scenario “Gaub Rising”**

CLA layers	Assessment
<b>Social systems and structures</b>	<p>High levels of polarisation coupled with the variety and potential ease of deploying information warfare ensures that it will be a major national security risk.</p> <p>The struggle for resources as well as profits in the economy is increasingly regarded as a zero sum game, triggering even more polarisation.</p> <p>Political, economic and social diversity are extensively used by the elites as popular mobilisation tools breeding even more polarisation.</p> <p>Power is viewed to be attained by mass mobilisation and not through reconciliation by way of utilising highly networked ICT capacities.</p> <p>The ruling elites and influential entities value the use of fear and exclusion as tools to establish and strengthen legitimacy.</p> <p>The themes for political mobilisation include nationality, race,</p>

	<p>religion, social status, educational level, technological proficiency and wealth.</p> <p>The power of mega-companies, especially technology companies, is not limited by governments, which leads to these companies playing a significant governance role. In a polarised environment this supercharges conflict and conflict potential.</p> <p>Technology is regarded as an instrument of power and it is playing a subservient role in addressing the many societal challenges.</p> <p>Information warfare is recognised as a crucial instrument of power, and fully exploited by especially the political and economic elite in society for these purposes.</p> <p>Highly controlled and fragmented global media is used to prop up their owners' positions in a polarised environment.</p>
<b>Worldview</b>	<p>In the light of high ICT embeddedness and high levels of polarisation, technology is viewed as central to power and control as well as defence against other centres of power. In order for the various centres of power to enhance their positions, economic mercantilism remains a preferred economic activity.</p> <p>The value of social interaction is regarded as a threat by the power elites. Significant effort is expended to control the social interaction and the narrative but this proves to be highly problematic in a highly connected environment. High levels of polarisation result in a fragmented, divisive and conflict-prone social environment.</p> <p>Politics is highly divisive with multi-lateralism under huge pressure and even being reversed in certain cases.</p>
<b>Myth</b>	<p>"Technology is able to provide the power to ensure sectarian interests" is the myth underlying the "Gauteng Rising" scenario.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a)

## **8.14 SCENARIO 3: “INKANYAMBA REDUCED”**

The third scenario is one in which polarisation is high while technology participation is low. This scenario is formed in the quadrant where the ICT embedding is low but polarisation is high; magnifying dissent, resulting in high levels of conflict and competition for resources. The technological part of information warfare in the form of cyberwar is limited, but the cognitive aspects in the form of netwar and psychological operations remain high. Elites control resources and inequality is widespread.

### **8.14.1 Information warfare and national security manifestation**

The potential for general anarchy is a significant national security risk resulting in security being a major but also expensive reality in South Africa as well as in many other countries. In most cases, only the wealthy in South Africa can afford security. The use of information warfare (especially netwar and psychological operations) is widespread. In general, the mix of kinetic and non-kinetic elements in war and conflict is common. Asymmetric war and conflict options form an ingrained part of conflict and war globally, although it is not as technology driven as it could be. Inequality leads to conflict and unrest in South Africa. Conflict about resources is common and hybrid warfare is widespread worldwide. The global non-proliferation system collapses and increases the possible use of WMD substantially. An arms race between states and even in some cases non-state entities are a reality.

The nation state including South Africa is under pressure as non-state entities organised on religious and ideological foundations assert alternative and hybrid configurations. Ultra-regulated digital and physical fortresses are maintained in South Africa, while outside of these a general “survival of the fittest” mind-set reigns. Private armies (mercenaries) are significant role-players in security as well as in the conduct of conflict. The Centre of Gravity (COG) for power projection will be strongly centred in hard power and control but also in intangibles such as the general population morale.

### **8.14.2 Technology manifestation**

Technological progress and innovation in South Africa are seriously under pressure and limited to “small islands of prosperity” in large areas of serious want. Developing societies are especially affected, which limits options for technological innovation. Global inequalities and socio-economic challenges are reflected on the technological level. Digital and network capabilities are restricted in South Africa with exponential growth drivers such as the IoT not functioning because of economic,

political and social challenges. Big data plays practically no role in the economy or society in South Africa. Elements of it might be used by elites to advance their own interests. Although a basic internet continues to exist worldwide, increasingly value-added content is only accessible to elites. The Deep Web is also fractured but its significance grows as it is established at the core of significant security, social and economic problems and competition. Robotics is limited to the enclaves in South Africa where elites live and is exclusively used to the advantage of these elites.

### **8.14.3 Economic manifestation**

The South African economy is constrained by high levels of conflict and a general lack of ICT embeddedness. Mutually exclusive economic competition is rife in South Africa and elsewhere while cooperation, especially over the global divides, diminishes. High levels of polarisation result in obstacles being created that limit the integration of the South African economy in the global economy. A divisive, multi-polar world rises in which the diversity of cultures, religions, worldviews, economies, political regimes and legal systems are celebrated and promoted to the exclusion of minorities and “the Other”.

The South African economy is not that vulnerable to information warfare, but the economy faces serious challenges. Inequality is a very real problem with elites creating wealthy enclaves, separate from the rest of the population. The poor is marginalised and paths out of poverty are limited. The middle classes' position is under extreme pressure in South Africa. Tariff barriers and other trade impediments hamper global trade. In marginalised economies globally slave labour will be common. Cheap communication technologies are available but the use thereof by especially marginalised groups is hampered by lack of ICT embeddedness. The manipulation of symbols is not so significant. The main source of energy in South Africa is fossil fuels, with renewable energy of lesser significance.

### **8.14.4 Political manifestation**

The political environment in South Africa is characterised by conflicting rather than cooperative behaviour. Globalisation's influence is actively being rolled back in South Africa with insular policies being adopted by the government and prominent political actors. In general, the South African elites are empowered by security forces while the rest of the population have limited access to high-level security. Multi-lateralism ceases to produce legitimate international treaties resulting in the global rule-making system to break down. No inclusive international actions in terms of climate change, non-proliferation of WMD, arms control and free trade can take place.

Hard power used within a system striving for a balance of power is underpinning political behaviour both internationally and domestically. Information warfare (especially netwar and psychological operations) is regarded as a significant instrument for power projection. Cyberwar plays a more subdued role because of the lower levels of ICT embeddedness in society. Non-state actors are significant in the political system in South Africa. Because of the high levels of polarisation non-state actors are also seriously disruptive influences in South Africa and elsewhere. In some parts of the world the nation state is under pressure as religious and ideological groups mobilise marginalised communities. E-government and governance are under stress in South Africa and collapse completely in some regions. Multi-party democracy is reversed in many developing states. The independent media's influence on political options is limited in South Africa as most media outlets become involved in distributing mainly propaganda for the opposing elites.

#### 8.14.5 Social manifestation

Low levels of social cohesion and technological participation make South Africa's society extremely prone to conflict and consequently the negative social outfall thereof. A pervasive knowledge network is not functioning optimally in South Africa. Social media and social networking are fragmented in South Africa because of the low levels of ICT embeddedness and high levels of polarisation. Mass protest and rioting are common in South Africa. Global migration is a major issue and some countries take harsh measures against migration. Psychological operations are rife which undermines media freedom in South Africa.

#### 8.14.6 CLA evaluation of scenario "Inkanyamba Reduced"

**Table 8.7: CLA assessment of the scenario "Inkanyamba Reduced"**

CLA layers	Assessment
<b>Social systems and structures</b>	<p>The use of information warfare (especially netwar and psychological operations) is widespread because of the high levels of polarisation. Lower levels of technology participation put limits on the effectiveness of cyber warfare.</p> <p>Hard power use is very attractive to elites by means of controlling natural resources, food and military might.</p> <p>Mega-corporations focusing on the technology</p>

	<p>field are limited and constrained by regulation and control.</p> <p>Group forming is focused on nationality, race, religion, social status, educational level and wealth.</p> <p>The struggle for resources is a major motivator in governance environment.</p>
<b>Worldview</b>	<p>In the light of low levels of ICT embeddedness and high levels of polarisation, technology is viewed as an instrument to promote interests because the polarised nature of society is significantly limited in what it can achieve.</p> <p>Popular views of the economy are closely associated with a struggle to survive mentality. The economy is regarded as primarily for the advancement of the group and its elite, with common good approaches being side-lined.</p> <p>The value of social interaction is regarded as a threat outside the power elites. Significant effort is expended in controlling the social interaction and the narrative. High levels of polarisation result in a fragmented and divisive social environment.</p> <p>Politics is highly divisive with multi-lateralism under huge pressure and even being reversed in certain cases.</p>
<b>Myth</b>	<p>“Protection of sectarian interests needs total mobilisation against the Other” is the myth underlying the “Inkanyamba Reduced” scenario.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

## **8.15 SCENARIO 4: “TSUNIGOAB REVIVED”**

High levels of social integration with low levels of technological participation ensure relative stability but also limit the potential value that technology could add to society. This scenario is formed in the quadrant where societal integration is high and ICT embeddedness is low. Levels of information warfare are lower but information warfare continues to be an instrument for power enhancement in society. Inequality continues to be a challenge.

### **8.15.1 Information warfare and national security manifestation**

The South African government remains paramount while non-state entities organised on religious, ideological and ethnic grounds do present some level of threat to national security. Information war is part of the power projection instruments available to state and non-state role-players. Cyber warfare's significance, however, is diminished by the lack of ICT embeddedness in society. Asymmetric threats and operations form part of conflict but are restrained because of high levels of global integration. These threats and operations are disruptive when they occur. The threats associated with global conflict types, such as nuclear war, are less significant as the multi-lateral system is more robust as a result of the high levels of international cooperation that are maintained. Global and national conflict continues but the risk of serious escalation is lower. The start of a new global Cold War is unlikely. Terrorism remains a threat but counter measures are more coordinated in this more cooperative global environment. The Centre of Gravity (COG) for power projection is partly centred on soft power.

### **8.15.2 Technology manifestation**

Technological progress and innovation are under pressure in South Africa because of the low levels of ICT embeddedness. Developing areas in particular are negatively affected, limiting options for technological innovation. The internet is operating and assists in cooperative endeavours but is not fully integrated into the centre of the global e-commerce as technological cooperation between individuals is more limited. The IoT is functioning in South Africa but limited in significance because of low levels of technology embeddedness. Technological advances are more focused on productive issues and less on consumer items. Big data is not used optimally in South Africa because of lower levels of technological participation. Global inequalities and socio-economic challenges are reflected on a technological level. Although the internet continues to exist, its influence on the broader economy is inhibited because of lower levels of ICT embeddedness. The Deep Web is on the margins of society and is mainly linked to criminal-related activities. Robotics' role is more limited in South Africa and mainly stays within the manufacturing sectors.

### **8.15.3 Economic manifestation**

Global inequality continues to exist despite high levels of cooperation potential. Technology is not sufficiently developed in South Africa to maximise the opportunities brought about by the high levels of social cohesion. The South African economy is cooperative with a focus on interdependence, collaboration, integration and globalisation as trends. Integration with the global economy is progressing but not at optimal rate. Commercial interests in South Africa are competitive while innovation is more limited because of lack of effective ICT cooperation. The South African economy is not so vulnerable to information warfare while facing other challenges such as persistent inequality. Inequality continues to persist in the country but it is difficult to find solutions as innovation is not sufficient for these purposes. Unemployment is a problem in South Africa but not a crisis. The South African economy is still dependent on fossil fuel as main energy resource. However, the significance of alternative energy resources in South Africa grows.

### **8.15.4 Political manifestation**

Political cooperation is paramount in South Africa but its full potential is not realised as society is not sufficiently networked. Collective security is prioritised in a global environment where multi-lateralism is generally respected and regarded as a practical and dependable way of organising and managing relations. The building of legitimate global and national political entities continues. Shifts take place towards multi-party democracy in many developing states while efforts continue to strengthen national and global good governance. Globalisation is continuing but not at full potential. E-government and good governance are promoted in South Africa but are limited in effectiveness because of the lack of ICT embeddedness. Globally the nation state continues to be prominent. Non-state actors are prominent role-players in South Africa and elsewhere but do not create significant system problems because of the high levels of social cohesion. The media in South Africa is in a position to have some influence on political processes.

### **8.15.5 Social manifestation**

South African society is interconnected but cannot reach its full potential as the expected cooperation cannot be achieved on technological level. The pervasive knowledge network in South Africa is not functioning optimally. While social openness in the country is high, social media and social networking is common. South African media is mostly free and fulfils a key role in society. Social participation in South Africa is high but not to its full potential because of technological constraints. The quality of life is relatively high for most in the South African society, although inequality persists..

## 8.15.6 CLA evaluation of scenario “Tsunigoab Revived”

Table 8.8: CLA assessment of the scenario “Tsunigoab Revived”

CLA layers	Assessment
<b>Social systems and structures</b>	<p>The use of information warfare (especially netwar and psychological operations) is somewhat more limited because of the high levels of integration. Lower levels of technology participation put some limits on the effectiveness of cyber warfare.</p> <p>Despite this, information warfare (especially netwar and psychological operations) is still regarded as a useful instrument of power by the political and economic elite in society.</p> <p>Larger corporations continue to be focussed on the technology field but are limited by lack of effective global interaction and technological constraints..</p> <p>Smaller companies and communities are taking the lead to create localised interaction.</p>
<b>Word view</b>	<p>In the light of low levels of ICT embeddedness and high levels of integration, technology is viewed as an instrument to promote interests. However, the influence of technology remains limited as a result of low levels of participation in technologies.</p> <p>A market-related approach to economic activity is regarded by governing elites as a viable approach to support mutual advancement. The lack of full technological participation, however, inhibits the possible positive economic consequences thereof.</p>

	<p>The value of social interaction is acknowledged. However, the full utilisation of this potential through options provided by ICT embeddedness lacks.</p> <p>Multilateral politics helps to strengthen expanding political, economic and social integration.</p>
<b>Myth</b>	<p>“Local integration and pursuance of shared values ensure global harmony” is the myth underlying the “Tsunigoab Revived” scenario.</p>

Source: Own compilation based on CLA levels (Inayatullah, 2008a).

## 8.16 CONCLUSION

Based on the outcome of the scenario exercise, information warfare will manifest as a national security threat by the 2030s in all possible scenarios. However, the significance of information warfare and the manifestation of its three components differ in each scenario. In both “Shango Rejuvenated” and “Gaunab Rising” information warfare is a major national security threat. In the case of “Shango Rejuvenated” this can be regarded as counter-intuitive as high levels of ICT embeddedness and social integration result in the most economically advanced scenario. However, in such a scenario advanced cognitive and technological capacities empower significant political actors – both governmental and non-state – to use information warfare as a preferred tool for power projection. In “Gaunab Rising”, information warfare could be somewhat inhibited in terms of potential success because polarisation is leading to much lower levels of trust in society. Although the interest in using information warfare is high in “Inkanyamba Reduced”, the low levels of ICT embeddedness and high distrust in society inhibit the successful employment thereof. In the “Tsunigoab Revived” scenario the high levels of integration combined with the lower levels of technology participation limit the practical threat posed by information warfare to society.

In Chapter 9 propositions are identified and applied to the plausible information warfare threat against South Africa in the 2030s

## CHAPTER 9

### EVALUATION

#### 9.1 SUMMARY

In an age where information is increasingly positioned at the centre of society, a future in which information also becomes a security liability is a reality for South Africa and the world at large. Information in all its manifestations – from data to wisdom – has been central to institutional power since the dawn of humankind. Technological efficacies brought about by the digital revolution and enhanced global networking activities have boosted the role of information in national power. Technological development catapulted information to the centre of most human endeavours, although high levels of inequality persist as manifested in the digital divide.

In this study the aim was to use multi-disciplinary theory from futures studies and especially international relations in conjunction with methodologies from mainly business studies and futures studies (environmental scanning, causal layered analysis, a Delphi method and a scenario study) to develop plausible futures regarding the potential threat that information warfare will pose to South Africa by the 2030s.

The problem statement focused on the manifestation of information warfare as a national security concern in South Africa during the 2030s. A multi-disciplinary approach, supported by futurist methodologies, proved to have the capacity to create knowledge addressing this problem statement.

Plausible scenarios on how information warfare will manifest as a national security concern in South Africa during the 2030s have been identified. Based on the results of this study, propositions are also identified applicable to plausible information warfare threats against South Africa in the 2030s.

In answering the research problem sub-problems were formulated and studied in depth.

##### 9.1.1 Sub-problem outcomes

In Chapter 2 the following sub-problems were dealt with: *What is the epistemological approach followed in this study and how does theory provide insight into information warfare as an upcoming national security threat?*

The study followed critical realism as epistemological approach. Information warfare is a new concept that has not been adequately addressed in current social science theoretical frameworks and it is closely linked with global power projection. Hence, in this study, information warfare was mainly framed within international relations theory. Overall, the philosophical approach in this study was a critical realist approach. Critical realism accepts the sceptical belief that humanity cannot have certain knowledge. Thus, knowledge can be regarded as justified true belief. Despite this,

critical realism is not abandoning efforts to understand and know. Knowledge is redefined as “conjectural knowledge”, allowing for the possibility of the fallibility of its conjectures. In this study foresight acts to promote knowledgeability and as such operates as a “higher-order” language.

International political theoretical worldviews provide theoretical insights into the broader environment in which information warfare is currently manifesting as a national security threat. The worldviews according to realism, rationalism, critical realism in international relations theory, critical security studies and postmodernism offer comprehension regarding diverse issues relevant to information warfare. These issues include shifting global power, network security, system integration, the role of symbolism, as well as non-state actors in the international system.

The realists’ worldview has a high regard for the value of national security, state survival, and international order and stability. Realists in general believe that there are no international obligations in the moral sense of the word (i.e. bonds of mutual duty) between independent states. Information warfare can thus be added to the realist’s existing assortment of power instruments. While this dimension has been part of the traditional power instrument in the past, it can be expected that its growth in scope, its sophistication and its role in information networked systems will increase significantly in the future.

The rationalist’s worldview acknowledges the existence of an international society sustained by the role of growing international interdependence and integration as an actuality closely interlinking states globally. Cooperation between states dealing with national security related issues is part of this worldview while at the same time the scope of national security threats is expanding to include issues such as environmental and human security. The challenge remains the intangible nature of information warfare which significantly complicates efforts to address the possible containment of information warfare on a multi-lateral level.

Critical realism in international relations theory and postmodernism provides some insights into the significance of the manipulation of the global information sphere. This has highlighted *inter alia* the influence of symbolism and networking to existence in today’s society. Opportunities are being created for information warfare to exponentially grow from a still upcoming issue in terms of national security to a substantial national security threat in the future.

The international political theoretical worldview provides a framework within which information warfare is currently manifesting as a national security threat. These insights are, however, also linked to the macro-historical environment. During the Industrial Age realism was closely linked to the Cold War global political stand-offs, while rationalism focused on efforts to expand international political and economic relations within the global community (Smith, 2013:4). Information Age concerns, as described by critical realism and postmodernism, reflect increased diversity, inconsistency and contradictions in human activity. These Information Age related theories highlight some trends relevant in human activity, namely renewal, relationship shifts, continuous modernisation, growing complexity and interconnectness. The dominance of any one theory is the

result of a prior assumption about the main issues in world politics that need explaining. However, all of these worldviews add value to the understanding of the broader framework within which information warfare manifest as a national security threat. Furthermore these worldviews are not representing completely mutually exclusive perceptions about international relations and security but are highlighting diverse insights regarding the role of information warfare in international security relations.

In Chapter 3, the second sub-problem was unpacked: *What is futures studies' contribution in providing insight into the future of information warfare?*

Information warfare is a subject intimately linked to the future because it is closely related to technology futures as well as the changing manifestation of warfare and conflict. Futures thinking is based on three interrelated inquiries into the future with the objective to create broad awareness about the future. These inquiries are measuring the future to obtain knowledge about the future; imagining the non-existing future; and purposefully designing or making the future. Measuring, imagining and making sustainable alternative futures should be the preferable outcome of holistic futures thinking and requires active interventions to realise (Spies, 2015). In this study, the focus was on the measuring and imagining dimensions, but it also provided insight regarding the design of countering information warfare futures. Thus, a futurist perspective does not entail prediction of the future. Instead, it strives to provide insight and foresight with the aim to promote knowledgeability which could assist in creating a preferable future.

The future is not specified or prearranged. A multitude of futures are possible but only one can manifest in the end. Futures studies promotes enquiry into how current activities (or lack thereof) will become the reality of the future. This includes endeavours to analyse the causes, sources and patterns of stability and change with the intention to create foresight and even different futures.

The relationship between society's entities, their environments and the central driving forces are sources of complexity and interdependence. These challenges are even more acute when possible and plausible futures are investigated. Using a systems approach is practical and provides an instrument for discovering the dynamics applicable when information warfare as future national security threat is studied. A system is a discernible whole that interacts purposefully with its environment and is comprised of interacting and interrelating parts that are organised for a specific purpose. Constant change is maintained by connections being established and broken within and among systems.

Effectively managing a system is done by visualising the possible futures by means of a futures map, which provides a conceptual frame for futures-related research. As extremely swift changes cannot be predicted and may be considered random, the focus of futures studies is mainly in the complex field. As the futures of information warfare largely fall within this complex field, the framework provided by the futures map assists in managing such complexity.

An additional method to manage the intricacy is by following a layered approach, which takes into account the vertical complexity of systems. The futures-orientated layered approach that was used in this study is CLA which consists of four levels of knowing: the litany, social causes, discourse/worldview and myth/metaphor levels of knowing. By moving up and down these layers, it is possible to integrate analyses, and synthesise and horizontally integrate discourses, ways of knowing and worldviews, thereby increasing the depth of the analysis.

Chapter 4 deals with the third sub-problem, namely: *What do the concepts information warfare and national security represent?*

Although information warfare is a recent concept that has only been used since the early 1990s, diverse and sometimes even contradictory definitions of information warfare have complicated study of this phenomenon. Existing definitions of information warfare have limitations. These are related to being too expansive or purely focusing on USA military-centric definitions, and lastly being limited or largely limited to attacks on the ICT infrastructure and capacities of countries and/or entities.

In this study, information warfare was defined as the manipulation of networking communication by entities with the aim to influence power relationships between countries and the state's governing capacity. Information warfare is taking place on a cognitive-technological continuum. Within the cognitive sphere information warfare manifests as netwar and psychological operations. Within the technological sphere information warfare manifests as cyberwar.

As information warfare can occur on all levels of society, its actions have implications for the security of the state. A range of information warfare fundamentals has been identified. As many of these fundamentals are related to the mind space and cyberspace environment within which information warfare takes place, these are new and provide a new dimension to power projection and security-related activities. With national security defined as the application of national will by the state with the aim to create an environment in which the country's population, state structures, territorial integrity and sovereignty are protected, information warfare presents a plethora of potential threats and risks to the modern state. The Information Age has a significant influence on national security. The contemporary challenge now is how to meet national security needs in this new and ever-changing technology environment.

The fourth sub-problem is dealt with in Chapter 5: *How does information warfare manifest in the current environment taking into account factors influencing its future manifestation in the 2030s?*

An environmental scan was used to evaluate the current milieu within which information warfare manifests with the capacity to also provide some level of insight into the driving forces which will influence how it might manifest in the future. The environmental scan focused on events, developments and manifestations related to information warfare and national security within the Technological, War/Conflict, Economical, Political and Social (TWEPS) macro-environmental

hexagon. This multi-disciplinary environmental scanning focuses on literature with the aim to identify current manifestations and to recognise possible trends and driving forces flowing from this.

Transformation, networking and the impact of technological innovation in all the environments investigated were highlighted as central to the manifestation of information warfare currently as well as in the future. These trends influence not only the entities involved in power relations in society, but also enhance the potential influence and power of small and marginalised entities in society. New forms of network-related actions such as the rhizome phenomenon (small, highly interconnected networks) using social network phenomena for cyber mobilisation have been identified as of particular use for information warfare in the future.

When taking into account the security dimension in terms of potential information warfare targeting, a wide range of pillars supporting the information society could become potential information warfare targets. The key vulnerable access points include factors underlining the networking, coordination, integration, compatibility and connectivity of the information and knowledge society.

Based on an evaluation of the recent manifestation of information warfare, it is concluded that practically all recent conflict situations have had an information dimension. While information warfare enhances military power, especially in developing countries, it also creates new vulnerabilities. It can be assumed that this trend will continue and that nearly all future conflict situations will have an information warfare dimension.

Social media and internet/mobile device platforms for such media empower most net-enabled individuals with an interest in participating in practically any global issue. This has created platforms for involvement and participation in social and political issues on a level never seen before in the history of humankind. Increasingly, it does not matter what the majority's view on issues are; it matters more what the majority of empowered individuals are doing.

In Chapter 6 the fifth sub-problem was articulated: *How can the output of the environmental scan be processed to assist in providing foresight into the future manifestation of information warfare as a future national security threat?*

Thematic qualitative text coding of the environmental scan output was done to open up the text for evaluation and the identification of the trends influencing information warfare futures.

The summative essence-capturing categories were identified as innovation, networks and transformation, which represented the three cross-cutting main trends identified from the environmental scan. Sub-categories were also identified, which are useful in the development of scenarios on how information warfare will manifest as a national security threat by the 2030s.

Grounded in data, a model was developed to produce the knowledgeability that brings about insight and eventually foresight regarding information warfare futures. Modelling is a visualisation and mental tool developed to add value to the analysis of the environmental scan output.

The model was constructed from three different but related constructs, namely the futures map, environmental scanning and CLA. The data collected during the environmental scan, which was coded in terms of the thematic qualitative text analysis method, led to the identification of three categories and thus also the main trends. Driving forces related to the manifestation of information warfare were collated in this study from the CLA-based strategic evaluation of factors potentially influencing the future. Eleven such driving forces were identified as issues which can precipitate shifts within society so immense that they cause other significant shifts in the context of the role of information as instrument of power.

The sixth sub-problem was dealt with in Chapter 7: *What are the main driving forces which will influence the shaping of the future of information warfare as a national security threat?*

The value of the identified driving forces is increased when the driving forces are scrutinised, integrated, prioritised and validated by panels of global and local experts knowledgeable about information within the TWEPS environments. For this purpose two Delphi studies were conducted as the most appropriate method for arriving at an expert validation and consensus on the key driving forces impacting the manifestation of information warfare as a national security threat by the 2030s.

Two separate Delphi studies were conducted. The one Delphi study used South African security experts while the second Delphi study used both domestic and international experts (knowledgeable in one or more TWEPS environments). Input from a multi-disciplinary pool of experts enhanced the value of the analysis already done during the environmental scan and also provided some additional input and insight to the development of scenarios.

The two Delphi studies refined and validated the ten most significant drivers influencing the manifestation of information warfare as a national security threat in the 2030s:

- The centre of power is shifting from the traditional developed countries to the developing countries.
- Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.
- An increase in integration and polarisation will contribute to systemic stresses.
- Information warfare will become a growing option for power projection.
- Symbolic, information-related phenomena are increasingly impacting behaviour.
- The speed of change is increasing exponentially with global communication becoming instantaneous.
- Non-state actors are increasing their influence related to global security.
- Global and intra-regional inequalities are stimulating conflict potential.
- Information communication technology (ICT) is embedding itself as a crucial part of society.

- Social media is a significant part of communication and this is expected to grow in the future.

The seventh sub-problem was explored in Chapter 8: *What are the plausible scenarios in which information warfare would manifest as a national security threat for South Africa?*

The two most significant driving forces for scenario building were obtained by combining the prioritisation of the Delphi studies and a cross-impact study. These two key drivers were:

- An increase in integration and polarisation will contribute to systemic stresses.
- ICT is embedding itself as a crucial part of society.

The horizontal axis of the scenario matrix represented the spectrum measuring the extent to which ICT is embedding itself as a crucial part of society. The upper side of this spectrum represented an environment in which ICT is highly embedded in society resulting in high connectivity. The lower side of the axis represented an environment in which ICT is poorly embedded in society resulting in lower connectivity. The vertical axis represented a spectrum measuring the extent to which integration and polarisation will contribute to societal systemic stresses. The right-hand side of this axis represented an environment in which society experiences high levels of integration. The left-hand side of this axis represented an environment in which society experiences high levels of polarisation. The following South African scenarios were created:

#### Scenario 1: "Shango Rejuvenated"

Rapid technological advances, boosted by high levels of social integration, stimulate rapid advancement while inequality remains a challenge. Information warfare is a preferred tool for power projection and consolidation. This takes place in the context of relatively advanced cognitive and technological capacities.

#### Scenario 2: "Gaunab Rising"

Low social cohesion combined with high levels of technological participation result in a potentially volatile society providing opportunities for authoritarian elites to expand control. Information warfare remains rife and is expanding on all societal levels. Inequality of capacities could lead to rapidly changing power configurations.

#### Scenario 3: "Inkanyamba Reduced"

The combination of low social cohesion and low levels of technological participation magnify dissent, resulting in high levels of conflict and competition for resources. The technological part of information warfare in the form of cyberwar is limited, but the cognitive aspects in the form of netwar and psychological operations remain high. Elites control resources and inequality is rife.

#### Scenario 4: “Tsunigoab Revived”

High levels of social integration with low levels of technological participation ensure relative stability, but also limit the potential value that technology could add to society. Levels of information warfare are lower but information warfare continues to be an instrument for power enhancement in society. Inequality continues to be a challenge.

Information warfare manifests as a national security threat by the 2030s in all four identified plausible scenarios. However, the significance of information warfare for national security and the manifestation of its three components differ in each scenario. In both “Shango Rejuvenated” and “Gaunab Rising” information warfare is a major national security threat. In the case of “Shango Rejuvenated” this can be regarded as counter-intuitive as high levels of ICT embeddedness and social integration result in the most economically advanced scenario. However, in such a scenario advanced cognitive and technological capacities empower governmental and non-state political actors to use information warfare as a preferred tool for power projection. At the same time, information warfare could be somewhat inhibited in terms of its potential success in “Gaunab Rising” because of the much lower levels of trust in a polarised society. Although the interest in using information warfare is high in “Inkanyamba Reduced”, the low levels of ICT embeddedness and high distrust in society inhibit the successful use thereof. In the “Tsunigoab Revived” scenario, the high levels of integration coupled with the lower levels of technology participation limit the practical threat posed by information warfare to society.

## 9.2 PROPOSITIONS

The last question remains: *What propositions can be identified applying to the plausible information warfare threats against South Africa in the 2030s?*

The formulation of the propositions is done from the viewpoint of endeavouring to find commonalities between the different information warfare scenarios. The specific scenarios in which the propositions could be valid are identified after each proposition. Although the propositions focus on South African situations similar to the scenarios, the perspective is applicable globally. Information warfare as national security threat is so ingrained in global society that it is difficult to only restrict these propositions to South Africa.

### Proposition 1

*Information warfare will be a national security threat of note by the 2030s.* This will be case irrespective of which scenario or combination of scenarios would emerge in South Africa by the 2030s. All driving forces identified in this study are empowering information warfare as a significant method to promote and protect power in society. As networked relations are growing, security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven. At the same time embedded ICT is expected to play a crucial role in the functioning of society and will be a significant driver of future economic activity. Additionally,

the speed of change will increase exponentially with global communication becoming instantaneous and cheap. Social media will form a significant part of communication and it will become an influential socio-political and economic force in South African society.

- Scenarios in which this proposition could be valid: “Shango Rejuvenated” and “Gaunab Rising”, somewhat more restrained in “Inkanyamba Reduced” “Tsunigoab Revived”.

### **Proposition 2**

*Multi-lateral measures would be ineffective to control information warfare.* Many of the challenges that the world faces can be countered (even if only partially) by collective and multi-lateral rule making. International society creates an image of states articulating and agreeing upon rules, based upon their mutual recognition as sovereign states, that concern acceptable behaviour and that address global and regional challenges. Underlying this is the notion that states, by acting in concert, achieve international order while also laying down criteria to determine which states are to be accepted as legitimate members of international society. Pressure is also mounting to endeavour to develop multi-lateral rules limiting information warfare. However, information warfare remains largely incorporeal in nature. Industrial related threats such as nuclear weapons do provide the scope for international cooperation because of the physical dimensions of this threat, namely highly radioactive material for which credible containment and management processes could be negotiated. This is not the case with information warfare. The active role that non-state actors are playing in terms of information warfare is expected to further complicate any such efforts. Although South Africa should call for multi-lateral rules regarding information warfare (as a principled position) and even participate in the building of such international norms, the effective impact of such norms would be limited.

- Scenarios in which this proposition could be valid: Especially within “Gaunab Rising” and “Inkanyamba Reduced”, although some political will might exist within “Shango Rejuvenated” and “Tsunigoab Revived” to create multi-lateral norms with albeit insignificant impact.

### **Proposition 3**

*Polarisation poses a significant risk for the boosting of information warfare as a national security threat.* The driving force linked to the polarisation – integration continuum will be significant in how the future pans out for South Africa and the world in general. While it is acknowledged that the current rapid embedding of ICT in human artefacts could also be hindered resulting in the four plausible information warfare scenarios, it is more likely that the polarisation integration driving force could harm the human future. Global divides on issues such as growth, economic wellbeing, political participation, group stratification and inequality have potential to guide the world on a divisive or cooperative road. The level of technological progress has not been reflected in terms of human behaviour as humanity continues to commit to policies resulting in negative consequences.

- Scenarios in which this proposition could be valid: “Gaunab Rising” and “Inkanyamba Reduced” in particular.

#### **Proposition 4**

*Innovative forms of network-related actions will transform information warfare into ever-changing manifestations in the national security threat environment.* As asymmetric information warfare evolves, information warfare capabilities will increasingly spread to more state actors, non-state entities and even individuals. Although unlikely, mass societal disruption could result from the innovative application of information warfare. South Africa as other countries would need to deploy resources before the 2030s to counter the threat posed by information warfare. The vulnerability of future South African society can be expected to grow as the symbolic is increasingly integrated into the production processes and wellness of society.

- Scenarios in which this proposition could be valid: “Shango Rejuvenated” and “Gaunab Rising” in particular.

#### **Proposition 5**

*While information warfare is a national security threat, it also potentially implies an information warfare threat from the state posed to the freedom of the population.* Just as innovation, transformation and networking provide the opponents of the state with capabilities to pose an information warfare threat to the state, these capabilities also empower states. In the context of growing polarisation these capabilities will become part of the arsenal of authoritarian states in their endeavours to counter dissent.

- Scenarios in which this proposition could be valid: “Gaunab Rising” and “Inkanyamba Reduced” but could also be used within “Shango Rejuvenated”.

#### **Proposition 6**

*Information warfare will become ingrained in society as the virtual and real worlds increasingly merge.* In a network-based system, computers communicate with computers. Information is stored digitally in electronic databases. Because computers are connected, every digital database in the world is, in principle, accessible from anywhere else in the world by anyone with the authority to access it. This happens practically instantaneously. Thus, the location of both the individual and the data is irrelevant. In this “virtual world” consisting of the information and communication layers, proximity does not matter anymore. Delays remain minimal, with the binding economic constraint not so much how much information can be found, but rather how much information can be processed. Networked-based information technology has considerably reduced transaction costs (Spence, 2010:227). Based on developments in the fields of IoT, additive manufacturing (3D printing) and computing everywhere, the merging of the “virtual world” and the “real world” is an upcoming trend (Carter, 2014).

- Scenarios in which this proposition could be valid: “Shango Rejuvenated” and “Gaub Rising”.

### **Proposition 7**

*The identified four information warfare scenarios for the 2030s as well as the information warfare future model can serve as frameworks or mental models for wider application in the TWEPS environments and further research.* Building on the scenario work done, conducting a variety of additional scenario and gaming methodologies, it is possible to produce heuristics or rules of thumb (Keats, 2015) to cover many uncertainties and to assist in producing preferable and probable information warfare scenarios. Furthermore, the value of the futures model, which also stresses the layered, interactive and system elements, lies in identifying the forces which will be crucial in creating insight into any issue within the TWEPS environments. The model can be applied in a wider context than only information warfare as it could also be applied to most upcoming issues within the TWEPS environments.

## **9.3 RESEARCH CONTRIBUTIONS**

The contributions of the study are both theoretical and practical and summarised as follows:

- Provides a strategic and more inclusive definition of information warfare taking into account the technological and non-technological dimensions of this phenomenon.
- The development of the Information Warfare Environment Futures Model is constructive for guiding further studies.
- Using CLA to evaluate the outcomes of a comprehensively modelled environmental scan has significant methodological value for use in future studies.
- The scenarios presented provide plausible futures which provide early warning insights on the manifestation of information warfare as a national security threat confronting South Africa during the 2030s.

In this study the weakness of definitions of information warfare was identified as a challenge. Three types of definitions were identified namely broad, ICT related and military definitions. Although all these definitions highlight some relevant aspects of information warfare, not one of these definitions does justice to the full spectrum of activities, which could be regarded as information warfare. Information warfare is defined as actions focused on destabilising or manipulating the core information networks of a state or entity in society with the aim to influence the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state. This definition additionally assisted to gain the insight that information warfare is taking place on a cognitive-technological continuum, resulting in the identification of netwar, psychological operations and cyberwar as its three manifestations.

The Information Warfare Environment Futures Model stresses the layered, interactive and system elements underlying the current but also future manifestation of information warfare. The development of this model is a methodological tool designed to provide guidance for an integrated approach to futures analyses, especially related to most upcoming national security threats but also broader TWEPS macro environmental challenges and opportunities.

CLA is an increasingly compelling analytical technique being applied in both futures research and social sciences. Since its development by Inayatullah, this technique has been applied to a diverse field of topics. The use of CLA to evaluate the outcomes of a comprehensively modelled environmental scan is unique and has significant methodological value for use in future studies. The study illustrates that the hybridisation of CLA with the development of scenarios is possible and create an application possibility which could lead to the development of more complex scenarios.

The study is also contribution to practice by providing plausible futures that provide early warning insights on the manifestation of information warfare as a national security threat confronting South Africa during the 2030s. This study is not conveying the present and therefore soon to be redundant fact. Rather it is a study embedded in the continuum of time capturing past, present and critical future perspectives. It does not neglect the past, or soon to be past, but rigorously displays the future utility of the research.

#### **9.4 CONCLUSION**

Globalisation and a high level of interconnectedness are changing the world, creating new national security challenges, processes and actors. Despite optimism that multi-lateral efforts would solve global security problems, it is clear that significant work still needs to be done in this regard. In terms of containing information warfare, it is even seriously questioned if any multi-lateral agreement to contain this phenomenon would even be possible, as verification would be practically impossible. It can be expected that national security will remain a national government responsibility, albeit a much more complex phenomenon in which individuals, non-state actors and alliances of individuals and other entities will be highly relevant actors. It can be expected that with technological development will come many innovations and improvements in the quality of life. At the same time, the negative side of these technologies will also be present and will mutate to hamper the development of solutions.

The two key driving forces on the continuum presented by the level of integration versus polarisation and the level of ICT embedding in society will be crucial in the manifestation of information warfare by the 2030s. On a strategic level, the management of these two driving forces and the countering of polarisation will be crucial in negating the threats posed by information warfare. However, irrespective of which scenario manifests, information warfare will become a national security threat of note by the 2030s. As economic, political and social life becomes more and more intertwined in everyday life, so does the vulnerability of humankind.

The study also highlights how countries are able to manage discontent through a collaborative ethic of common purpose namely the ability of countries to build and sustain partnerships to combat discontent will increasingly depend on bolstering a country's credibility with the broader global population and forging an ethic of common purpose. It can be expected that political credibility and international esteem will probably grow in political significance in the future. The Western model of political development and values was dominant up to the 20th century but is increasingly being challenged by the rise of Asia and Africa. The political democratic models as conceived and developed by the West will not necessarily represent the models for the political environment of the future.

The threat of some form of global anarchy is an underlying theme regarding the nexus of the identified main driving forces namely polarisation and ICT embeddedness in the future. Therefore the importance of strengthening national and social will to enhance collaboration and shared common purpose might be that which will differentiate places of human progress from places of increasing inequality and increased chaos in the future.

This study provided a basis for applying future studies to a specific futures national security threat. Further research can be conducted on new forms of network-related actions such as the rhizome phenomenon (of small, highly interconnected networks) using social network phenomena for cyber mobilisation, which has been identified as of particular use for information warfare in the future. Social media empowers most net-enabled individuals interested in participating in practically any global issue. This has created platforms for involvement and participation in social and political issues on a level never seen before in the history of humankind. Increasingly, it does not matter what the majority's views are in terms of current issues; it matters more what the majority of empowered individuals are doing in terms of such issues.

The viability of futures research is related to the quality of the research methods used. The viability of futures research is also associated with the diversity of research methods used, specifically in the developing world. As long as futures research is seen as a sole domain of the developed North, it will struggle to maintain its global position as an instrument of change and sustainable growth.

## LIST OF SOURCES

Africa Centre for Strategic Studies. 2005. *Background Paper on the Senior Leader Seminar*. Gaborone, Botswana, 19 June to 1 July.

African Centre for the Constructive Resolution of Disputes (ACCORD). 2004. *Conflict Trends*. Presentation in Pretoria during February.

Agostini, A. 2010. *Trends vs. Driving Forces: A Clarity-Driven Pathway Before a Universal Management and Scientific Blunder!* [Online] Available: <http://www.slideshare.net/andresagostini/1-4950979> Accessed: 6 August 2015.

Alberts, D.S. & Czerwinski, T.J. 2002. Preface. In Alberts, D.S. & Czerwinski, T.J. (Eds.), *Complexity, Global Politics and National Security*. 2nd edition. Honolulu: University Press of the Pacific.

Alger, J.I. 1996. Introduction. In Schwartz, W., *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*. 2nd edition. New York: Thunder's Mouth Press.

Allan, G. 2003. A Critique of Using Grounded Theory as a Research Method. *Electronic Journal of Business Research Methods*, 2(1), 1-10.

Allen, E. & Seaman, C. 2007. *Likert Scales and Data Analyses*. [Online] Available <http://mail.asq.org/quality-progress/2007/07/statistics/likert-scales-and-data-analyses.html> Accessed: 30 March 2015.

Angstrom, J. & Widen, J.J. 2015. *Contemporary Military Theory: The Dynamics of War*. Abingdon: Routledge.

Antonopoulos, A.M. 2008. *Georgia Cyberwar Overblown*. 19 August. [Online] Available: [http://www.pcworld.com/businesscenter/article/150021/georgia\\_cyberwar\\_overblown.html](http://www.pcworld.com/businesscenter/article/150021/georgia_cyberwar_overblown.html) Accessed: 20 August 2008.

Apple, M.W., Ball, S.J. & Gandin, L.A. 2010. Introduction: Mapping the Sociology of Education: Social Context, Power and Knowledge. In Apple, M.W., Ball, S.J. & Gandin, L.A. (Eds.), *The Routledge International Handbook of the Sociology of Education*. New York: Routledge.

Armistead, L. 2004. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington DC: Brassey's.

Armstrong, J.S. 2001. Introduction. In Armstrong, J.S. (Ed.). *Principles of Forecasting: A Handbook for Researchers and Practitioners*. Boston: Kluwer Academic Publishers.

Aronson, J.D. 2001. The Communications and Internet Revolution. In Baylis, J. & Smith, S. (Eds.), *The Globalization of World Politics*. 2nd edition. Oxford: Oxford University Press.

Arquilla, J. & Ronfeldt, D. 1995. Cyberwar and Netwar: New Modes, Old Concepts, of Conflict. [Online] Available: <http://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/Cyberwar.html> Accessed: 27 July 2016.

Arquilla, J. & Ronfeldt, D. 1997. Information, Power and Grand Strategy. In Arquilla, J. & Ronfeldt, D. (Eds.), *Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation, MR-880. [Online] Available: <http://www.rand.org/publications/MR/MR880/index.html> Accessed: 15 April 2005.

Arquilla, J. & Ronfeldt, D. 2001. The Advent of Netwar (Revisited). In Arquilla, J. & Ronfeldt, D. (Eds.), *Networks and Netwars: the Future of Terror, Crime, and Militancy*. Santa Monica: National Defence Research Institute, RAND.

Arquilla, J., Ronfeldt, D. & Zanini, M. 1999. Networks, Netwar, and Information – Age Terrorism. In Khalilzad, Z.M. & White, J.P. (Eds.), *The Changing Role of Information in Warfare*. Washington DC: RAND Project Air Force.

Ashton, W.B. & Klavans, R.A. 1997. An Introduction to Technical Intelligence in Business. In Ashton, W.B. & Klavans, R.A. (Eds.), *Keeping Abreast of Science and Technology: Technical Intelligence for Business*. Columbus: Battelle Press.

Bailes, A.J.K. 2012. The Strategic Object of War. In Boyer, Y. & Lindley-French, J. (Eds.). *The Oxford Handbook of War*. Oxford: Oxford University Press.

Balaam, D.N. & Veseth, M. 2001. *Introduction to International Political Economy*. 2nd edition. Upper Saddle River: Prentice Hall.

Balagangadharan, A.K. 2009. *Web 2.0: Powering the Information Age News*. 25 May [Online] Available:[http://www.domain-b.com/infotech/itfeature/20090525\\_web\\_2.0\\_information.html](http://www.domain-b.com/infotech/itfeature/20090525_web_2.0_information.html) Accessed: 26 May 2009.

Baker, J.R. 1997. *Understanding the Revolution in Military Affairs (RMA): A Guide to America's 21st Century Defence*. Washington DC: Progressive Policy Institute Report.

Basu, I. 2009. Cyber snooping rattles exiled Tibetans. 21 April. [Online] Available: [http://www.upiasia.com/Security/2009/04/21/cyber\\_snooping\\_rattles\\_exiled\\_tibetans/7609/](http://www.upiasia.com/Security/2009/04/21/cyber_snooping_rattles_exiled_tibetans/7609/) Accessed: 21 April 2009.

Basu, R. 2012. Realism. In Basu, R. (Ed.), *International Politics Concepts, Theories and Issues*. New Delhi: Sage Publications India.

Baszanger, I. 1998. The Work Sites of an American Interactionist: Anselm L. Strauss, 1917-1996. *Symbolic Interaction*, **21**(4), 353-377.

Baudrillard, J. 1983. *Simulations*. New York: Semiotext.

Baumard, P. 1996. *From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift*. [Online] Available: [http://gcc.uni-paderborn.de/www/WI/WI2/WI2\\_LIT.NSF/fb8fb1b65f7e25e3412568ce0052e511/6dee8c20b2de65004125692e00693585/\\$FILE/baumard.htm](http://gcc.uni-paderborn.de/www/WI/WI2/WI2_LIT.NSF/fb8fb1b65f7e25e3412568ce0052e511/6dee8c20b2de65004125692e00693585/$FILE/baumard.htm) Accessed: 6 April 2005.

BBC News. 2015. *Richest 1% to Own More Than Rest of World, Oxfam says*. 19 January. [Online] Available: <http://www.bbc.com/news/business-30875633> Accessed: 29 July 2015.

BBC News. 2009. *Internet Brings Events in Iran to Life*. 14 June. [Online] Available: [http://news.bbc.co.uk/2/hi/middle\\_east/8099579.stm](http://news.bbc.co.uk/2/hi/middle_east/8099579.stm) Accessed: 24 June 2009.

Bell, W. 2005. An Overview of Futures Studies. Volume 1: Foundations. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Bell, W. 2007. *Foundations of Futures Studies: Human Science for a New Era*. Volume 1: *History, Purposes and Knowledge*. 3rd edition. New Brunswick, NJ: Transaction Publishers.

Bell, W. 2004. *Foundations of Futures Studies: Human Science for a New Era*. Volume 2: *Values, Objectivity and the Good Society*. New Brunswick, NJ: Transaction Publishers.

Bello, R.A. 2007. Model Building and Usage in Social Science Research. In Lasisi, R.O. & Fayeye, J.O. (Eds.). 2007. *Leading Issues in General Studies: Humanities and Social Sciences*. Ilorin: The General Studies Division, University of Ilorin.

Benkler, Y. 2006. *The Wealth of Networks How Social Production Transforms Markets and Freedom*. New Haven and London: Yale University Press.

Berridge, G.R. 1997. *International Politics: States, Power and Conflict since 1945*. 3rd edition. Harlow: Pearson Education.

Bhaskar, R. 2008. *A Realist Theory of Science*. London: Taylor and Francis e-Library.

Bildt, C. 2004. "Peace and War in the World after Westphalia: Some Reflections on the challenges of a Changing International Order." In Slaughter, A., Bildt, C. & Ogura, K., *The New Challenges to International, National and Human Security Policy*, The Triangle Papers: 58, Washington DC: The Trilateral Commission.

Bishara, M. 2001. An Enemy with no Forwarding Address. *Le Monde Diplomatique*, 3 October. [Online] Available: <http://mondediplo.com/2001/10/03asymmetry> Accessed: 12 January 2004.

Bishop, P. & Hines, A. (Eds.). 2013. *Thinking about the Future: Guidelines for Strategic Foresight*. Houston: Hinesight.

Bocking, S. 2004. *Nature's Experts: Science, Politics, and the Environment*. New Brunswick, NJ: Rutgers University Press.

Bodissey, B. 2007. *All Information Warfare is Local*. [Online] Available: <http://gatesofvienna.blogspot.com/2007/12/all-information-warfare-is-local.html> Accessed: 31 December 2007.

Bonkovsky, F.O. 1980. *International Norms and National Policy*. Grand Rapids: William B. Eerdmans.

Booz Allen Hamilton Inc. 2012. *Increasing Cyber Threats Call for More Innovative Cybersecurity*. [Online] Available: <http://www.boozallen.com/insights/2012/03/cyber-threats-innovative-cybersecurity> Accessed: 23 June 2015.

Bower, M. 2007. Battle Lab Explores Information Warfare. *Leavenworth Lamp Weekly*, 13 December. [Online] Available: <http://www.ftleavenworthlamp.com/articles/2007/12/13/news/news1.txt> Accessed: 17 December 2007.

Brand, S. 1999. *The Clock of the Long Now: Time and Responsibility*. New York: Basic Book Publishers.

Bratich, J.Z. 2009. *Social Media and the Rise of Genetically Modified Grassroots Organizations: The Fog Machine*. [Online] Available: <http://www.counterpunch.org/bratich06222009.html> Accessed: 23 June 2009.

Bremmer, I. 2006, Thinking Beyond States. *The National Interest*, **83**, Spring, 66.

Bromley, S. 2004. International Politics: States, Anarchy and Governance. In Bromley, S., Mackintosh, M., Brown, W. & Wuyts, M. *Making the International: Economic Interdependence and Political Order*. London: Pluto Press.

Brown, C. & Ainley, K. 2005. *Understanding International Relations*. 3rd edition. Basingstoke: Palgrave Macmillan.

Brown, H. 1983. *Thinking about National Security*. Boulder: Westview Press.

Bruno, G. 2008. *The Evolution of Cyber Warfare*. [Online] Available: [http://www.cfr.org/publication/15577/evolution\\_of\\_cyber\\_warfare.html](http://www.cfr.org/publication/15577/evolution_of_cyber_warfare.html) Accessed: 28 February 2008.

Bull, H. 1987. Does Order Exist in World Politics? In Viotti, P.R. & Kauppi, M. *International Relations Theory: Realism, Pluralism, Globalism*. New York: Macmillan Publishers.

Bull, H. 1992. Order and Anarchy in International Society. In Luard, E. (Ed.), *Basic Texts in International Relations: The Evolution of Ideas about Society*. London: Macmillan Publishers.

Bunge, M. 2009. *Causality and Modern Science*. New Brunswick: Transaction Publishers.

Burchill, S. 2005. Liberalism. In Burchill, S., Linklater, A., Devetak, R., Donnelly, J., Paterson, M., Reus-Smit, C. & True, J. *Theories of International Relations*. 3rd edition. New York: Palgrave Macmillan.

Burchill, S. & Linklater, A. 2005. Introduction. In Burchill, S. Linklater, A., Devetak, R., Donnelly, J., Paterson, M., Reus-Smit, C. & True, J. *Theories of International Relations*. New York: Palgrave Macmillan, Third Edition.

Burns, A. & Burns, R. 2008. *Basic Marketing Research*. 2nd edition. New Jersey: Pearson Education.

Bussey, M. 2014. CLA as Process: Mapping the Theory and Practice of the Multiple. *Journal of Futures Studies*, **18**(4), 45-58.

Butler, M. 2008. *The Technological Environment*. Presentation at conference by the Institute for Futures Research, 14 November, Sandton, Johannesburg.

Caldwell, R.L. 2003. *Driving Forces*. University of Arizona's "Anticipating the Future" course page. [Online] Available: <http://ag.arizona.edu/futures/fut/dfmain.html> Accessed: 3 September 2010.

CALRESCO, 2006. Complexity. [Online] Available <http://www.calresco.org/> Accessed: 12 June 2006.

Campen, A.D. 1992. Précis. In Campen, A.D. (Ed.), *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War*. Fairfax, Va.: AFCEA International Press.

Campen A.D. 2008. Cyberwar, Anyone? *SIGNAL Magazine*, January. [Online] Available: [http://www.afcea.org/signal/articles/templates/Signal\\_Article\\_Template.asp?articleid=1452&zoneid=223](http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1452&zoneid=223) Accessed: 3 January 2008.

Candolin, C. 2003. *A study of infrastructure warfare in relation to information warfare, net warfare, and network-centric warfare*. Article obtained from author on 7 January 2004.

Canton, J. 2007. *The Extreme Future: The Top Trends that will Reshape the World in the Next 20 Years*. New York: Plume.

Carr, E.H. 1964. *The Twenty Years' Crisis, 1918-1939: An Introduction to the Study of International Relations*. New York: Harper and Row.

Carter, S. 2014. *Top Ten Strategic Technology Trends for 2015*. Slide from Gartner IT Symposium. [Online] Available: [https://twitter.com/sandy\\_carter/status/651436729266765824/photo/1?utm](https://twitter.com/sandy_carter/status/651436729266765824/photo/1?utm)

\_content=buffer045f0&utm\_medium=social&utm\_source=twitter.com&utm\_campaign Accessed: 13 October 2015.

Cavelty, M.D. 2007. Is Anything Ever New? – Exploring the Specificities of Security and Governance in the Information Age. In Cavelty, M.D., Mauer, V. & Krishna-Hensel, S.F. (Eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate Publishing Company.

Cavelty, M.D. & Brunner, E.M. 2007. Introduction: Information, Power, and Security: An Outline of Debates and Implications. In Cavelty, M.D., Mauer, V. & Krishna-Hensel, S.F. (Eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate Publishing Company.

Chadwick, A. 2006. *Internet Politics: States, Citizens, and New Communication Technologies*. Oxford: Oxford University Press.

Chalus-Sauvannet, M-C. 2011. Human Resources Scanning: A Tool for the Implementation of Sustainable Development? In Lesca, N. (Ed.), *Environmental Scanning and Sustainable Development*. London: ISTE Ltd.

Charette, R.N. 2007. Open-Source Warfare. November. *IEEE Spectrum*. [Online] Available: <http://blogs.spectrum.ieee.org/riskfactor> Accessed: 15 December 2007.

Charmaz, K. 1983. The Grounded Theory Method: An Explication and Interpretation. In Emerson, R. (Ed.), *Contemporary Field Research: A Collection of Readings*. Boston: Little Brown.

Charmaz, K. 2006. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. London: Sage Publications.

Chermack, T.J. 2003. The Role of Scenarios in Altering Mental Models and Building Organizational Knowledge. *Futures Research Quarterly*, Spring, 25-41.

Chermack, T.J. 2011. *Scenario Planning In Organizations: How to Create, Use, and Assess Scenarios*. San Francisco: Berrett-Koehler Publishers, Inc.

Choo, C.W. 1999. The Art of Scanning the Environment. *Bulletin of the American Society for Information Science*, **25**(3), 21-24. [Online] Available: <http://www.asis.org/Bulletin/Feb-99/choo.html> Accessed: 15 March 2007.

Choo, C.W. 2001. Environmental scanning as information seeking and organizational learning. *Information Research*, 7(1), 1-25. [Online] Available: <http://InformationR.net/ir/7-1/paper112.html>. Accessed: 8 March 2007.

Coates, J.F. 1985. *Issues Identification and Management: The State of the Art of Methods and Techniques*. Research Project 2345-28. Palo Alto: Electric Power Research Institute.

Coleman, K. 2009. *The New Internet Interview with Technolytics Institute Founder: Obama Needs To Get The Ball Rolling*. 13 July. [Online] Available: <http://thenewnewinternet.com/2009/07/13/the-new-new-internet-interview-with-technolytics-institute-founder-obama-needs-to-get-the-ball-rolling>. Accessed: 14 July 2009.

Computerhope.com. 2007. *Cyberwar*. [Online] Available: [www.computerhope.com/jargon/c/cyberwar.htm](http://www.computerhope.com/jargon/c/cyberwar.htm). Accessed: 11 December 2007.

Cook, T. & Campbell, D.T. 1979. *Quasi-Experimentation: Design and Analysis Issues for Field Settings*. Chicago: Rand McNally.

Cornish, E. 2004. *Futuring: The Exploration of the Future*. Bethesda: World Future Society.

Courtney, H. 2001. *20/20 Foresight: Crafting Strategy in an Uncertain World*. Boston: Harvard Business School Press.

Cronin, B. & Crawford, H. 1999. Information Warfare: Its Application in Military and Civilian Contexts. *The Information Society*, 15(4), 257-263.

Cronje, F. 2014. *A Time Traveller's Guide to our Next Ten Years*. Cape Town: Tafelberg Publishers.

Cronje, F.J. 2013. *Beyond The High Road: A Scenario Analysis of the Prospects for Political Stability or Instability in South Africa over the Period to 2024*. PhD thesis. Potchefstroom: North-West University.

Crossman, A. 2014. *Pilot Study*. [Online] Available: [http://www.sociology.about.com/od/P\\_Index/g/Pilot-Study.htm](http://www.sociology.about.com/od/P_Index/g/Pilot-Study.htm). Accessed: 17 August 2014.

Crumm, R.K. 1996. *Information Warfare: An Air Force Policy for the Role of Public Affairs*. School of Advanced Airpower Studies, USAF, Maxwell Air Force Base. Alabama: Air University Press.

Curran, K. Concannon, K. & McKeever, S. 2008. Cyber Terrorism Attacks. In Janczewski, L. & Colarik, A.M. (Eds.), *Cyber Warfare and Cyber Terrorism*. New York: Hershey.

Dajani, J.S., Sincoff, M.Z. & Talley, W.K. 1979. Stability and Agreement Criteria for the Termination of Delphi Studies. *Technological Forecasting and Social Change*, 13(1), 83-90.

Dalby, S. 1992. Security, Modernity, Ecology: The Dilemmas of Post-Cold War Security Discourse. *Alternatives*, 17(1), 95-134.

Dale, H.C. 2009. The Iranian Elections and Public Diplomacy 2.0: A Tale of Untapped Potential. *The Heritage Foundation*, WebMemo #2497. [Online] Available: <http://www.heritage.org/Research/PublicDiplomacy/wm2497.cfm>. Accessed: 21 June 2009.

Danermark, B., Ekström, M., Jakobsen, L. & Karlsson, J.C. 2005. *Explaining Society: Critical Realism in the Social Sciences*. London: Taylor and Francis e-Library.

Darnton, G. 2006. Information Warfare and the Laws of War. In Halpin, E., Trevorrow, P. & Webb, D. (Eds.), *Cyberwar, Netwar and the Revolution in Military Affairs*. New York: Palgrave Macmillan.

Dasnois, M. 2015. 0% and the Rise of Leaderless Movements. *iLIVE*, 2 November. [Online] Available: <http://www.timeslive.co.za/ilive/2015/11/02/0-and-the-rise-of-leaderless-movements-iLIVE> Accessed: 5 November 2015.

Dator, J.A., Sweeney, J.A. & Yee, A.M. 2014. *Mutative Media: Communication Technologies and Power Relations in the Past, Present, and Futures*. Heidelberg: Springer.

Day, J. & Bobeva, M. 2005. A Generic Toolkit for the Successful Management of Delphi Studies. *The Electronic Journal of Business Research Methodology*, 3(2), 103-116.

Deep, A. 2015. *Hybrid War: Old Concept, New Techniques*. [Online] Available: <http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques> Accessed: 2 March 2015.

De Jouvenel, B. 1967. *The Art of Conjecture*. New York: Basic Book Publishers.

- Dekkers, R. 2015. *Applied Systems Theory*. Cham: Springer.
- De Landa, M. 1991. *War in the Age of Intelligent Machines*. New York: Swerve Press.
- Deleuze, G. & Guattari, F. 1980. *A Thousand Plateaus: Capitalism and Schizophrenia*. London and New York: Continuum.
- Denning, D.E. 1999. *Information Warfare and Security*. Reading MA: Addison-Wesley.
- Dey, I. 2005. *Qualitative Data Analysis: A User-friendly Guide for Social Scientists*. London: Taylor and Francis e-Library.
- Dictionary.com. 2015. [Online] Available: <http://dictionary.reference.com/browse>  
Accessed: 6 August 2015.
- DiNardo, R.L. & Hughes D.J. 1995. Some Cautionary Thoughts on Information Warfare. *Airpower Journal*, **9**(4), 1-10.
- Dostal, E. 2007. *Systems Thinking and Futures Research*. PowerPoint presentation. Bellville: University of Stellenbosch Business School.
- Dostal., E, Cloete, A. & Járos, G. 2007. *Biomatrix: A Systems Approach to Organisational and Societal Change*. 3rd edition. Cape Town: Mega Digital.
- Dougherty, J.E. & Pfalzgraff, R.L. 1997 *Contending Theories of International Relations: A Comprehensive Survey*. 4th edition. Addison-Wesley Longman.
- Downes, A.B. 2008. *Targeting Civilians in War*. Ithaca: Cornell University Press.
- Durodié, B. 2007. Understanding the Broader Context. In Rappert, B. (Ed.), *Technology and Security: Governing Threats in the New Millennium*. Basingstoke: Palgrave Macmillan.
- Duyvesteyn, I. 2005. The Concept of Conventional War and Armed Conflict in Collapsed States. In Duyvesteyn, I. & Angstrom, J. (Eds.). *Rethinking the Nature of War*. London: Frank Cass.
- Easton, D. 1965. *A System Analysis of Political Life*. New York: John Wiley & Sons, Inc.
- Edwards, D.V. 1969. *International Political Analysis*. New York: Holt Rinehart & Winston Inc.

Elbirt, A.J. 2003. Information Warfare: Are You At Risk? *IEEE Technology and Society Magazine*, **22**(4), 13-19.

Elkus, A. 2009. *The Rise of Cyber-Mobilization*. [Online] Available: <http://www.groupintel.com/2009/02/13/the-rise-of-cyber-mobilization>. Accessed: 16 February 2009.

Enzer, S. 2006. Plastics and Competing Materials by 1985: A Delphi Forecasting Study. In Linstone, H.A. & Turoff, M. (Eds.), *The Delphi Method Techniques and Application*. Revised e-book.

Eriksson, E.A. 1999. Viewpoint: Information Warfare: Hype or Reality? *The Nonproliferation Review*, Spring-Summer, 57-64.

Fink, A., Kosecoff, J., Chassin, M. & Brook, R. 1991. *Consensus Methods: Characteristics and Guidelines for Use*. Santa Monica: RAND.

FireEye, 2016. Red Line Drawn: China Recalculates its Use of Cyber Espionage. Special Report. [Online] Available: <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf> Accessed: 27 July 2016.

Flanagin, A. & Metzger, M. 2008. Digital media and youth: Unparalleled opportunity and unprecedented responsibility. In M. Metzger, M. & Flanagin, A. (Eds.), *Digital media, youth, and credibility*. Cambridge, MA: The MIT Press.

Flood, R.L. 2001. *The Relationship of 'systems thinking' to Action Research: Handbook of Action Research*. London: Sage Publications.

Ford, M. 2015. *Rise of the Robot: Technology and the Threat of a Jobless Future*. New York: Basic Books.

Forrester, J.W. 1973. *World Dynamics*. 2nd edition. Cambridge, Mass: Wright-Allen Press Inc.

Fourie, P. 2007. The future of AIDS in Africa: Lessons from two scenario projects. *African Journal of AIDS Research*, **6**(2), 97-107.

Galtung, J. 2005. Peace, Vision and the Future. Volume 4: The Views of Futurists. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Gharajedaghi, J. 2006. *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*. 2nd edition. Burlington: Elsevier Ltd.

Ghosh, J. 2013. Inequality is the Biggest Threat to the World and Needs to be Tackled Now. The future of development poverty blog. 20 February. [Online] Available: <http://www.theguardian.com/global-development/poverty-matters/2013/feb/20/inequality-threat-to-world-needs-tackling>. Accessed: 31 August 2015.

Gilat, A. 2009. Information Warfare in the 21st Century: Ideas are sometimes stronger than bombs. [Online] Available: [http://www.eurekalert.org/pub\\_releases/2009-03/uoh-iwi031809.php](http://www.eurekalert.org/pub_releases/2009-03/uoh-iwi031809.php). Accessed: 23 March 2009.

Gilpin, R.G. 1984. The Richness of the Tradition of Political Realism. *International Organisation*, **38**(2), 287-304.

Glenn, J.C. 2003. Scenarios. In Glenn, J.C. & Gordon, T.J. (Eds.), *Futures Research Methodology V2.0*. New York: American Council for the United Nations University, Millennium Project, CD ROM.

Global Business Environment. 2003. *Scenarios: an Explorer's Guide*. London: Shell International.

Goldman, E.O. 2004. Introduction: Security in the Information Technology Age. In Goldman, E.O. (Ed.), *National Security in the Information Age*. London: Frank Cass.

Goldstein, F.L. & Jacobowitz, D.W. 2002. Psychological Operations: An Introduction. In Goldstein, F.L. & Findley, B.F. (Eds.), *Psychological Operations: Principles and Case Studies*. Maxwell Air Force Base, Alabama: Air University Press.

Gompert, D.C. 1998. *Right Makes Might Freedom and Power in the Information Age*. McNair Paper No. 59. Washington DC: National Defence University Press.

Gompert, D.C. 1999. Right Makes Might Freedom and Power in the Information Age. In Khalilzad, Z.M. & White, J.P. (Eds.), *The Changing Role of Information in Warfare*. Washington D.C: RAND Project Air Force.

Gordon, J.T. 2003. The Delphi Method. In Glenn, J.C. & Gordon, T.J. (Eds.), *Futures Research Methodology V2.0*, New York: American Council for the United Nations University, Millennium Project CD ROM.

Gordon, J.T. 1994. *The Delphi Method in Futures Research Methodology*. AC/UNU Project. [Online] Available: <http://www.gerenciamento.ufba.br/Downloads/delphi%20%281%29.pdf> Accessed: 8 November 2013.

Gordon, J.T. & Glenn, J.C. 2003. Environmental Scanning. In Glenn, J.C. & Gordon, T.J. (Eds.), *Futures Research Methodology V2.0*. New York: American Council for the United Nations University, Millennium Project, CD ROM.

Goulding, C. 2002. *Grounded Theory: A Practical Guide for Management, Business and Market Researchers*. London: Sage Publications.

Grant, R. 2008. The Dogs of Web War. *Air Force Magazine*, 91(1), 23-27. [Online] Available: <http://www.afa.org/magazine/jan2008/0108dogs.asp>. Accessed: 2 January 2008.

Green, J.A. (Ed), 2015. *Cyber Warfare: A Multidisciplinary Analysis*. Abingdon: Routledge.

Grey, C. 2007. *Another Bloody Century: Future Warfare*. Phoenix: Phoenix Press.

Haberman, M. 2013. Four Ways to do Environmental Scanning. [Online] Available: <http://omegahrsolutions.com/2013/04/four-ways-to-do-environmental-scanning.html>. Accessed: 25 July 2016.

Hahn, G. 2008. Georgia's Propaganda War. [Online] Available: <http://warisboring.com/p1339> Accessed: 4 September 2008.

Hammes, T.X. 2004. *The Sling and the Stone: On War in the 21st Century*. St Paul: Zenith Press.

Hammond, G.T. 2001. *Globalization, Technology and the Transformation of the Security Environment: The Real Revolution in Military Affairs*. Paper presented at the meeting of the American Political Science Association, San Francisco, August.

Harknett, R.J. 2004. Integrated Security: A Strategic Response to Anonymity and the Problem of the Few. In Goldman, E.O. (Ed.), *National Security in the Information Age*. London: Frank Cass.

Harvey, R. 2003. *Global Disorder*. London: Constable.

Hayward, P. 2005. The Lineage of Foresight. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Hauschild, E. 1999. Modern and Information Warfare a Conceptual Approach. *Studies in Contemporary History and Security Policy*, 3. Bern: Peter Lang.

Heathfield, D. 2008. Improving Decision Making in the Area of National and International Security: The Future Map Methodology. In Minai, A., Braha, D. & Bar-Yam, Y. (Eds.), *Unifying Themes in Complex Systems: Proceedings of the Sixth International Conference on Complex Systems*. Berlin: Springer-Verlag.

Heidrick & Struggles. 2015. *The CEO Report: Embracing the Paradoxes of Leadership and the Power of Doubt*. [Online] Available: <http://www.heidrick.com/Knowledge-Center/Publication/The-CEO-Report>. Accessed: 14 May 2015.

Heinonen, S. 2008. Multidimensional Concept of Risks in Horizon Scanning and Future Thinking. In Tan, H.N. & Hoo, T.B. (Eds.), *Thinking about the Future: Strategic Anticipation and RAHS*. Singapore: National Security Coordination Secretariat and S. Rajaratnam School of International Studies.

Helbing, D. Lämmer, S. 2008. Managing Complexity: An Introduction. In Helbing, D. (Ed.) *Managing Complexity: Insights, Concepts, Applications*. Heidelberg: Springer-Verlag.

Held, D. 1989. *Political Theory and the Modern State*. Stanford: Stanford University Press.

Heywood, A. 2002. *Politics*. 2nd edition. Basingstoke: Palgrave Macmillan.

Hiltz, S.R. & Turoff M. 1978. *The Network Nation: Human Communication via Computer*. London: Addison-Wesley.

Hodge, N. 2009. Gaza War's New Front: Facebook. [Online] Available: <http://blog.wired.com/defense/2009/01/facebook-fundra.html>. Accessed: 12 January 2009.

Hoffman, F. 2007. *Conflict in the 21st Century: The Rise of Hybrid War*. Arlington: Potomac Institute for Policy Studies.

Holsti, K.J. 1980. Change in the International System: Interdependence, Integration, and Fragmentation. In Holsti, O.R., Siverson, R.M. & George, A.L. (Eds.), *Change in the International System*. Boulder: Westview Press.

Horton, A. 1999. A Model for a Successful Foresight Process. *Foresight*, **1**(1), 5-9.

Houle, D. 2013. *Entering the Shift Age: The End of the Information Age and the New Era of Transformation*. Naperville: Sourcebooks.

Howard, M. 1970. Military Power and International Order. In Masannat G.S. & Abcarian, G. (Eds.), *International Politics, Introductory Readings*. New York: Charles Scribner's Sons.

Howkins, J. & Valantin, R. 1997. *Development and the Information Age: Four Global Scenarios for the Future of Information and Communication Technology*. [Online] Available: [http://www.idrc.ca/en/ev-28768-201-1-DO\\_TOPIC.html](http://www.idrc.ca/en/ev-28768-201-1-DO_TOPIC.html). Accessed: 8 February 2010.

Hsu, C.C. & Sandford, B.A. 2007. The Delphi Technique: Making Sense of Consensus. *Practical Assessment, Research & Evaluation*, **12**(10), 1-8.

Hutchinson, W. & Warren, M. 2001. Principles of Information Warfare. *Journal of Information Warfare*, **1**(1), 1-6.

Ilbury, C. & Sunter, C. 2003. *The Mind of a Fox: Scenario Planning in Action*. Cape Town: Human & Rousseau and Tafelberg.

Inayatullah, S. 2000. *Causal Layered Analysis: Poststructuralism as Method*. [Online] Available: <http://www.tukkkk.f/tutu/vanhat/MeSe2000/mespapers/Inayatullah>. Accessed: 12 January 2007.

Inayatullah, S. 2004. Causal Layered Analysis: Theory, Historical Context and Case Studies. In Inayatullah, S. (Ed.), *The Causal Layered Analysis (CLA) Reader: Theory and Case Studies of an Integrative and Transformative Methodology*. Tamkang: Tamkang University Press.

Inayatullah, S. 2005a. *Questioning the Future: Methods and Tools for Organizational and Societal Transformation*. Taipei: Tamkang University.

Inayatullah, S. 2005b. Methods and Epistemologies in Futures Studies. Volume 1: Foundations. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Inayatullah, S. 2005c. Introduction to Volume 4: Telling the Story – Futures Studies, Methods and Visions. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Inayatullah, S. 2005d. *Futures and Change: From Strategy to Transformation*. International Asia Pacific Course in Future Studies and Policymaking.

Inayatullah, S. 2005e. Macrohistory and Layers of Reality. Volume 4. The Views of Futurists. Knowledge Base of Future Studies. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Inayatullah, S. 2008a. Six Pillars: Futures Thinking for Transforming. *Foresight*, **10**(1), 4-21. DOI: <http://dx.doi.org/10.1108/14636680810855991>.

Inayatullah, S. 2008b. E-mail response to question about approaches to future studies, 3 December.

Inayatullah, S. 2008c. *Causal Layered Analysis Graphic*. Wikimedia, GNU license, 28 August.

Inayatullah, S. 2014a. *Futures Thinking and Strategy Development*. Presentation in Brussels, 25 November.

Inayatullah, S. 2014b. Interview with Sohail Inayatullah by Sirkka Heinonen on Futures Studies and CLA Method. Helsinki, Finland, 12 June. [Online] Available: <https://www.youtube.com/watch?v=sic1tZHIss>. Accessed: 30 July 2015.

Inayatullah, S. & Milojević, I. (Eds.). 2015. *CLA 2.0: Transformative Research in Theory and Practice*. Tamkang: Tamkang University Press.

Inayatullah, S. & Wildman, P. 1996. Ways of Knowing, Culture, Communication and the Pedagogies of the Future. *Futures*, **28**(8), 723-740.

Inayatullah, S., Minkinen, M. & Heinonen, S. 2015. *A CLA Game on Neo-Carbon Energy Scenarios in Action Learning*. Futures Studies Tackling Wicked Problems Conference, organised by Finland Futures Research Centre, Turku, CLA Game Session, 11 June.

Ingram, M. 2012. How Social Media is Rewriting the Rules of Modern Warfare. Gigaom Research. 19 November. [Online] Available: <https://gigaom.com/2012/11/19/how-social-media-is-rewriting-the-rules-of-modern-warfare/> Accessed: 8 November 2015.

International Telecommunications Union (ITU). 2015. Internet of Things Global Standards Initiative. [Online] Available: <http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx> Accessed: 30 July 2015.

itu4u. 2015. *Digital Divide Progress Report: 15 Year Review*. [Online] Available: <https://itu4u.wordpress.com/2015/08/26/digital-divide-progress-report-15-year-review/> Accessed: 8 November 2015.

ITWeb. 2014. Top ICT trends for Africa in 2015. [Online] Available: <http://www.itweb.co.za/?id=139293:Top-ICT-trends-for-Africa-in-2015> Accessed: 14 May 2015.

Jaccard, J. & Jacoby, J. 2010. *Theory Construction and Model-Building Skills: A Practical Guide for Social Scientists*. New York: The Guilford Press.

Jackson, R. & Sørensen, G. 2003. *Introduction to International Relations: Theories and Approaches*. Oxford: Oxford University Press.

Jairath N. & Weinstein J. 1994. The Delphi Methodology: A Useful Administrative Approach. *Canadian Journal of Nursing Administration*, 7(3), 29-42.

Ji, Y. 1999. The Revolution in Military Affairs and the Evolution of China's Strategic Thinking. *Contemporary Southeast Asia*, 21(3), 325-345.

Joey, A.W. 2011. *The Role of Non-state Actors in International Relations*. [Online] Available: [http://www.academia.edu/5124220/The\\_Role\\_of\\_Non-state\\_Actors\\_in\\_International\\_Relations](http://www.academia.edu/5124220/The_Role_of_Non-state_Actors_in_International_Relations). Accessed: 23 June 2015.

Johnson, P.A. 2002. Is it Time for a Treaty on Information Warfare? In Schmitt, M.N. & O'Donnell, B.T. (Eds.), *International Law Studies*, 76. Computer Network Attack and International Law, US Naval War College.

Jones, A, Kovacich, G. & Luzwick, P. 2002. *Global Information Warfare: How Businesses, Governments, and Others Achieve and Attain Competitive Advantages*. Boca Raton: Auerback Publications.

Jones, R.W. 1996. Travel without Maps: Thinking about Security after the Cold War. In Davis, M.J. (Ed.), *Security Issues in the Post-Cold War World*. Cheltenham Brookfield: Edward Elgar.

Jordan, D. 2008. Air and Space Warfare. In Jordan, D., Kiras, J.D., Lonsdale, D.J., Speller, I., Tuck, C. & Walton, C.D., *Understanding Modern Warfare*. Cambridge: Cambridge University Press.

Jordan, M. 2004. *Dictionary of Gods and Goddesses*. 2nd edition. New York: Facts On File, Inc.

Judd, D. 2003. *Critical Realism and Composition Theory*. London: Routledge.

Keal, P. 2000. An International Society? In Fry, G. & O'Hagan, J., *Contending Images of World Politics*. London: Macmillan Press.

Keats, J. 2015. *Let's Play War: Could War Games Replace the Real Thing?* [Online] Available: <http://nautil.us/issue/28/2050/lets-play-war>. Accessed: 25 September 2015.

Keeney, S., Hasson, F. & McKenna, H. 2011. *The Delphi Technique in Nursing and Health Research*. Chichester: Wiley-Blackwell.

Kegley, C.W. & Wittkopf, E.R. 1997. *World Politics: Trend and Transformation*. 6th edition. New York: St Martin's Press.

Kellner, D. 1989. *Jean Baudrillard: From Marxism to Postmodernism and Beyond*. Cambridge: Polity Press.

Kellner, D. 2007. *Jean Baudrillard*. *Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, CSLI, Stanford University. [Online] Available: <http://plato.stanford.edu/entries/ baudrillard/>. Accessed: 11 June 2008.

Keohane, R.O. 1989. *International Institutions and State Power: Essays in International Relations Theory*. Boulder: Westview Press.

Keohane, R.O. & Nye, J.S. 2000. *Power and Interdependence*. 3rd edition. Boston: Little Brown.

Kerlinger, F.N. 1973. *Foundations of Behavioral Research*. New York: Holt, Rinehart & Winston, Inc.

- Kilibarda, K. 2003. *Defining Information Warfare*. [Online] Available: <http://www.infowar-monitor.net/modules.php/op1>. Accessed: 30 June 2004.
- Kobilnyk, A. 2008. *2008 – Year of the first cyber-war?* [Online] Available: [www.firstscience.com/home/perspectives/editorials/2008-year-of-the-first-cyber-war-page.htm](http://www.firstscience.com/home/perspectives/editorials/2008-year-of-the-first-cyber-war-page.htm). Accessed: 14 April 2008.
- Knibbs, K. 2015. China Finally Admits It Has an Army of Hackers for Cyberwar. [Online] Available: <http://gizmodo.com/china-finally-admits-it-has-an-army-of-hackers-for-cybe-1692188006>. Accessed: 20 March 2015.
- Knöbl, W. 2003. Theories that won't Pass Away: The Never-ending Story of Modernization Theory. In Delanty, G. & Isin, E.F. (eds.). *Handbook of Historical Sociology*. London: Sage Publications.
- Kolodziej, E.A. 2005. *Security and International Relations*. Cambridge: Cambridge University Press.
- Kosow, H. & Gassner, R. 2008. *Methods of Future and Scenario Analysis: Overview, Assessment, and Selected Criteria*. Bonn: German Development Institute.
- Kristof, T. 2006. Is it possible to make Scientific Forecasts in Social Sciences? *Futures*, **38**(5), 561-574.
- Krypt3ia Blog. 2014. Assessment: The ZunZuneo “Hummingbird” Social Network and The Cuban Spring. [Online] Available: [https://krypt3ia.wordpress.com/2014/04/06/assessment-the-zunzuneo-hummingbird-social-network-and-the-cuban-spring/?utm\\_source=dvtr.it&utm\\_medium=twitter](https://krypt3ia.wordpress.com/2014/04/06/assessment-the-zunzuneo-hummingbird-social-network-and-the-cuban-spring/?utm_source=dvtr.it&utm_medium=twitter) Accessed: 7 April 2014.
- Kuckartz, U. 2014. *Qualitative Text Analysis: A Guide to Methods, Practice and Using Software*. London: Sage.
- Kuckartz, U. 2015. Personal e-mail communication responding to question on the use of documentary material in qualitative text analysis, 3 April.
- Kuehl, D. 2004. Foreword. In Armistead, E.L., *Information Operations: The Hard Reality of Soft Power*. Washington DC: Brassey's.

Kuehl, D. 2007. Information Operations: the Policy and Organizational Evaluation. In Armistead, L. (Ed.), *Information Warfare: Separating Hype from Reality*. Washington DC: Potomac Books.

Kuhn, T.S. 1962. *The Structure of Scientific Revolutions*. Chicago: University of Chicago.

Kurian, G.T. & Molitor, G.T.T. 1996. *Encyclopaedia of the Future*, Volume 2. New York: Simon and Schuster Macmillan.

Kurki, M. 2008. *Causation in International Relations: Reclaiming Causal Analysis*. Cambridge: Cambridge University Press.

Kurzweil, R. 2006. *The Singularity is near: When humans transcend biology*. London: Viking Penguin Books.

Kuusi, O., Cuhls, K. & Steinmüller, K. 2015. Quality Criteria for Scientific Futures Research. Pre-Publish Copy. *Futura*, 1/2015.

Lai, D. 2009. Chinese Military Going Global. *China Security*, 5(1), Winter, 3-9.

Lamy, P, 2012. *Emerging Economies have Shifted the Balance of Power in World Trade*. Director-General of the World Trade Organisation (WTO) presentation at Richard Snape Lecture, Melbourne, Australia, 26 November.

Landler, M. & Stelter, B. 2009. Washington Taps into a Potent New Force in Diplomacy. 16 June, *New York Times*.

Lanier, J. 2006. *Digital Maoism: The Hazards of the New Online Collectivism*. [Online] Available: [http://www.edge.org/3rd\\_culture/lanier06/lanier06\\_index.html](http://www.edge.org/3rd_culture/lanier06/lanier06_index.html) Accessed: 2 January 2013.

Larsdotter, K. 2005. New Wars, Old Warfare? Comparing US tactics in Vietnam and Afghanistan. In Duyvesteyn, I. & Angstrom, J. (Eds.), *Rethinking the Nature of War*. London: Frank Cass.

Latham, R. 2003. Introduction. In Latham, R. (Ed.), *Bombs and Bandwidth: The emerging Relationship between Information Technology and Security*. New York: The New Press.

Leyden, J. 2009. *Russian politician: 'My assistant started Estonian cyberwar'*. [Online] Available: [http://www.theregister.co.uk/2009/03/10/estonia\\_cyberwarfare\\_twist/](http://www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/) Accessed: 10 March 2009.

Libicki, M.C. 1995. *What is information warfare?* Strategic Forum Number 28, May, Washington, DC: National Defense University, Institute for National Strategic Studies.

Libicki, M.C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

Lill, A. & Gräber, S. 2006 Human-Environmental Interactions. [Online] Available:[http://www.uni-kiel.de/ecology/users/fmueller/salzau2006/studentpages/Human\\_Environmental\\_Interactions/index.html](http://www.uni-kiel.de/ecology/users/fmueller/salzau2006/studentpages/Human_Environmental_Interactions/index.html). Accessed 25 July 2016.

Lin, A.C. 2000. Comparison of the Information Warfare Capabilities of the ROC and PRC. [Online] Available: <http://cryptome.org/cn2-infowar.htm>. Accessed: 27 October 2005.

Lindgren, M. & Bandhold, H. 2003. *Scenario Planning: The link between future and strategy*. New York: Palgrave Macmillan.

Linstone, H.A. 2005. Multiple Perspectives. Volume 4: The Views of Futurists. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Linstone, H.A. & Turoff, M. 1975. Introduction. In Linstone, H.A. & Turoff, M. (Eds.), *The Delphi Method: Techniques and Applications*. Reading: Addison-Wesley.

Linstone, H.A. & Turoff, M. 2002. Introduction. In Linstone, H.A. & Turoff, M. (Eds.), *The Delphi Method Techniques and Application*. Revised e-book.

Little, J.D.C. 1993. *On Model Building*. Massachusetts Institute of Technology, Cambridge, MA, Alfred P. Sloan School of Management, W.P. #3556-93. [Online] Available: <https://www.dspace.mit.edu/.../1/.../SWP-3556-28226976.pdf> Accessed: 21 May 2015.

Lonsdale, D.J. 2004. *The Nature of War in the Information Age: Clausewitzian Future*. London: Frank Cass.

Loveridge, D. 2009. *Foresight: The Art and Science of Anticipating the Future*. New York: Routledge.

Macionis, J.J. & Gerber, L.M. 2011. *Sociology*. 7th edition. Toronto: Pearson Canada.

- Mader, C. 1974. *Information Systems: Technology, Economics, Applications*. Chicago: Science Research Associates, Inc.
- Magsig, D.E. 1995. *Information Warfare: In the Information Age*. [Online] Available: <http://carlisle-www.army.mil/usacsl/divisions/std/branches/iw/tutorial/refer.htm>. Accessed: 6 December 2004.
- Maiden, S. 2015. Australia Declares Cyber War on Islamic State's Social Media Propagandists. *The Sunday Telegraph*. 15 February. [Online] Available: <http://www.dailytelegraph.com.au/news/nsw/australia-declares-cyber-war-on-islamic-states-social-media-propagandists/story-fni0cx12-1227219902546>. Accessed: 16 February 2015.
- Malaska, P. & Virtanen, I. 2009. Theory of Futuribles and Historibles. *Futura* 28(1), 65-84.
- Mangold, P. 1990. *National Security and International Relations*. London: Routledge.
- Marsh, B.1998. Using Scenarios to Identify, Analyze, and Manage Uncertainty. In Fahey, L. & Randall, R.M. (Eds.). *Learning from the Future: Competitive Foresight Scenarios*. New York: John Wiley & Sons Inc.
- Martin, P.Y. & Turner, B.A. 1986. Grounded Theory and Organizational Research. *The Journal of Applied Behavioral Science*, 22(2), 141-157.
- Masini, E.B. 1993. *Why Future Studies?* London: Grey Seal.
- Masini, E.B. 2005. Invisible Made Visible. Volume 4: The Views of Futurists. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.
- Matthews, W. 2009. *The New Next Generation*. [Online] Available: <http://www.facebook.com/ext/share.phpsid=87084903281&h=HE95Z&u=Oup2A&ref=nf>. Accessed: 8 June 2009.
- Mayer-Schoenberger, V. & Brodnig, G. 2001. *Information Power: International Affairs in the Cyber Age*. John F. Kennedy School of Government Harvard University Faculty Research Working Papers Series RWP01-044, November.
- Mayring, P. 2000. Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 1(2), Art. 20. [Online] Available: <http://nbn-resolving.de/urn:nbn:de:0114-fqs0002204> Accessed: 22 May 2015.

Mazarr, J.M. 1997. *Global Trends 2005: The Challenge of the New Millennium*. Cambridge, MA: Center for International Studies.

McCgwire, M. 2001. The Paradigm that lost its Way. *International Affairs*, **77**(4), 777-803.

McCuen, J. 2008. Hybrid Wars. *Military Review*, **88**(2), 107-113.

McCullagh, P. 1980. Regression Models for Ordinal Data. *Journal of the Royal Statistical Society. Series B (Methodological)*, **42**(2), 109-142.

McDevitt, C. 2009. *Cyberattack Aftermath*. [Online] Available: <http://www.reuters.com/article/bigMoney/idUS292302408420090709>. Accessed: 9 July 2009.

McGrew, A.G, 1992. Conceptualizing Global Politics. In Baylis, J. & Rengger, N.J. (Eds.), *Dilemmas of World Politics: International Issues in a Changing World*. Oxford: Clarendon Press.

McHale, J.A. 2009. *Public Diplomacy: A National Security Imperative*. Address by Under Secretary of State at the Center for a New American Security in Washington, DC., 11 June 2009. [Online] Available: <http://www.state.gov/r/remarks/124640.htm>. Accessed: 11 June 2009.

McKendrick, J. 2015. *Why the Internet of Things Heralds the Next Great Economic Disruption*. [Online] Available: <http://www.forbes.com/sites/joemckendrick/2015/03/25/is-the-internet-of-things-heralding-the-next-great-economic-shift/>. Accessed: 1 April 2015.

McLendon, J.W. 2008. *Information Warfare: Impacts and Concerns*. [Online] Available: <http://warandgame.wordpress.com/2008/02/24/information-warfare-impacts-and-concerns/>. Accessed: 2 March 2008.

McSweeney, B. 1996. Identity and Security: Buzan and the Copenhagen School. *Review of International Studies*, **22**, 81-93.

Mediatechno Blog. 2008. *A Different Kind of Net-Centric Warfare in Iraq*. [Online] Available: <http://patch1hotmailcom.blogspot.com/2008/05/different-kind-of-net-centric-warfare.html>. Accessed: 5 May 2008.

Merriam-Webster. 2015. [Online] Available: <http://www.merriam-webster.com/dictionary/complex>. Accessed: 25 May 2015.

Miles, M.B. & Huberman, A.M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. 2nd edition. London: Sage Publications.

Milojević, I. 2014. *The Evolution of Foresight and Its Impact on Policy Making: Case studies from Australia and Asia*. Paper for the European Commission's Joint Research Centre. [Online] Available: [https://ec.europa.eu/jrc/sites/default/files/fta2014-t3practice\\_198.pdf](https://ec.europa.eu/jrc/sites/default/files/fta2014-t3practice_198.pdf) Accessed: 5 March 2015.

Mohammed, A. 2013. Deepening Income Inequality. World Economic Forum. Global Agenda Trend 1. [Online] Available: <http://reports.weforum.org/outlook-global-agenda-2015/top-10-trends-of-2015/1-deepening-income-inequality>. Accessed: 26 September 2015.

Molander, R.C., Riddile, A.S & Wilson, P.A. 1996. *Strategic Information Warfare: A New Face of War*. Santa Monica: National Defense Research Institute.

Molander, R.C., Wilson, P.A., Mussington, D.A. & Mesic, R.F. 1998. *Strategic Information Warfare Rising*. Santa Monica: Rand Corporation.

Molitor, G.T.T. 1977. How to Anticipate Public-Policy Changes. *SAM Advanced Management Journal*, 4 - 13.

Molitor, G.T.T. 2003. Molitor Forecasting Model: Key Dimensions for Plotting the "Patterns of Change." *Journal of Futures Studies*, 8(1), 61-72.

Morgenthau, H.J. 1973. *Politics Among Nations: The Struggle for Power and Peace*. 5th edition. New York: Alfred A. Knopf.

Morozov, E. 2009. *The Fog of Cyberwar: NATO military strategists are waking up to the threat from online attacks*. [Online] Available: <http://www.newsweek.com/id/194605>. Accessed: 21 April 2009.

Morozov, E. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Morrison, J.L. 1992. Environmental Scanning. In Whitely, M.A., Porter, J.D. & Fenske, R.H. (Eds.), *A Primer For New Institutional Researchers*. Tallahassee: The Association for Institutional Research.

Morse, J.M. 1994. Emerging from the data: The cognitive process of analysis in qualitative enquiry. In J.M. Morse (Ed.), *Critical Issues in Qualitative Research Methods*. Thousand Oaks, CA: Sage.

Murphy, D. 2006. Preface. In Murphy, D., Groh, J.L., Smith, D.J. & Ayers, C.E. (Eds.), *Information as Power: An Anthology of Selected United States Army War College Student Papers, Volume 1*. Carlisle: US War College.

Naisbitt, J. 2009. *Prophecy on China's Megatrends*. Interview on CCTV 9 Programme Dialogue. [Online] Available: [http://english.cctv.com/program/e\\_dialogue/20091026/101838.shtml](http://english.cctv.com/program/e_dialogue/20091026/101838.shtml) English Channel 2009-10-26 10:06:42. Accessed: 26 October 2009.

National Planning Commission. 2011. *National Development Plan: Vision for 2030*. Pretoria: South African Government.

Naude, J. H. 2016. *Constructive environmental scanning: A method in creating positive world paradigms for more sustainable alternative futures*. Unpublished PhD Thesis. Stellenbosch: Stellenbosch University.

Nicholson, M. 2002. *International Relations: A Concise Introduction*. 2nd edition. New York: New York University Press.

Nielsen, C. & Thangadurai, M. 2007. Janus and the Delphi oracle: Entering the new world of international business research. *Journal of International Management*, **13**(2), 147-163.

Niiniluoto, I. 2002. *Critical Scientific Realism*. Oxford: Oxford Scholarship Online.

North Atlantic Treaty Organisation (NATO). 2010. *NATO 2020: Assured Security; Dynamic Engagement: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*. 7 May. [Online] Available: [http://www.nato.int/cps/en/natolive/official\\_texts\\_63654.htm](http://www.nato.int/cps/en/natolive/official_texts_63654.htm). Accessed: 7 May 2010.

North Atlantic Treaty Organisation (NATO). 2015. *Cyber Security*. [Online] Available: [http://www.nato.int/cps/en/natohq/topics\\_78170.htm](http://www.nato.int/cps/en/natohq/topics_78170.htm). Accessed: 2 August 2015.

Nye, J.S. 1990a. *Bound To Lead: The Changing Nature of American Power*. New York: Basic Books.

Nye, J.S. 1990b. Soft Power. *Foreign Policy*, 80, 153-171.

Nye, J.S. 2011. *The Future of Power*. New York: PublicAffairs.

Nye, J.S. 2005. *Understanding International Conflicts: An Introduction to Theory and History*. New York: Pearson Education.

Nye, J.S. & Owens, W.A. 1996. America's Information Edge. *Foreign Affairs*, No. 75, March/April.

O'Callaghan, J.R. & Evans, D.P. 1973. Problems of Power: Modification versus Innovation [and Discussion]. *Philosophical Transactions*, **267**(882).

Ogilvy, J. 2005. Abstract: Scenario Planning, Art or Science? *World Futures: The Journal of Global Education*, **61**(5), 331-346.

Ogilvy, J. & Schwartz, P. 1998. *Plotting Your Scenarios*. Global Business Network.

Okello, F., Ayres, R., Bullock, P., Erhili, B., Harding, B. & Perdigao, J. 1996. *Information Warfare: Planning the Campaign*. Research paper presented to the Directorate of Research Air Command and Staff College, ACSC/DEC/124/96-04.

Okoli, C. & Pawlowski, S.D. 2004. The Delphi method as a research tool: An example, design considerations and applications. *Information and Management*, **42**(1), 14-29.

Oman, C. 1999. Globalization, Regionalization, and Inequality. In Hurrell, A. & Woods, N. (Eds.), *Inequality, Globalization, and World Politics*. Oxford: Oxford University Press.

Oxford Dictionaries. 2014. [Online] Available: <http://www.oxforddictionaries.com/definition/english/expert> Accessed: 12 Augustus 2014.

Palmer, J. 2015. All-seeing, All-knowing: Since Imperial Times Chinese Governments have Yearned for a Perfect Surveillance State. Will Big Data Now Deliver It? *Aeon Magazine*, 16 February. [Online] Available: <http://aeon.co/magazine/technology/will-china-use-big-data-as-a-tool-of-the-state/>. Accessed: 17 February 2015.

Parks, P.J. 2013. *The Digital Divide*. San Diego: ReferencePoint Press, Inc.

- Patman, R.G. 2006. Globalization and the End of the Cold War. In Patman, R.G. (Ed.), *Globalization and Conflict: National Security in a 'New' Strategic Era*. New York: Routledge.
- Patomäki, H. 2002. *After International Relations Critical Realism and the (Re) Construction of World Politics*. London: Routledge.
- Peerenboom, R. 2011. The Future of Law in a Multi-Polar World: Toward a Global New Deal. In Muller, S., Zouridis, S., Frishman, M. & Kistemaker, L. (Eds.), *The Law of the Future and The Future of Law*. Oslo: Torkel Opsahl Academic EPublisher.
- Pensky, M. 2005. Globalizing Theory, Theorizing Globalization: Introduction. In Pensky, M. (Ed.), *Globalizing Critical Theory*. Lanham: Rowman and Littlefield Publishers.
- Pick, J.B. & Sarkar, A. 2015. *The Global Digital Divides: Explaining Change*. Heidelberg: Springer.
- Pillkahn, U. 2008. *Using Trends and Scenarios as Tools for Strategy Development Shaping the Future of Your Enterprise*. Erlangen: Publicis Corporate Publishing.
- Pinker, S. 2011. *The Better Angles of our Nature: Why Violence has Declined*. New York: Viking.
- Popper, K. 1962. *Conjectures and Refutations: The Growth of Scientific Knowledge*. New York: Basic Books.
- Powell, C. 2003. The Delphi Technique: Myths and Realities. *Journal of Advanced Nursing*, **41**(4), 376-382.
- Prince, G. 2002. *The Heart of War: On Power, Conflict and Obligation in the Twenty-First Century*. London: Routledge.
- Princeton University. 2015. *Futurology*. [Online] Available: <http://wordnetweb.princeton.edu/perl/webwns=futurology> Accessed: 11 May 2015.
- Ralston, B. & Wilson, I. 2006. *The Scenario-Planning Handbook: A Practitioner's Guide to Developing and Using Scenarios to Direct Strategy in Today's Uncertain Times*. Mason: Thomson South-Western.
- Rappert, B. & Croft, S. 2007. Introduction. In Rappert, B. (Ed.), *Technology and Security: Governing Threats in the New Millennium*. Basingstoke: Palgrave Macmillan.

- Reid, N. 1988. The Delphi Technique: Its Contribution to the Evaluation of Professional Practice. In Ellis, R. (Ed.), *Professional Competence and Quality Assurance in the Caring Professions*. London: Chapman and Hall.
- Richard, H., Rohm, A. & Crittenden V.L. 2011. We're all Connected: The Power of the Social Media Ecosystem. *Business Horizons*, **54**(3), 265-273.
- Richards, J. 2009. Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. *International Affairs Review*, **18**(2). [Online] Available: <http://www.iaar-gwu.org/node/65>. Accessed: 31 July 2015.
- Richter, W.E. 2009. The Future of Information Operations. *Military Review*, January-February, 103-113.
- Ringland, G. 2006. Introduction to Scenario Planning. In Ringland, G. & Young, L. (Eds.), *Scenarios in Marketing: From Vision to Decision*. Chichester: John Wiley & Sons Ltd.
- Riordan, S. 2003. *The New Diplomacy*. Cambridge: Polity.
- Ritzer, G. 2007. *Contemporary Sociological Theory and Its Classical Roots, the Basics*, 2nd edition. New York, NY: McGraw Hill.
- Ritzer, G. & Goodman, D.J. 2004. *Sociological Theory*. 6th edition. New York: McGraw Hill.
- Roach, S. 2013. Critical Theory. In Dunne, T, Kurki, M. & Smith, S. (Eds.), *International Relations Theories Discipline and Diversity*. 3rd edition. Oxford: Oxford University Press.
- Robb, J. 2007. *Brave New War: The Next Stage of Terrorism and the End of Globalization* Hoboken: John Wiley & Sons.
- Robertson, D. 2002. *The Routledge Dictionary of Politics*. 3<sup>rd</sup> edition. London: Routledge.
- Robinson, E. 2005. Becoming a Foresight Practitioner. Volume 1: Foundations. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Roggio, W. 2014. ISIS announces formation of Caliphate, rebrands as 'Islamic State'. [Online] Available: [http://www.longwarjournal.org/archives/2014/06/isis\\_announces\\_formation\\_of\\_ca.php](http://www.longwarjournal.org/archives/2014/06/isis_announces_formation_of_ca.php) Accessed: 19 July 2016.

Rosenau, P. 1990. Once Again into the Fray: International Relations Confronts the Humanities. *Millennium: Journal of International Studies*, **19**(1), 83-110.

Ross, A.L. 1993. The Dynamics of Military Technology. In Dewitt, D., Haglund, D. & Kirton, J. *Building a New Global Order*. Don Mills: Oxford University Press Canada.

Rossouw, J. 2002. Groepverdoemenis, oftewel die geval van "Generasie Z". LitNet. [Online] Available: <http://www.oulitnet.co.za/seminaar/jrgenz.asp>. Accessed: 30 March 2008.

Rothkopf, D.J. 1998. Cyberpolitik: The Changing Nature of Power in the Information Age. *Journal of International Affairs*, **51**(2), 325-359.

Roux, A. 2006. *Thinking about the future and scenarios*. Presentation by the Director of the Institute for Future Studies, SANAI, Pretoria, 25 October.

Roux, A. 2007. *Scanning the Environment*. Master's in Futures Studies presentation, Module: Scanning the Environment. Bellville: University of Stellenbosch Business School.

Roux, A. 2012. Discussion with author on the Delphi Method. 26 June, Beijing.

Rowe, E. 1994. Enhancing Judgment and Decision Making: A critical and empirical investigation of the Delphi technique. Unpublished PhD thesis. Bristol: University of Western England.

Rowe, G. & Wright, G. 1999. The Delphi technique as a forecasting tool: Issues and analysis. *International Journal of Forecasting*, **15**(4), 353-375.

Rowe, G. & Wright, G. 2001. Expert Opinions in Forecasting: The Role of the Delphi Technique. In Armstrong, J.S. (Ed.), *Principles of Forecasting: A Handbook for Researchers and Practitioners*. Boston: Kluwer Academic Publishers.

Rowe G., Wright G. & Bolger F. 1991. Delphi: A re-evaluation of research and theory. *Technical Forecasting Social Change*, **39**(3), 235-251.

Russo, F. 2009. *Causality and Causal Modelling in the Social Sciences: Measuring Variations*. New York: Springer.

Sackman, H. 1974. *Delphi Assessment: Expert Opinion, Forecasting, and Group Process*. R-1283-PR. Report prepared for United States Air Force Project Rand. Santa Monica: Rand.

Saffo, P. 2007. Six Rules for Effective Forecasting. *Harvard Business Review*. July/August Issue. [Online] Available: <https://hbr.org/2007/07/six-rules-for-effective-forecasting> Accessed 26 July 2016.

Said, A.A., Lerche, C.O. (Jr) & Lerche III, C.O. 1995. *Concepts of International Politics in Global Perspective*. 4th edition. Englewood Cliffs: Prentice Hall.

Saldaña, J. 2009. *The Coding Manual for Qualitative Researchers*. London: Sage.

Sandholtz, W. 1999. Globalization and the Evolution of Rules. In Prakash, A. & Hart, J.A. (Eds.), *Globalization and Governance*. London: Routledge.

Sanger, D.E., Markoff, J. & Shanker, T. 2009. *U.S. Steps Up Effort on Digital Defenses*. [Online] Available: <http://www.nytimes.com/2009/04/28/us/28cyber.html?hp> Accessed: 29 April 2009.

Scheibe, M., Skutsch, M. & Schofer, J. 1975. Experiments in Delphi Methodology. In Linstone, H.A. & Turoff, M. (Eds.), *The Delphi Method: Techniques and Applications*. Reading: Addison-Wesley.

Schneier, B. 2008. *America's Dilemma: Close Security Holes, or Exploit Them Ourselves*. [Online] Available: [http://www.wired.com/politics/security/commentary/securitymatters/2008/05/blog\\_securitymatters\\_0501](http://www.wired.com/politics/security/commentary/securitymatters/2008/05/blog_securitymatters_0501) Accessed: 4 May 2008.

Scholtz, R. 2009. *Internal Corporate Venturing as a Tool for Corporate Renewal*. Unpublished MA Thesis. Stellenbosch: University of Stellenbosch.

Schwartz, W. 1996. *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*. 2nd edition. New York: Thunder's Mouth Press.

Schwartz, P. 1991. *The Art of the Long View: The Path to Strategic Insight for Yourself and Your Company*. New York: Doubleday Dell.

Schwartz, P. & Ogilvy, J.A. 1998. Plotting Your Scenarios. In Fahey, L. & Randall, R.M. (Eds.), *Learning from the Future: Competitive Foresight Scenarios*. New York: John Wiley & Sons Inc.

SearchNetworking.com. 2015. *Networks*. [Online] Available: <http://searchnetworking.techtarget.com/definition/network> Accessed: 20 May 2015.

Searle, J.R. 1995. *The Construction of Social Reality*. New York: The Free Press.

Segal, N. 2007. *Breaking the Mould: The Role of Scenarios in Shaping South Africa's Future*. Stellenbosch: Sun Press.

Senge, P.M. 1990. *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York: Doubleday.

Senge, P.M., Smith B., Kruschwitz, N., Laur, J. & Schley, S. 2008. *The Necessary Revolution: How Individuals and Organizations are Working Together to Create a Sustainable World*. London and Boston: Nicholas Brealey Publishing.

Sheehan, M. 2000. *National and International Security*. Dartmouth: Ashgate Publishing.

Shaughnessy, H. 2015. *Shift: A User's Guide to the New Economy*. New York: Tru Publishing.

Shulsky, A.N. 1993. *Silent Warfare: Understanding the World of Intelligence*. 2nd edition. Washington DC: Brassey's.

Singer, P.W. & Friedman, A. 2014. *Cybersecurity and Cyberwar: What Everyone Needs To Know*. Oxford: Oxford University Press.

Singh, J.P. 2002. Introduction: Information Technologies and the Changing Scope of Global Power and Governance. In Rosenau, J.N. & Singh, J.P., *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. New York: State University of New York Press.

Situated Relational Biosensing (SiReBi). 2011. *Participatory Systems: Introduction*. [Online] Available: [http://www.sirebi.org/open/Intro\\_ParticipatorySystems.pdf](http://www.sirebi.org/open/Intro_ParticipatorySystems.pdf) Accessed: 4 August 2015.

Skagestad, P. 1981. Hypothetical realism. In Brewer & Collins, B.E. (Eds.), *Scientific Inquiry and the Social Sciences*. San Francisco: Jossey-Bass.

- Skulmoski, G.J., Hartman, F.T. & Krahn, J. 2007. The Delphi Method for Graduate Research. *Research Journal of Information Technology Education*, 6, 1-21.
- Slaughter, A. 2004. Introduction. In Slaughter, A., Bildt, C. & Ogura, K., *The New Challenges to International, National and Human Security Policy*. The Triangle Papers: 58, Washington DC: The Trilateral Commission.
- Slaughter, R.A. 1994. Why we should care for future generations now? *Futures*, 26(10), 1077-1085.
- Slaughter, R.A. 1995. *The Foresight Principle: Cultural Recovery in the 21st Century*. London: Adamantine.
- Slaughter, R.A. 1999. *Futures for the Third Millennium: Enabling the Forward View*. Sydney: Prospect Media.
- Slaughter, R.A. 2005a. Futures Concepts. Volume 1: Foundations. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.
- Slaughter, R.A. 2005b. Series Introduction. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.
- Smith, D. 2005. *Strategic Roadmaps*. White Paper by Technology Futures Inc. [Online] Available: [http://tfi.com/pubs/w/pdf/ti\\_sroadmaps.pdf](http://tfi.com/pubs/w/pdf/ti_sroadmaps.pdf) Accessed: 6 May 2015.
- Smith, S. 1997. New Approaches to International Theory. In Baylis, J. & Smith, S. (Eds.), *The Globalization of World Politics*. Oxford: Oxford University Press.
- Smith, S. 2013. Introduction: Diversity and Disciplinarity in International Relations. In Dunne, T., Kurki, M. & Smith, S. (Eds.), *International Relations Theories Discipline and Diversity*. 3rd edition. Oxford: Oxford University Press.
- Snijders, C., Matzat, U. & Reips, U-D. 2012. 'Big Data': Big Gaps of Knowledge in the Field of Internet. *International Journal of Internet Science*, 7(1), 1-5.
- Snow, D.M. 2004. *National Security for a New Era: Globalization and Geopolitics*. New York: Pearson Longman.

- Social-Media.com. 2009. *Social Media*. [Online] Available: <http://cncc.bingj.com/cache.aspx=social+media=76658085814259&mkt=zh-CN&setlang=en-US&w=fffad18a,b3e484bb> Accessed: 14 September 2009.
- Spence, M. 2010. *The Next Convergence: The Future of Economic Growth in a Multispeed World*. New York: Picador.
- Spies, P. 2005. Measuring and Making the Future. Volume 4: The Views of Futurists. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.
- Spies P. 2015. *Futures Studies' 'Holy Trinity' within the Context of a Trained Futures Mind*. Stellenbosch: Institute for Futures Research, Stellenbosch University. Learning Hub Lecture Notes, Principles of Futures Studies.
- Stacy, R. 2008. *The Social Media Revolution: Post-Gutenberg Revolution*. Presentation, 26 November in Budapest at Kreative Magazine's Digital PR conference. [Online] Available: <http://www.slideshare.net/RichardStacy/the-social-media-revolution-presentation-809948> Accessed: 7 April 2015.
- Stanford Encyclopaedia of Philosophy. 2006. *Aristotle on Causality*. [Online] Available: <http://plato.stanford.edu/entries/aristotle-causality/> Accessed: 24 July 2015.
- Stanko, J. 2013. *Social Media, Political Upheaval, and State Control*. Unpublished Master's thesis. St Louis: Graduate School of Arts and Sciences, Washington University.
- Stein, G.J. 1995. Information Warfare. *Airpower Journal*, **9**(1), 30-39.
- Sterling-Folker, J. 2006. Postmodernism and Critical Theory. In Sterling-Folker, J. (Ed.), *Making Sense of International Relations Theory*. Boulder: Lynne Rienner Publishers.
- Stiegler, B. 1998. *Technics and Time, 1: The Fault of Epimetheus*. Stanford: Stanford University Press.
- Strange, S. 1996. *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge: Cambridge University Press.
- Strauss, A.L. & Corbin, J.M. 1998. *Basics of Qualitative Research Techniques and Procedures for Developing Grounded Theory*. 2nd edition. Thousand Oaks: Sage Publications.

Striglitz, J. 2002. *Globalization and its Discontents*. London: Penguin Books.

Suddendorf, T., Addis, D.T & Corballis, M. 2009. Mental Time Travel and the Shaping of the Human Mind. *Philosophical Transactions of the Royal Society*. B (2009) 364, 1317–1324.

Suganami, H. 1997. *On the Causes of War*. Oxford: Oxford University Press.

Surowiecki, J. 2004. *The Wisdom of Crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations*. New York: Doubleday.

Swinburne, R.G. 1966. Knowledge of Past and Future. *Analysis*, **26**(5), 166-172.

Szafranski, R.A. 1995. Theory of Information Warfare: Preparing for 2020. *Airpower Journal*, **9**(1), 56-65. [Online] Available: <http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm> Accessed: 10 January 2008.

Taipale, K.A. 2006. *Deconstructing Information Warfare*. Presentation by the Executive Director of the Center for Advanced Studies in Science and Technology Policy to the Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare at the National Academies, Washington D.C. 30 October.

Taleb, N. 2007. *The Black Swan: The Impact of the Highly Improbable*. London: Penguin Books.

Teece, D.J. 2010. Business Models, Business Strategy and Innovation. *Long Range Planning*, **43**(2-3), 172-194.

Thefreedictionary.com. 2015. [Online] Available: <http://www.thefreedictionary.com/addition> Accessed: 25 May 2015.

The World Bank. 2015. *Poverty Overview*. [Online] Available: <http://www.worldbank.org/en/topic/poverty/overview> Accessed: 29 July 2015.

Thomson, I. 2008. *Georgia gets allies in Russian cyberwar*. [Online] Available: <http://www.vnunet.com/vnunet/news/2223776/georgia-gets-allies-russian-cyberwar> Accessed: 13 August 2008.

Thuraisingham, J.J.E. 2005. *Mystic Journey*. Volume 4: The Views of Futurists. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Toffler, A. 1970. *Future Shock*. London: The Bodley Head.

Toffler, A. 1980. *The Third Wave*. London: Bantam Books.

Toffler, A. 1990. *Powershift, knowledge, wealth and violence at the edge of the 21st century*. London: Bantam.

Toffler, A. & Toffler, H. 1993. *War and anti-war: Survival at the dawn of the 21st century*. New York: Little, Brown and Company.

Trager, F.N. & Simonie, F.L. 1973. An Introduction to the Study of National Security. In Trager, F.N. & Kronenberg, P.S. (Eds.), *National Security and American Society: Theory, Process, and Policy*. Lawrence: University Press of Kansas.

Tuck, C. 2008. Land Warfare. In Jordan, D., Kiras, J.D., Lonsdale, D.J., Speller, I., Tuck, C. & Walton, C.D., *Understanding Modern Warfare*. Cambridge: Cambridge University Press.

Twitchett, K.J. 1971. Strategies for Security: Some Theoretical Considerations. In Twitchett, K.J. (Ed.), *International Security: Reflections on Survival and Stability*. London: Oxford University Press.

Tzu, S. 1963. *The Art of War*. New York: Oxford University Press.

United Nations of America. 2004. *Report of the Secretary-General's High-level Panel on Threats, Challenges and Change, A More Secure World: Our Shared Responsibility*. [Online] Available: [http://www.un.org/en/peacebuilding/pdf/historical/hlp\\_more\\_secure\\_world.pdf](http://www.un.org/en/peacebuilding/pdf/historical/hlp_more_secure_world.pdf). Accessed: 2 July 2014.

United Nations Development Programme (UNDP). 1994. *Human Development Report 1994*. Oxford: Oxford University Press.

University of Arizona. 2006. *Tutorial 2: Building Scenarios*. University of Arizona Course on Methods and Approaches for Studying the Future. [Online] Available: <http://cals.arizona.edu/futures/tou/tut2-buildscenarios.html>. Accessed: 8 November 2006.

- University of Pittsburgh. 2015. *Coding Analysis Toolkit (CAT)*. Qualitative Data Analysis Program (QDAP). [Online] Available: <http://cat.ucsur.pitt.edu/app/main.aspx>. Accessed: 18 to 20 May 2015.
- UPI Newswire. 2007. *Israel used Cyberwar against Syria*. 13 December.
- Upton, G. & Cook, I. 1996. *Understanding Statistics*. Oxford: Oxford University Press.
- Vail, J. 2007. *What is Rhizome?* [Online] Available: <http://www.jeffvail.net/2007/01/what-is-rhizome.html>. Accessed: 5 December 2008.
- Van Creveld, M. 1999. The Future of War. In Patman, R.G., *Security in a Post-Cold War World*. Basingstoke: Macmillan Press.
- Van der Heijden, K. 2004. Afterword: Insights into Foresight. In Tsoukas, H. & Shepherd, J. (Eds.), *Managing the Future: Strategic Foresight in the Knowledge Economy*. Malden: Blackwell Publishing Ltd.
- Van der Heijden, K. 2005. *Scenarios: The Art of Strategic Conversations*. Chichester: John Wiley & Sons Inc.
- Van der Laan, L. & Yap, J. 2016. *Foresight & Strategy in the Asia Pacific Region: Practice and Theory to Build Enterprises of the Future*. Singapore: Springer.
- Van Niekerk, B. & Maharaj, M. 2013. Social Media and Information Conflict. *International Journal of Communication*, **7**, 1162-1184.
- Van Notten, P.W.F. 2014. After the Arab Spring: An Opportunity for Scenarios. *European Journal for Futures Research*, **2**(1), 1-6.
- Van Vuuren, R. 2003. *Nuclear Non-Proliferation: The South African experience in global context*. Unpublished MA Thesis. Pretoria: University of South Africa.
- Van Vuuren, R. 2009. Inligtingsoorlogvoering, die Opkomende Magprojekteringinstrument: Soeke na 'n Definisie. *LitNet Akademies*, **6**(2), August.
- Van Vuuren, R. 2011. Toekomststudie: Instrument vir Toekomsskepping. *LitNet Akademies*, **8**(2), August.

vcpost.com. 2015. *Anonymous Hacker Group Declares Cyber War Against ISIS, Destroying Hundreds Of Websites, Social Media Accounts*. [Online] Available: <http://www.vcpost.com/articles/42831/20150213/anonymous-hacker-group-declares-cyber-war-against-isis-destroying-hundreds-htm> Accessed: 16 February 2015.

Velamoor, S. 2005. Human Futures: An eternal play. Volume 3: Directions and Outlooks. In Slaughter, R.A. (Ed.), *Knowledge Base of Future Studies*. Foresight International, CD-ROM.

Vernardakis, N. 2016. *Innovation and Technology: Business and Economics Approaches*. New York: Routledge.

Ventre, D. (Ed). 2011. *Cyberwar and Information Warfare*. London: ISTE Ltd & John Wiley and Son Inc.

Ventre, D. 2009. *Information Warfare*. London: ISTE Ltd & John Wiley and Son Inc.

Viotti, P.R. & Kauppi, M. 1999. *International Relations Theory: Realism, Pluralism, Globalism, and Beyond*. Boston: Allyn & Bacon.

Vlahos, M. 1998. The emergence of the Infosphere and its Impact on Military Operations. In Campen, A.D. & Dearth, D.H. (Eds.), *Cyberwar 2.0: Myths, Mysteries and Reality*. Fairfax: AFCEA International Press.

Von Clausewitz, C. 1989. *On War*. Princeton: Princeton University Press.

Von der Gracht, H.A. 2012. Consensus Measurement in Delphi Studies: Review and Implications for Future Quality Assurance. *Technological Forecasting and Social Change*, **79**(8), 1525-1536.

Voros, J. 2006. Introducing a Classification Framework for Prospective Methods. *Foresight*, **8** (2), 43 – 56.

Vreÿ, F. 2005. *An Analysis of the Evolving Military Futures Debate: Explaining Alternative Military Futures for the South African National Defence Force*. Unpublished PhD Thesis Stellenbosch: University of Stellenbosch.

Wakefield, R. & Watson, T. 2013. A Reappraisal of Delphi 2.0 for Public Relations. *Public Relations Review*, **40**(3), 577-584.

- Walton, S. 2001. *Performance and Innovation Unit Strategic Futures Drivers Synthesis*. Farnborough: Defence Evaluation and Research Agency.
- Waltz, E. 1998, *Information Warfare: Principles and Operations*. Boston: Artech House.
- Waltz, K.N. 1987. The Balance of Power in International Politics. In Votti, P.R. & Kauppi, M. (Eds.), *International Relations Theory: Realism, Pluralism, Globalism*. New York: Macmillan Publishing Company.
- Waltz, K.N. 1979. *Theory of International Politics*. Boston: McGraw Hill.
- Wasserman, S. & Faust, K. 1994. *Social Network Analysis: Methods and Applications*. Cambridge: University Press.
- Watson, I. 2012. CNN at SXSW: Social Media in the Arab Spring. [Online] Available: [https://www.youtube.com/watch?v=1bSj4f9f8Eg&desktop\\_uri=%2Fwatch%3Fv%3D1bSj4f9f8Eg&app=desktop](https://www.youtube.com/watch?v=1bSj4f9f8Eg&desktop_uri=%2Fwatch%3Fv%3D1bSj4f9f8Eg&app=desktop). Accessed: 4 August 2015.
- Webopedia. 2009. *Astrourfing*. [Online] Available: <http://www.webopedia.com/sgsearch/results?cx=partner-pub-8768004398756183%3A6766915980&cof=FORID%3A10&ie=UTF-8&q=Astrourfing>. Accessed: 5 June 2009.
- Webster, F. 2005. Information. In Bennett, T., Grossberg, L. & Morris, M. (Eds.), *New Keywords: A Revised Vocabulary of Culture and Society*. Malden: Blackwell Publishing.
- Weis, B.X. 2015. *From Idea to Innovation: A Handbook for Inventors, Decision Makers and Organizations*. Berlin: Springer-Verlag.
- Weltman, J.J. 1995. *World Politics and the Evolution of War*. Baltimore: The Johns Hopkins University.
- Whitham, B. 2014. *The Neoliberal Way of War: A Critical Analysis of Contemporary British Security in Policy and Practice*. Unpublished PhD thesis. Reading: University of Reading.
- Widnall S.E. & Fogelman, R.R. 1997. *Cornerstones of Information Warfare*. Doctrine/Policy Document, United States Air Force.
- Wight, C. 2006. *Agents, Structures and International Relations*. Cambridge: Cambridge University Press.

Wight, C. & Joseph, J. 2010. Scientific Realism and International Relations. In Joseph, J. & Wight, C. (Eds.), *Scientific Realism and International Relations*. Basingstoke: Palgrave Macmillan.

Wight, M. 1966. Western Values in International Relations. In Butterfield, H. & Wight, M. (Eds.), *Diplomatic Investigations: Essays in the Theory of International Politics*. London: George Allen and Unwin.

Wight, M. 1991. *International Theory: The Three Traditions*. London: Leicester University Press.

Williams, P. 2001. Transnational Criminal Networks. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: National Defence Research Institute, RAND.

Wilson, C. 2007. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. CRS Report for Congress, 20 March, Washington DC: Congressional Research Service (CRS).

Wilson, I. 1998. Mental Maps of the Future: An Intuitive Logic Approach to Scenarios. In Fahey, L. & Randall, R.M. (Eds.), *Learning from the Future: Competitive Foresight Scenarios*. New York: John Wiley & Sons Inc.

Wing, I. 2002. *Australian Defence in Transition: Responding to New Security Challenges*. Unpublished PhD thesis. Sydney: University of New South Wales.

World Economic Forum (WEF). 2015. *Global Risks 2015*. Geneva: WEF.

World Future Society (WFS). 2005. Methods, CLA. *Future Survey*, 27(8).

Young, O.R. 1967. *Systems of Political Science*. Englewood Cliffs: Prentice-Hall Inc.

Zetter, K. 2015. A Cyberattack has Caused Confirmed Physical Damage for the Second Time Ever. [Online] Available: <http://www.wired.com/2015/01/german-steel-mill-hack-destruction/>. Accessed: 8 January 2015.

Zickmund, S. 2009. *Qualitative Coding 101: Strategies for Coding Texts and Using a Qualitative Software Program*. Cyber Seminar. Center for Health Equity Research and Promotion (CHER). [Online] Available: [http://www.hsrp.research.va.gov/for\\_researchers/cyber\\_seminars/archives/hsrm-061410.pdf](http://www.hsrp.research.va.gov/for_researchers/cyber_seminars/archives/hsrm-061410.pdf). Accessed: 29 May 2015.

Ziegler, D.W. 2000. *War, Peace and International Politics*. New York: Longman.

## APPENDIX A: THEMATIC QUALITATIVE TEXT CODING OF THE ENVIRONMENTAL SCAN OUTPUT

**TABLE A: 1 Example of coding of text in categories and sub-categories done by using the Coding Analysis Toolkit (CAT) provided and developed by the University of Pittsburgh's Qualitative Data Analysis Program (QDAP) (Raw initial unedited text version)**

Category / Subcategory	CAT Coding Paragraph
Innovation: Modification	Technology, in the context of this study, does not just refer to artefacts (devices, equipment, machines or material objects) but also knowing how to achieve practical purposes in the world. It includes methods and systems which are the result of scientific knowledge being used for practical reasons.]
Transformation: Renewal	Material technologies are much more visible because their roles in change are more identifiable than the social and intellectual technologies (laws, institutions and theories) (Cornish, 2004:14– 15). As humanity's scientific understanding grows, so too does the ability to engineer instruments to manipulate the world (Rappert and Croft, 2007:5).
Transformation: Renewal	Intellectual technologies do, however, play a significant role in the changes in society's power structures and remains, especially relevant to the use of information as a power instrument, in a world where there is increased consciousness of certain values such as human rights that cross national frontiers (Nye, 2005:260).
Innovation: Modernization	Technological progress provides a useful perspective for analysing the rapid phase of change currently experienced in global society. The main driving force in recent socio-economic development seems to be the accumulation and use of technological knowledge. Thus changes in society have speeded up enormously in recent centuries due to rapid technological innovation and progress, which leads to massive change in the economy, government, and institutions of society (Cornish, 2004:20)
Transformation: Revolution	Through the ages technological development has been an indispensable trigger for change. See Table 5.1 for a

	summary of the benefits, uses and effects of the three major technological revolutions experienced by humanity namely the agricultural, industrial and information ages. The previous ages (agricultural and industrial) do not go away, they just become layered sequentially parts of humanity' s history of socio-economic and political evolution (Houle, 2013:13).
Transformation: Revolution	The current age can also be called the "age of technology", but the more apt name is the information age. The idea of the information age comes from the writings of Toffler (1970 and 1980), whose 'wave-theory' of technological and civilization enhancing development argues that human history can be seen as the unfolding of three successive and overlapping technological revolutions or waves (i.e. the agricultural, industrial and informational)
Innovation: Modification	Currently humanity is experiencing the ascendancy of the Third Wave, namely the informational age, with its associated developmental transformations (Kilibarda, 2003). The benefits of pervasive technologies include economic productivity, global collaboration, e-commerce, efficiencies and change in government and society, information richness, data-rich scientific and technological advances, political transparency, and societal knowledge (Pick and Sarkar, 2015:1).
Transformation: Shift	Increasingly, in the information age, technology and information are interdependent, with advances in one entailing and dependent on, advances in the other. The expanding flow of information, the evolution of the global economy, and the creation of the internet are all factors in development, boosting innovation and globalisation (Masini, 2005). Information and communication technology continues to remain central to continuing innovation.
Networks: Interconnecting	While computing devices are the most visible symbols of globalization, ICT is also proving to be one of the most potent agents of change. No area of the world and no arena of politics, economics, society, and culture are immune from the pervasive impact of computer technology (Kegley and Wittkopf, 1997:251).
Networks: System	ICT can be regarded as a force multiplier (Bendrath, 1999). Miniaturization, growing capacity and software innovation have propelled computing devices rapid worldwide spread. These devices owe their growth and impact to a phenomenon dubbed Moore' s Law (after Gordon Moore, the founder of Intel), which says that computing power and capacity double every eighteen months. This exponential growth has led to the digital revolution impacting on practically all spheres of life (Kegley and Wittkopf, 1997:

	251)
Transformation: Renewal	Although computer technology and especially the Internet are agents of a rapidly globalizing world, wide differences exist in different countries' ability to shape (and be shaped by) a computer-driven technocratic world (Kegley and Wittkopf, 1997:252).
Innovation: Addition	Despite overall growth a global digital divide remains pervasive. There remain distinct geographic patterns of technology utilization worldwide, and continents and countries have fairly persistent relative high or low levels of information technologies. Likewise, within states, and provinces, regions are uneven in geographic patterns of prevalence of information technologies (Pick and Sarkar, 2015:1). Although the digital divide is a problem throughout the world, developing states struggle far more than industrialized states (Parks, 2013:8).
Networks: Complex	Focusing on the immediate future key ICT trends include: ongoing innovation in integrated applications, storage, display technology, wireless transmission media, omnipresence / pervasiveness of technology and continuous innovation with software applications (Butler, 2008:Slide 11). Additional trends include the expansion of mobile applications and big data analytics growing exponentially (ITWeb, 2014)
Transformation: Renewal	The effects of the ICT trends and the information age in general are much more profound than just the explosion of the use of information but the significant impact on most aspects of modern society and economy. The decreasing cost and increasing performing power of computing devices have led to the application of information technologies in virtually all corners of society (Arquilla and Ronfeldt, 1997:52). Information technology presents humanity with remarkable ability to network and to simultaneously localise and globalise (glocalisation), decentralise and centralise, fragment and integrate (Linstone, 2005).
Transformation: Shift	The information revolution is transforming the role various types of actors play in international relations. The information revolution has altered the role and operation of governments and their policy-makers in four ways. First, there is more information available to governments; indeed governments may have access to too much information. Paralysis through information overload is a real and growing threat and policy-makers need to prioritise. Second, global networks provide decision-makers with options to centralize or decentralise decision-making. Third, global networks erode the monopoly of information available to governments. Fourth, global networks advance transparency and thereby accentuate the global interest and involvement

	regarding issues such as environmental challenges, making it difficult for countries unilaterally to take national policy decisions when the problem is global (Aronson, 2001:549). Although states will remain the dominant actor globally, they will be challenged and find it increasingly difficult to control. A much larger part of the population both within and among countries has access to the power that comes from information (Nye, 2011:114).
Networks: System	While technological development, especially related to the ICT/digital fields is exponential, this should not be viewed from a technology determinism vantage point. Complexity and change are not all new to the contemporary world, but were already widely discussed in the 1960s and the 1970s. Back then, as now, developments in the technical sphere continually seem to outpace the capacity of individuals and social systems to adapt. Thus, the notion of “out-of-control” technology and fears of vulnerabilities due to dependency on technology are recurring themes in political and philosophical thought (Cavelty, 2007:21).
Transformation: Revolution	Although, fears of technology slipping out of human control for now or the near future are unfounded, technology is having a significant impact on human society in general. Enabled by technological change, humanity is experiencing a series of economic, social, and cultural adaptations that make possible a radical transformation of how the information environment is used by individuals, citizens, and members of cultural and social groups (Benkler, 2006:2).
Transformation: Renewal	Technology development in the information age results frequently in technology competitive disruptions, if technological breakthroughs result in players changing the rules of competition. The result can be hyper competition and conditions that are analogous to warfare (Ashton and Klavans, 1997:56). This competition coupled with the fragmenting consequences of technology do pose significant challenges to government and social harmony if misused.
Modification	Changes brought about by technology and especially ICT related technologies have both globalising and fragmenting consequences. See Table 5.2 for the globalising and fragmenting consequences of transport, telecommunication, television and IT technologies. Despite the positive consequences of these technologies, there is also negative influence resulting in a potential fault lines in society. This consequently also had an effect on the nature of conflict and war in society.
Networks: Complex	The role of technology developments especially networking related technologies are critical elements influencing the global security environment in the information age. The transformative power relations boosted by technology are

	coming to the fore, especially in so far as fomenting transformative social change (Dator, Sweeney and Yee, 2014:20).
Transformation: Shift	The disruptive and destructive potential of technology can be expected to play a noteworthy role in the future as individuals and entities explore the potential power projection related value of these technologies. While the technological impact have a significant effect on all identified environments the links between the technological and war/conflict environment are especially relevant for the manifestation of information warfare.
Transformation: Shift	Changes brought about by the advancement of technology, especially during the information age also had a profound effect on the war and conflict environment. As Toffler and Toffler (1993:3) state: “ A revolutionary new economy is arising based on knowledge, rather than conventional raw materials and physical labor (sic). This remarkable change in the world economy is bringing with it a parallel revolution in the nature of warfare.”

**APPENDIX B:  
DELPHI ADMINISTRATION**

**TABLE B: 1 Round 1 Delphi Questionnaire**

	<b>Driving Force influencing the future manifestation of Information Warfare</b>	Please Mark		<b>Your Comments</b> Suggested changes, arguments, questions:
		Current Significance	Futures Relevancy	
		1 = Least Important	10 = Most Important	
1	Globally the centre of power is shifting, enhancing the political, social and economic influence of individuals and sub-state's entities in the world.	1 2 3 4 5	1 2 3 4 5	
2	Security is increasingly becoming a more encompassing, globally influenced and networked phenomenon.	6 7 8 9 10	6 7 8 9 10	
3	Integration of systems, processes are exponential in the information age.	1 2 3 4 5	1 2 3 4 5	
4	Despite the dominance of integration many human endeavours are also faced with systemic stress as challenges associated with centralization and decentralization are impacting on entities globally.	6 7 8 9 10	6 7 8 9 10	
5	Symbolic, information related phenomena are increasingly impacting on behaviour.	1 2 3 4 5	1 2 3 4 5	
6	The speed of change is increasing exponentially while global communication became instantaneous.	6 7 8 9 10	6 7 8 9 10	

7	<b>Non-state actors</b> increasing their influence on international politics but especially related to national security.	1 2 3 4 5 6 7 8 9 10	1 2 3 4 5 6 7 8 9 10	
8	<b>Global inequality</b> in terms of economic, social and technological access continues to be a major global challenge.	1 2 3 4 5 6 7 8 9 10	1 2 3 4 5 6 7 8 9 10	
9	<b>ITC is embedding itself</b> as a crucial part of society.	1 2 3 4 5	1 2 3 4 5	
10	<b>Social media</b> is a significant part of communication and this is expected to grow in the future.	6 7 8 9 10 1 2 3 4 5	6 7 8 9 10 1 2 3 4 5	
11	The <b>threshold</b> required to <b>exploit</b> the advantages of information technology is relatively low and decreasing rapidly as the recursive simplicity within the ITC sector, which supports a clear trend of ever expanding growth in access, availability, and speed with a simultaneous reduction in cost and skill barriers	6 7 8 9 10 1 2 3 4 5 6 7 8 9 10	6 7 8 9 10 1 2 3 4 5 6 7 8 9 10	

Identify any additional driving forces which would be relevant in the context of the future manifestation of information warfare.	
---	--

**APPENDIX C:****DELPHI ADMINISTRATION: LETTER FOR FIRST ROUND DELPHI****TABLE C: 1 Letter provided with first round Delphi questionnaire**

<b>PARTICIPATION IN A STUDY ON THE FUTURE OF INFORMATION WARFARE</b>
<p>I am currently a part time PhD candidate at the Business School of the University of Stellenbosch. The topic of my dissertation is "Information Warfare as Future South African National Security Threat."</p> <p>As an individual with relevant knowledge and experience applicable to how information warfare is going to manifest in the future, I would highly appreciate it, if you could participate in a Delphi Study on the future of information warfare.</p> <p>Information warfare is a phenomenon confronting us nearly daily in the news media. Many difficulties remains associated with this phenomenon including differences of definitions, marketing hype by companies with vested interests, sensationalized news reports, efforts by businesses not to provide information because of sensitive nature of losses.</p> <p>It is assumed that no person has a way of knowing the future, but the aim here is to obtain expert insight on the issue of information warfare from individuals' knowledgeable about a diverse range of fields. You are specifically requested to participate because of your knowledge and experience relevant to the possible future manifestation of information warfare. These inputs will serve as basis to develop broad consensus on possible future scenarios related to the manifestation of information warfare as a national security threat.</p> <p>The aim of the study is to identify the most significant contemporary driving forces which will impact on the manifestation of information warfare by 2030. (For the purpose of this study information warfare is defined as actions focused on destabilizing or manipulating the core information networks of a state or entity in society with the aim of influencing the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state. The definition proposed for information warfare encompasses three forms of manifestation of information warfare, namely netwar, psychological warfare and cyberwarfare.)</p> <p>Attached is a questionnaire with 11 potential driving forces statements. Please measure these driving forces' impact on the manifestation of information warfare, firstly against their current relevancy and secondly against their potential impact by 2030. The identified driving forces stems from an environmental analysis conducted previously, but please feel free to add modify or reject these driving forces. Also please provide analysis and or motivations as far as possible. During the first round of the Delphi the aim is to generate a wide spectrum of opinions. Feedback will be provided to move towards consensus on these driving forces. No more than three rounds will be conducted, so participating in this Delphi Study would not be a burden on your time, a valuable commodity today.</p> <p>Participation in this study will be in line with the following principles:</p> <p><b>Informed consent:</b> Participants must give their consent.</p> <p><b>Voluntary participation:</b> Participants will be informed that, inter alia, they have the right to refuse to answer questions and to withdraw from participation at any time.</p> <p><b>Privacy:</b> Steps will be taken to ensure that personal data of participants will be secured from improper access.</p> <p><b>Confidentiality and anonymity:</b> Confidentiality of information and anonymity of participants will be maintained unless waived by the participant.</p>

**APPENDIX D:**  
**DELPHI ADMINISTRATION**  
**TABLE D: 1 Second Delphi Round 1 Delphi Questionnaire Example**

	Driving Force influencing the future manifestation of Information Warfare	Please Mark		Comments Suggested changes, arguments, questions:
		Current Significance ① = Least Important ② ③ ④ ⑤	Futures Relevancy ⑩ = Most Important ① ② ③ ④ ⑤	
1	The centre of power is shifting from the traditional developed countries to the developing countries	① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ Collective group score: 5.5 Your score: 7	① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ Collective group score: 6.8 Your score: 9	Your Comment: None  Other comments: Yes. But I think we're in the very early stages of this shift and, if that is so, then the tensions between the two worlds could be high as the developing tries to assert power it does not yet have and the other finds it increasingly difficult to exert yesterday influence. However, 2030 may be too close for this to be a very important factor.  Only some developing countries - in mainly Asia - have and will have the necessary technological advances currently and in the near future.  Certainly I see power shifting in the way described but I am less certain that this will be a driver for IW - or a result

			<p>of it. I suppose I think that it would have happened without the shift in power-blocks.</p> <p>The definition of power is unclear here. Moreover, the statement contains a state-centric bias.</p> <p><b>Remark: Realists postulate that any political unit (such as a state) will act in such a way as to maximise its power, which is defined mainly in terms of the security of its territory. Political power can be seen as a psychological relation between those who exercise it and those over whom it is exercised. Those who exercise power gain control by actions which have an impact on the minds of those over whom it is exercised. The impact derives from three sources, namely " ...the expectation of benefits, the fear of disadvantages, and the respect or love for men and institutions." Power may be exerted through orders, threats, the authority or charisma of person or of an office, or a combination of any of these.</b></p> <p>Additional Remarks:</p>
2	<p>Security in a networked environment will increase in complexity as its physical and non-physical elements become more tightly interwoven.</p> <p>Definition of security is included as suggested in previous round:</p> <p>Security refers to being protected or safe from</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score : 6.5</p>	<p>Your Comment: None</p> <p>Other comments:</p> <p>I think that this cannot be seriously challenged. The complexity of the networked world presents opportunities for criminals and other never-do-wells. In the absence of a cataclysm, this will increase and offer even more</p>

<p>harm.</p>	<p>Your score: 5</p> <p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score: 5.2</p> <p>Your score: 8</p>	<p>Your score: 9</p> <p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score: 6.8</p> <p>Your score: 9</p>	<p>opportunities.</p> <p>The definition of security is unclear here.</p> <p>Additional Remarks:</p> <p>Your Comment: None</p> <p>Other comments:</p> <p>Include a definition of "centripeta!" and "centrifugal" forces. I interpreted it as opposing Forces.</p> <p>I was slightly unclear about this point but I think I understand it. The convergence in some matters seems to be counterbalanced by a balkanisation. On the principle that IW gives power to smaller players with a grievance – I see this point as similar to 4, 7 and 11.</p> <p>Do not really understand the question.</p> <p>I am unsure what these centripetal/centrifugal forces are.</p> <p>The definition of forces is unclear here.</p> <p>This could be constant over time i.e. the ever present forces of change – so I wouldn't regard it as a peculiar driving force.</p>
<p>3</p> <p>An increase in integration and polarisation will contribute to systemic stresses.</p> <p>Round One this driving force was formulated as follows:</p> <p>Systemic stresses from clashing centripetal and centrifugal forces will increase exponentially.</p>			

4	Information warfare will become a growing option for power projection.	<p>1 2 3 4 5</p> <p>6 7 8 9 10</p> <p>Collective group score : 6.5</p> <p>Your score: 7</p>	<p>1 2 3 4 5</p> <p>6 7 8 9 10</p> <p>Collective group score : 8.9</p> <p>Your score: 8</p>	<p>Question is somewhat confusing and 5 is therefore given for both.</p> <p><b>[General Remark: Driving force reformulated based on feedback]</b></p> <p>Additional Remarks:</p>	<p>Your Comment: None</p> <p>Other comments: I think that this is the most powerful driver of its increase today but I believe that countermeasures will mature and in due course, other things will finally supplant it.</p> <p>Reference to information – rather than cyber - warfare is unclear. [Remark: Information warfare is a more encompassing term than cyberwarfare which is a constituent element thereof. The definition proposed for information warfare encompasses three forms of manifestation of information warfare, namely netwar, psychological warfare and cyberwarfare.]</p> <p>Additional Remarks:</p>
---	--	---	---	--	--

5	<p>Symbolic, information related phenomena are increasingly impacting on behaviour.</p> <p>Symbolic refers to representations (in the media and social media) which reflect perceived reality.</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score: 6.4</p> <p>Your score: 6</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score: 8</p> <p>Your score: 8</p>	<p>Your Comment: None</p> <p>Other comments:</p> <p>This is more subtle and a fascinating point which possibly could be the subject of a PhD on its own. Being unsure about the answer to this has been one of the reasons for delay in reply. I think that there can be no contest that the point is true and it is seen in recent ISIS related matters (and I am sure lots of other things). Possibly my scores should be higher.</p> <p>Do not really think it is important.</p> <p>I'm unsure what behaviour refers to here. Behaviour of the general public? <b>[Remark: Behaviour refers to the way in which people conducts themselves toward others and the world in general.]</b></p> <p>Venturing into the realm of symbolism requires elaboration on the importance of political rituals.</p> <p>Additional Remarks:</p>
---	--	--	--	---

6	<p>The speed of change is increasing exponentially with global communication becoming instantaneous.</p> <p>Definition of change is included as suggested in previous round:</p> <p>Change refers to the act or process of transforming which results in a change in form, appearance, nature, or character.</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩ Collective group score : 6.5 Your score: 8</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩ Collective group score : 8.6 Your score: 9</p>	<p>Your Comment: None</p> <p>Other comments: Security vulnerability discovery (as a main driving force behind cyber attacks) isn't so much a factor of the speed of communication, but the integrity of software. [Remark: This is the case in terms of the cyber aspect, but the definition of information warfare addresses power related influence on cognitive continuum for which speed is a relevant issue]</p> <p>Change is not defined here.</p> <p>Additional Remarks:</p>
7	<p>Non-state actors are increasing their influence related to global security.</p> <p>Minor reformulation based on feedback received.</p> <p>Original formulation</p> <p>Non-state actors increasing their influence on international politics but especially related to national security.</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩ Collective group score : 6.8 Your score: 5</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩ Collective group score : 8.5 Your score: 8</p>	<p>Your Comment: None</p> <p>Other comments: I saw some link between this point and number 4. Again, the recent events in Iraq come to mind. The US government also because involved in the recent cyber attack on Sony.</p> <p>Does the statement assume that non-state actors are influential in international politics but not influential in international security? [Remark: Non-state actors are</p>

8	<p>Global and Intra-regional inequalities are stimulating conflict potential.</p> <p>Reformulation based on feedback received.</p> <p>Original formulation</p> <p>Global inequality in terms of economic, social and technological access continues to be a major global challenge</p>	<p>1 2 3 4 5</p> <p>6 7 8 9 10</p> <p>Collective group score : 5.8</p> <p>Your score: 7</p>	<p>1 2 3 4 5</p> <p>6 7 8 9 10</p> <p>Collective group score : 7.9</p> <p>Your score: 5</p>	<p>influential in both international politics and international security]</p> <p>Additional Remarks:</p>	<p>Your Comment: None</p> <p>Other comments:</p> <p>My problem with this was whether I though global inequality was going to increase – not whether it was a driver.</p> <p>I think inequality will decrease.</p> <p>The difference in economic/social/technological gains as a means of polarizing nations may contribute to the increase of information warfare.</p> <p>Statement vague. Global inequality continues to be a major global challenge. But: the qualifier ('in terms of economic, social and technological access') should be rephrased.</p> <p>Global and intra-regional inequality in terms of economic, social and technological access continues to be a major global challenge.</p>
---	--	---	---	--	--

9	Information communication technology (ICT) is embedding itself as a crucial part of society.	<p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score : 8.1</p> <p>Your score: 6</p>		<p><b>[General Remark: Driving force reformulated based on feedback]</b></p> <p>Additional Remarks:</p>
		<p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score : 9.1</p> <p>Your score: 9</p>		<p>Your Comment: None</p> <p>Other comments:</p> <p>I think this is undeniable in the absence of some catastrophic change -- but catastrophic change does sometimes happen.</p> <p>Increased ubiquity implies increased opportunity for IW.</p> <p>The present day significance is in that the shift is still ongoing, from isolation and separation to highly integrated global connection. Eventually in the mid-term future, it will be a forgone expectation that everything is interconnected and integrated, like the roads we have to getting anywhere. As a subject, ICT as it get enhanced and integrated will become less of a concern, just as our road infrastructure which is crucial, but not something we think about. Over-time, advancements become trivialised and decline in importance as subjects of discourse.</p> <p><b>Not all technology is related to communication. [Remark: Yes that is the case. The focus in this study remains on</b></p>

10	<p>Social media is a significant part of communication and this is expected to grow in the future.</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score : 7.4 Your score: 6</p>	<p>①②③④⑤ ⑥⑦⑧⑨⑩</p> <p>Collective group score : 9 Your score: 9</p>	<p>the communication aspect and influence of technologies. However, even technologies not previously associated with communication are being connected by the expected exponential rise of telemetry in terms of fast developing Internet of Things (IoT))</p> <p>Additional Remarks:</p>
				<p>Your Comment: None</p> <p>Other comments:</p> <p>Also undeniable. 15 year olds now will be 30 in 2030 and in positions of influence.</p> <p>I think social media has reached its peak.</p> <p>On a nation-state conflict level, protection of classified information is prioritized over social media-related information.</p> <p>Additional Remarks:</p>

<p>Any additional comments on driving forces which would be relevant in the context of the future manifestation of information warfare.</p>	<p>Your comment: None</p> <p>Other comments:  The World Economic Forum identified a number of trends in their latest Risk Report, eg. Hyper-connectivity. They also refer to cyber-security as one of the 10 main risks. Very interesting.</p> <p>Information can be defined as many things including commands and algorithms driving machines. As the world progresses into the a-Commerce driven economy within the next few decades and we see mass automation where our cars and aeroplanes function autonomously, information warfare of the future will be about gaining access information to the machines, programmes and systems for the purpose of manipulation for sabotage; it is a real threat that if the road transportation system in the future is hacked and hijacked, the very vehicles that transport us and our inventory will become weapons used against us. That includes passenger planes. The trouble with network technology is that, the machines could be hijacked and abused remotely. In a-Commerce model of business, sabotage means disappearance of account, money and information critical to continuation or recovery of business. Nations could cripple nations without deploying a single soldier by such information warfare outcomes.</p> <p>Some of the above seems to be about asymmetric conflicts and terrorism without saying so. The possibility of the non-governmental groups being terrorist groups focuses the mind. Is the world still moving away from divisions around ideology and towards divisions on culture? If so this could be driver. The embedded nature of IT making us more vulnerable could be made more of. It seems to up the ante on terrorism. Once upon a time terrorists could threaten to place a bomb to cause disruption and fear. Now they just need to threaten a network.</p>
---	--

## APPENDIX E: DELPHI ADMINISTRATION: LETTER FOR THE SECOND ROUND DELPHI

TABLE E: 1 Letter provided with second round Delphi questionnaire

<p><b>PARTICIPATION IN A STUDY ON THE FUTURE OF INFORMATION WARFARE: ROUND TWO</b></p> <p>It is much appreciated that you participated in the First Round of the Delphi Study aimed at identifying the most significant contemporary driving forces which will impact on the manifestation of information warfare<sup>30</sup> by 2030.</p> <p>Feedback and ratings have been received from all panel members. Based on these some changes have been made to the formulation of the driving forces. Your response to the first round questionnaire is included for easy reference. The average score for each dimension is listed as well as the score you provided.</p> <p>It would be appreciated if you could again consider each driving force and make a judgement on the score you provided in the context of the collective average Likert score of the Delphi Group. The comments from the other Delphi participants are also included in the questionnaire. Your rating can stay the same or be closer or further away from the average rating. Any additional comments would also be appreciated.</p> <p>Participation in this study will be in line with the previously stated principles:</p> <p><b>Informed consent:</b> Participants must give their consent.</p> <p><b>Voluntary participation:</b> Participants will be informed that, inter alia, they have the right to refuse to answer questions and to withdraw from participation at any time.</p> <p><b>Privacy:</b> Steps will be taken to ensure that personal data of participants will be secured from improper access.</p> <p><b>Confidentiality and anonymity:</b> Confidentiality of information and anonymity of participants will be maintained unless waived by the participant.</p> <p>Thanks again for your willingness to participate in this study.</p> <p>Rianne van Vuuren 8 January 2015</p>
--

---

<sup>30</sup> For the purpose of this study information warfare is defined as actions focused on destabilizing or manipulating the core information networks of a state or entity in society with the aim of influencing the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state. The definition proposed for information warfare encompasses three forms of manifestation of information warfare, namely netwar, psychological warfare and cyberwarfare.

## APPENDIX F: PILOT DELPHI STUDY: ROUND 1 RESULTS

**TABLE F: 1 Results of Pilot Delphi Study's first round**

A Current Significance

	PM03	PM06	PM07	PM08	PM09	PM10	PM11	PM12	PM14	PM15	Total	Average
Q1	5	5	4	3	6	9	6	7	10	8	63	6.3
Q2	6	6	7	7	5	8	7	8	7	6	67	6.7
Q3	6	7	4	7	6	8	6	7	6	7	64	6.4
Q4	7	5	6	6	5	9	5	8	7	4	62	6.2
Q5	7	5	7	7	5	8	5	8	5	5	62	6.2
Q6	7	8	7	8	7	10	6	8	7	6	74	7.4
Q7	7	4	4	8	3	9	7	7	7	4	60	6
Q8	7	6	3	8	4	9	6	7	9	8	67	6.7
Q9	9	8	7	8	8	10	6	8	7	6	77	7.7
Q10	7	8	8	8	5	9	7	8	7	7	74	7.4
Q11	7	8	6		7	8	6	8	7	6	63	7

B Futures Relevancy

Q1	5	5	6	5	9	9	9	9	10	5	72	7.2
Q2	7	8	8	10	6	9	9	9	8	8	82	8.2
Q3	7	9	8	9	9	9	10	10	8	7	86	8.6
Q4	7	5	4	8	5	10	8	6	6	4	63	6.3
Q5	8	5	8	9	7	9	6	10	6	5	73	7.3
Q6	7	10	9	10	10	10	10	10	9	8	93	9.3
Q7	7	4	8	8	6	10	9	10	10	3	75	7.5
Q8	5	8	4	10	7	9	8	9	9	5	74	7.4
Q9	9	10	8	10	10	10	8	10	9	8	92	9.2
Q10	8	10	9	10	8	10	10	10	9	9	93	9.3
Q11	7	10	9		9	10	8	10	9	8	80	8.888889

**APPENDIX G:**  
**PILOT DELPHI STUDY: ROUND 2 RESULTS**

**TABLE G: 1 Results of Pilot Delphi Study's second round**

A Current Significance

	PM03	PM06	PM07	PM08	PM09	PM10	PM11	PM12	PM14	PM15	Total
Q1	5	7	4	6	6	7	6		10		51
Q2	6	7	8	6	6	7	6		8		54
Q3	6	7	3	7	6	7	7		6		49
Q4	6	9	5	7	6	5	7		5		50
Q5	7	6	7	7	5	7	6		7		52
Q6	7	9	7	8	7	8	7		7		60
Q7	7	5	4	7	6	8	8		6		51
Q8	7	7	4	7	4	8	6		6		49
Q9	8	8	7	8	8	9	6		7		61
Q10	7	8	8	7	5	9	8		8		60
Q11	7	8	7	6	7	8	6		7		56

B Futures Relevancy

Q1	6	8	6	7	8	8	8		10		61
Q2	7	7	9	7	7	8	10		9		64
Q3	7	8	6	9	9	9	10		7		65
Q4	7	9	7	9	9	7	9		6		63
Q5	8	6	8	9	7	8	6		7		59
Q6	7	10	9	9	10	8	10		9		72
Q7	7	6	8	7	8	9	10		7		62
Q8	6	8	5	8	7	9	8		7		58
Q9	8	10	9	10	10	10	7		10		74
Q10	8	10	9	9	9	10	10		9		74
Q11	7	10	9	7	9	9	8		9		68

## APPENDIX H: SECOND DELPHI STUDY: ROUND 1 RESULTS

**TABLE H: 1 Results of the Second Delphi Study's first round**

**A Current Significance**

	PM01	PM02	PM03	PM05	PM06	PM15	PM14	PM16	PM17	PM18	PM19	Total	Average
Q1	7	3	8	6	5	5	5	4	4	10	4	61	5.545455
Q2	5	3	7	8	5	10	7	7	8	8	4	72	6.545455
Q3	8	5	1	6	5	10			5	4	3	47	5.222222
Q4	7	6	4	10	5	10		6	5	7	5	65	6.5
Q5	6	6	10	7	2	6	5	7	6	9	6	70	6.363636
Q6	8	6	10	7	5	6	2	7	7	7	7	72	6.545455
Q7	5	6	10	9	5	10	7	7	5	5	6	75	6.818182
Q8	7	6	10	7	5	6	6	6	8	7	7	75	6.818182
Q9	6	7	10	9	10	10	7	8	8	7	7	89	8.090909
Q10	6	6	10	9	6	10	7	7	7	8	5	81	7.363636

**B Futures Relevancy**

Q1	9	4	10	4	7	7	5	5	7	10	7	75	6.818182
Q2	9	10	10	9	8	10	7	9	8	9	9	98	8.909091
Q3	9	6	3	8	5	10			5	6	9	61	6.777778
Q4	8	10	8	9	9	10		8	8	10	9	89	8.9
Q5	8	9	10	7	2	10	6	9	9	10	8	88	8
Q6	9	9	9	9	9	10	2	10	9	9	10	95	8.636364
Q7	8	9	10	9	5	10	7	9	8	9	10	94	8.545455
Q8	5	9	10	9	4	8	8	7	9	8	10	87	7.909091
Q9	9	10	3	9	10	10	9	10	10	10	10	100	9.090909
Q10	9	10	10	9	7	10	7	10	9	9	9	99	9

## APPENDIX I: SECOND DELPHI STUDY: ROUND 2 RESULTS

**TABLE I: 1 Results of the Second Delphi Study's second round**

**A Current Significance**

	PM01	PM02	PM03	PM05	PM06	PM15	PM14	PM16	PM17	PM18	PM19	Total	Average
Q1		3	8	6	5		5	4	4	5	5	45	5
Q2		7	7	8	5		7	7	8	6	5	60	6.666667
Q3		5	1	6	5		5		5	5	5	37	4.625
Q4		6	4	10	5		7	6	5	7	5	55	6.111111
Q5		7	10	8	6		6	7	6	7	6	63	7
Q6		6	10	7	7		6	7	7	7	7	64	7.111111
Q7		6	10	9	6		7	7	5	7	6	63	7
Q8		7	10	7	6		6	6	8	7	7	64	7.111111
Q9		7	10	9	10		7	8	8	8	8	75	8.333333
Q10		7	10	9	7		7	7	7	7	7	68	7.555556

**Futures Relevancy**

Q1		6	10	5	7		6	5	7	7	7	60	6.666667
Q2		9	10	9	8		8	9	8	9	9	79	8.777778
Q3		7	3	8	5		5		5	7	8	48	6
Q4		9	8	10	9		9	8	8	9	9	79	8.777778
Q5		9	10	8	6		7	9	9	9	8	75	8.333333
Q6		9	9	9	9		7	9	9	9	9	79	8.777778
Q7		9	10	9	7		7	9	8	9	9	77	8.555556
Q8		9	10	9	7		8	7	9	8	8	75	8.333333
Q9		10	3	9	10		9	10	10	9	10	80	8.888889
Q10		9	10	9	7.5		7	10	9	9	9	79.5	8.833333