UNIVERSITY OF KWAZULU-NATAL

VULNERABILITY ASSESSMENT OF MODERN ICT INFRASTRUCTURE FROM AN INFORMATION WARFARE PERSPECTIVE

By

Brett van Niekerk

991160530

A thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

In Information Systems and Technology

School of Management, IT, and Governance

College of Law and Management Studies

Supervisor: Professor Manoj S. Maharaj

2011

Permission to Submit

Supervisor's permission to submit for examination

Date:

Student Name: Brett van Niekerk

Student no.: 991160530

Dissertation Title: Vulnerability Assessment of Modern ICT Infrastructure from an Information Warfare Perspective

As the candidate's supervisor I agree to the submission of this dissertation for examination. **To the best of my knowledge, the dissertation is primarily the student's own work and the student has acknowledged all reference sources.**

The above student has also satisfied the requirements of English language competency.

Name of Supervisor: Prof. Manoj S. Maharaj

Signature:

Declaration

I, Brett van Niekerk, declare that:

(i) The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.

(ii) This dissertation/thesis has not been submitted for any degree or examination at any other university.

(iii) This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced;

b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

(vi) This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signed: …….. Date:……..

Acknowledgements

Such an undertaking would not be possible without the support of those around the candidate, all of whom contributed to making this project a fulfilling experience. Firstly, appreciation needs to be given to my supervisor, Prof. Manoj Maharaj, for his enthusiastic guidance and support throughout the period of the study.

As with any project, financial support is required; this was provided for through the UKZN Doctoral Grant and the LEDGER Program of Armscor and the Department of Defence, through the Cyber-defence research group of the Council for Scientific and Industrial Research Defence, Peace, Safety and Security.

Appreciation is given to those who participated in the study, and those who assisted with the various arrangements thereof. Special thanks should go to my colleagues and friends with whom I published and with whom we formed a support group: Trishana Ramluckan, Kiru Pillay, Peter Denny, and Nurudeen Ajayi.

And lastly I would like to express my gratitude to my family, in particular my parents Matthys and Dawn van Niekerk, for their much appreciated support and patience through this project and my previous studies.

Abstract

The overall objective of the study is to provide a vulnerability assessment of the mobile communications infrastructure to information warfare attacks; this study has a South African focus. The mobile infrastructure was selected as the infrastructure and mobile devices incorporate the majority of modern ICT technologies, namely social networking, wireless connectivity and mobility, mass storage, as well as the telecommunications elements. The objectives of the study are to:

- Propose a new information warfare model, and from this deduce a vulnerability assessment framework from the specific information warfare perspective. These are the guiding frameworks and model for the study.
- Gather information regarding threats and vulnerabilities, with particular focus on potential use in information warfare and relevance to South Africa.
- Establish the criticality of the mobile infrastructure in South Africa.
- Use the gathered information in the vulnerability assessment, to assess the vulnerability of the mobile infrastructure and related devices and services.

The model and framework are generated through desk-based research. The information is gathered from research protocols that are relevant to both research and risk and vulnerability assessment, these include: expert input through interviews and a research workshop, incident and trend analyses through news and vendor reports and academic publishing, computer simulation, questionnaire survey, and mathematical analyses. The information is then triangulated by using it in the vulnerability assessment.

The primary and secondary data shows that attacks on confidentiality are the most prevalent for both computer-based networks and the mobile infrastructure. An increase in threats and incidents for both computer and mobile platforms is being seen. The information security trends in South Africa indicate that the existing security concerns are likely to worsen, in particular the high infection rates. The research indicates that the mobile infrastructure is critical in South Africa. The study validates the proposed framework, which indicates that South Africa is vulnerable to an information warfare attack in general. Key aspects of vulnerability in the mobile infrastructure are highlighted; the apparent high load of the mobile infrastructure in South Africa can be seen as a high risk vulnerability. Suggestions to mitigate vulnerabilities and threats are provided.

Contents

List of Figures

List of Tables

List of Abbreviations

3G	-	Third generation
API	-	Application programming interface
AuC	-	Authentication centre
BER	-	Bit error rate
C2	-	Command and control
C2W	-	Command and control warfare
CDMA	-	Code-division multiple-access
CERT	-	Computer emergency response team
CI	-	Critical infrastructure
CII	-	Critical information infrastructure
CIKR	-	Critical infrastructure and key resources
CIP	-	Critical infrastructure protection
CIIP	-	Critical information infrastructure protection
COMINT	-	Communications intelligence
CSIRT	-	Computer security incident response team
DDoS	-	Distributed denial of service
DII	-	Defence information infrastructure
DoC	-	Department of Communications
DoS	-	Denial of service
DPSA	-	Department of Public Services and Administration
DS-CDMA	-	Direct-spread code-division multiple-access
EDGE	-	Enhanced data rates for GSM evolution
EIR	-	Equipment identity register

ELINT	-	Electronic intelligence
EM	-	Electromagnetic
EMCON	-	Emissions control
EMP	-	Electromagnetic pulse
EMS	-	Electromagnetic spectrum
ERP	-	Effective radiated power
ESME	-	External short messaging entity
EW	-	Electronic warfare
FAIR	-	Factor analysis of information risk
FRAAP	-	Facilitated risk analysis and assessment process
GII	-	Global information infrastructure
GPRS	-	General packet radio service
GSM	-	Global system for mobile communications
HLR	-	Home location register
IaaS	-	Infrastructure as a service
IBW	-	Intelligence based warfare
ICT	-	Information and communications technology
IDS	-	Intrusion detection system
IED	-	Improvised explosive device
IEEE	-	Institute for Electrical and Electronic Engineers
IIW	-	Information infrastructure warfare
IO	-	Information operations
IOP	-	Instrument of power
ISP	-	Internet service provider
IW	-	Information warfare

JSR	-	Jamming to signal ratio
LPI	-	Low probability of interception
MAC	-	Media access control
MEII	-	Minimum essential information infrastructure
MMC	-	Multi-media card
MMS	-	Multimedia message service
MSC	-	Mobile switching centre
NETINT	-	Network intelligence
NIA	-	National Intelligence Agency
NII	-	National information infrastructure
NIST	-	National Institute for Standards and Technology
NW	-	Network warfare
OCTAVE	-	Operationally critical threat, asset, and vulnerability evaluation
OII	-	Organisational information infrastructure
PaaS	-	Platform as a service
PESTEL	-	Political, economic, social, technical, environmental, and legal
PSTN	-	Public switched telephone network
PSYOP	-	Psychological operations
SaaS	-	Software as a Service
SANDF	-	South African National Defence Force
SDCCH	-	Stand-alone dedicated control channel
SIGINT	-	Signals intelligence
SIM	-	Subscriber identity module
SIW	-	Strategic information warfare
SMS	-	Short message service

SNR	-	Signal to noise ratio
SMME	-	Small, medium, and micro enterprise
SMSC	-	Short message service centre
SWOT	-	Strengths, weaknesses, opportunities, and threats
URL	-	Universal resource locator
USAF	-	United States Air Force
USB	-	Universal serial bus
VLR	-	Visitor location register
VOIP	-	Voice over Internet Protocol
WAP	-	Wireless access protocol
WEP	-	Wired equivalent privacy
WCDMA	-	Wideband code division multiple access
WLAN	-	Wireless local area network
WPA	-	Wi-Fi protected access

Chapter 1. Introduction

1.1 Introduction

This chapter introduces the thesis and research study. The background to the study is provided in Section 1.2, and the problem is stated in Section 1.3. The objectives of the study and relevant methodologies used are introduced in Section 1.4, and the relevance of the study is discussed in Section 1.5. The layout of the thesis and the research output from this thesis are presented in Sections 1.6 and Section 1.7, respectively. Section 1.8 presents writing conventions, and Section 1.9 concludes the chapter.

1.2 Background

This section presents the background to the study; many concepts will be summarised here, as they will be covered in more detail in the literature review. The growth of the Internet and World Wide Web has resulted in the networking and connection of many infrastructures and persons. This effectively has connected malicious actors electronically with potential targets for attack or exploitation.

During the 1990s the concept of information warfare (IW) gained prominence, particularly in the United States (Armistead, 2010; Kopp, 2000). This encompassed a number of areas, some of which were relatively old, and others still emerging. Of particular concern were the emerging threats due to the growth of the Internet; it was realised that malicious actors could potentially access and disrupt infrastructures that were of national strategic importance, and therefore considered critical. The initial concept that attacks could be mounted on the critical infrastructure through the Internet was named "strategic information warfare" (Molander, Riddile, & Wilson, 1996; Molander, Wilson, Mussington, & Mesic, 1998). A series of publications also highlighted the possibility of a virtual "cyber-war" or "netwar" (Arquilla & Ronfeldt, 1996; 1997; 2001). The overall concept of IW, and the extended philosophy of information operations (IO), is still developing and undergoing changes as researchers and practitioners attempt to understand the many subtleties and complexities in such a philosophy (Armistead, 2010).

Information warfare can be loosely defined as actions that are taken to attack or defend information and related resources and processes; Chapter 2 will provide a more detailed discussion of different definitions. As the term "information warfare" suggests, this was initially a military concept;

however it is also applicable to the corporate, economic, and social spheres (Cronin & Crawford, 1999). The IW constructs by Libicki (1995) and the Indian military (Chatterji, 2008) both list economic information warfare as one of the functional areas; this indicates non-military infrastructures which are critical to national economies may be considered as a legitimate target for IW. Potential aggressors can vary from state actors such as military, intelligence, or other government agencies; and non-state actors, such as rogue groups, terrorists, non-government organisations, and even individuals (Anderson, *et al*., 1999; Arquilla & Ronfeldt, 2001; Molander, Riddile, & Wilson, 1996).

The field of critical infrastructure protection developed due to the growing concerns that these strategic infrastructures were vulnerable to attack; in particular there was increased effort to protect the critical information infrastructures. This led to a research focus on vulnerability and risk assessments of information infrastructures, notable early works include Anderson *et al*. (1999), Cordesman (2000), the Critical Infrastructure Assurance Office (2000), and Ware (1998). One of the earlier vulnerability assessments is the Minimum Essential Information Infrastructure Process proposed by Anderson *et al*. (1999), since then there have been multiple vulnerability and risk assessment frameworks proposed for information systems; these will be covered in more detail in the literature review. Many of these frameworks focus the assessment on assets, and not on an entire infrastructure; there also does not appear to a suitable mix of broad considerations and in-depth technical analysis that is suitable for assessment from the specific IW perspective.

As technology evolves, so does the IW landscape; therefore new threats and vulnerabilities emerge. This modern technology that this thesis is primarily concerned with is the evolved mobile infrastructure and technologies. The introduction of smart mobile devices and their growing prevalence in society is impacting of information security (Fleizach, Liljenstam, Johansson, Voelker, & Mehes, 2007; Roman, 2011). Similarly, Web 2.0 social media also results in many security challenges (Lawton, 2007); these social networking applications are also available on many mobile devices, converging the security concerns that each technology presents. There is a growing prevalence of mobile devices (Global Mobile Suppliers Association, 2011a; 2011b), particularly in Africa where often there is a vastly higher penetration rate of mobiles compared to traditional fixed-line telecommunications (International Telecommunications Union, 2011).

The concerns highlighted by the above researchers are beginning to unfold. Large-scale cyber-attacks were conducted against Estonia and Georgia in 2007 and 2008, respectively (Hart, 2008; Landler & Markoff, 2007). In 2010, the financial impact of cyber-crime in South Africa was

estimated at R10.9 billion; it is estimated that 62% of South Africa adults who are online experienced some form of cyber-crime in the twelve months prior to the survey (Symantec Corporation, 2011b). In 2009 a "world-first" attack on the mobile infrastructure in South Africa allowed cyber-criminals to intercept online banking one-time passwords sent by SMS, providing them with access to individuals' bank accounts (van Rooyen, 2009). Throughout the period that this study was being conducted numerous incidents illustrated the growing prevalence of IW, and the roles modern technologies were playing in these incidents.

Due to these continuing developments, it is necessary to continuously gather data to analyse trends and incidents, and to conduct a vulnerability assessment of the critical infrastructure. The thesis will focus on the mobile infrastructure due to the prevalence of mobile communications in Africa. This infrastructure also appears to be a central point around which various information and communication technologies (ICTs) are converging; social media applications, wireless networking, access to cloud computing resources, and traditional computing functionality are now found in one smart mobile device. From the Banking SMS incident mentioned above, the threats and vulnerabilities associated with these technologies will also be applicable to mobile communications. Therefore by considering the mobile infrastructure, there is the ability to analyse multiple modern ICTs.

1.3 Problem Statement

Many vulnerability and risk assessments are general and high-level in nature; a framework is required which provides for the high-level structure down to the technical implementation and data acquisition methods. The framework should also be dedicated towards the assessment infrastructure (as opposed to individual asset risk assessment). The IW perspective may also require an integration of some broad, non-technical aspects to the technical aspects of assessment; there may also be the case that some considerations become irrelevant, or new considerations are introduced. To conduct a vulnerability assessment of this type, a current holistic view of the information security and IW aspects globally and in the relevant nation is required. This information needs provide an indication of potential threats, vulnerabilities, and potential impacts of incidents.

Much of the research focuses on specific vulnerabilities or threats relating to the mobile infrastructure, and a broader consolidated view is scarce. Due to the prevalence of the mobile infrastructure, it can be considered critical and a vulnerability assessment needs to be conducted in

order to protect this infrastructure as a national asset. The problem statement for this thesis can be formalised as:

- To provide a broad view of incident trends and IW and security aspects globally and how it relates to South Africa, with relevance to modern ICT technology;
- To assess the vulnerability of a modern ICT infrastructure to IW attacks, with focus on the case of a mobile communications infrastructure.

1.4 Objectives and Methodologies

The main aim of the thesis will be to provide a vulnerability assessment of a generic mobile infrastructure in a South African setting. To accomplish this, the thesis has four primary objectives:

- To further develop a framework that may be used in the vulnerability assessment of critical infrastructure from an IW perspective;
- To gather data relating to attacks and other security incidents on infrastructure;
- Establish the criticality of the mobile infrastructure in South Africa; and,
- Apply the proposed framework to the mobile infrastructure to conduct the vulnerability assessment.

Secondary objectives of the thesis are to apply the framework to a second infrastructure, and identify or propose solutions to mitigate the vulnerabilities considered in the study. The methodologies to be employed in this research are as follows:

- Desk-based research (incident and trend analysis through document analysis);
- Interviews;
- A research workshop;
- A survey;
- Computer simulations; and,
- Mathematical simulations.

Sections 1.4.1 to 1.4.5 will discuss the objectives in more detail, and relate them to the relevant research methodologies.

1.4.1 Develop a Vulnerability Assessment Framework

As mentioned in Section 1.3, the existing vulnerability assessment frameworks do not provide a single metric for rating the vulnerability or risk of an entire infrastructure; most also do not consider

the specific case of IW. The objective is to propose a vulnerability assessment framework that is scalable to different infrastructure sizes and types, and is adaptable to allow for different methodologies as required by the infrastructure being assessed. The assessment framework will provide a single metric that can be used to monitor changes in the vulnerability and risk ratings, or compare different aspects of the existing vulnerability environment.

This objective is sub-divided into two sub-objectives:

- The various IW models that will be discussed in Chapter 2 need to be consolidated into one model relating the various aspects of IW; and
- The vulnerability assessment framework needs to be generated from the various existing vulnerability and risk frameworks and methodologies that will be discussed in Chapter 2. This needs to be related to the IW model above.

The model and framework will be generated by deskwork, where the existing models and frameworks will be analysed and discussed; from this common or significant areas will be identified to propose an IW model and vulnerability assessment framework.

1.4.2 Data Gathering on Incidents and Attack Trends

As mentioned earlier, a coherent big picture is required of incidents and trends relating to information warfare and security; there is a particular shortage of information pertaining to South Africa (Scheepers, 2009). The objective is to collate information regarding incidents and trends from various sources to indicate what vulnerabilities and threats are prominent, what attack types have been successful, and what the concerns are regarding threats and vulnerabilities.

The trends and incidents will be analysed for the following categories:

- General trends in conflict and the roles of technology, and the resulting impact on IW;
- General IW and information security trends and incidents globally;
- Trends and incidents related to mobile technology;
- Trends and incidents related to social media;
- Trends and incidents relevant to Africa and South Africa.

These trends and incidents will be drawn from deskwork, where both physical and online documents and secondary data will be referred to for information to illustrate and investigate the trends. The proposed IW model will be used to analyse incidents; common factors amongst the considered incidents will indicate trends. Expert interviews will illustrate concerns and perceptions

related to the general vulnerabilities and threats, and those related to the mobile infrastructure. The respondents will be both South African and international, thus providing both local and international contexts. The research workshop will indicate the trends and incident types that South African information security practitioners and researchers are noticing in the country. Computer simulations and mathematical calculations will be used test the feasibility and potential impacts of proposed attacks on the mobile infrastructure in a South African setting.

1.4.3 Establish the Mobile Infrastructure as Critical

As the primary focus of the vulnerability assessment will be the mobile infrastructure and it is to be treated as part of the critical information infrastructure, the criticality of the mobile infrastructure needs to be determined. The expert interviews will provide insight into their perceptions of the relevance of the mobile infrastructure to the critical information infrastructure. A pilot questionnaire-based survey of informal traders in the eThekwini (Durban) area will provide indications of the reliance of the informal sector on mobile communications. Secondary data and incidents from the trend and incident analysis will also provide insights into the criticality of the mobile infrastructure.

1.4.4 Application of the Framework to the Mobile Infrastructure

This objective employs the framework to organise the information gathered to assess the threats, vulnerabilities, potential impacts of incidents, and associated risks to the mobile infrastructure. This comprises primarily of deskwork and some mathematical calculation as the data from the trend and incident analysis, interviews, workshop, and simulations and calculations are triangulated.

A generic mobile infrastructure will be assessed using open source information only; this is to protect sensitive information relating to the specific mobile networks in the country. The mobile infrastructure was chosen as the infrastructure and devices dependent upon this infrastructure exhibit most, if not all, of the modern information and communication technologies, such as social media, wireless networking, mass storage, messaging, and both voice and data communications. This provides the opportunity to investigate the vulnerabilities and threats related to a wider range of technologies.

1.4.5 Secondary Objectives

There are two secondary objectives in this study: applying the framework to a second infrastructure; and providing solutions to mitigate the identified threats and vulnerabilities. Applying the

framework to a second infrastructure will not do so at the level as described in Section 1.4.4; instead, it will be a smaller case to initially provide some validation of the framework. This is done in Section 4.3.2. Some solutions will arise from the interviews, workshop, and incident or trend analysis; the candidate also proposes some methods of mitigating attacks or vulnerabilities in publications or in this thesis.

1.5 Relevance of the Study

As discussed in Section 1.2, the evolution of ICTs results in a changing landscape for threats, vulnerabilities, and IW. This indicates that previous studies may become rapidly out-dated, and new research is required to keep track of the changing trends. During the study, numerous incidents occurred which are directly relevant to the study, which illustrates the need for such research.

The research conducted in these fields is very often centred on developed nations, and not on the developing countries; the available data on the developed countries is readily available, but is sometimes scarce for the developing nations. As illustrated in Section 1.2, malicious online activity impacts South Africa both economically and socially. As this research considers South Africa and other developing nations throughout the study, it aims at filling this gap in the knowledge. In some areas in this thesis research conducted in the United States is applied to the case of South Africa.

Research regarding the security of mobile devices and infrastructures tends to focus on specific technical aspects; these will be covered in the document analysis in Chapter 5. Vendor reports focus on malware and cyber-crime from a high-level statistical point of view, and mobile or Web 2.0 security concerns only form a portion of these reports. Whilst these reports provide trends, not all facets or incidents are covered. The study aims at providing a holistic view of incidents and trends, from both a high-level context and technical view points; this provides a more coherent bigger picture which provides knowledge about the likelihood and potential for further incidents to occur.

Vulnerability assessment is cited as one of the main aspects of South Africa's defensive IW efforts (Hefer & Theron, 2009). Due to the prevalence of mobile communications in the country, this infrastructure should be considered as critical. Therefore, a holistic vulnerability assessment of the mobile infrastructure can be considered as relevant to South Africa's defensive IW concerns and socio-economic outlook.

1.6 Layout of the Thesis

This section presented the layout of the thesis, and provides a brief overview of each chapter. There are a total of nine chapters in this thesis, including this introduction. Chapter 2 presents literature review, where the theory and models for IW, critical information infrastructure, and vulnerability assessment is introduced and discussed. The vulnerability and risk assessment methodologies discussed in the literature reviews are also the applicable research methodologies used in the thesis. The literature reviews also presents the relevant technical background to the infrastructures and technologies that will be considered in this thesis.

The research methodology is presented in Chapter 3; this provides more detail on the research instruments, the research processes (both administrative and implementation), and relates the methodologies to the research objectives in more detail than was covered in Section 1.4.

Chapter 4 presents the proposed IW model and vulnerability assessment framework. The IW model is applied to a series of incidents to illustrate its validity; this also forms part of the incident analysis and deskwork to acquire data. The vulnerability assessment framework validity is also illustrated by application to a generic cloud computing scenario; this also satisfies the secondary objective of applying the framework to a second infrastructure.

Chapter 5 presents the incident and trend analysis; this constitutes the deskwork, where information regarding incidents and trends are extracted from documents such as news reports, online sources, academic research output, and vendor reports. Secondary data is also presented and analysed here. General trends in IW and information security are presented, and trends in mobile and social network incidents are discussed. Specific trends relating to South Africa are also presented. The trend and incident analysis is related to the objective of gathering data to provide a holistic view of the IW landscape; the information will also be used in the vulnerability assessment, and some information will provide insight into the criticality of the mobile infrastructure.

The primary data and the analysis thereof are presented in Chapter 6; this constitutes the interviews, research workshop, and pilot survey of informal traders. The data gathered from these methods will provide an indication of the perceived criticality of the mobile infrastructure, and threats and vulnerabilities globally and in South Africa. This relates to the objectives of gathering data on trends and establishing the criticality of the mobile infrastructure.

Chapter 7 presents the computer simulations and mathematical calculations; these are used to identify the feasibility and limitations of proposed attacks, the potential impact of such attacks, and identify centralised components or singularities in the mobile infrastructure. This relates to the objectives of gathering data and conducting analysis for the vulnerability assessment.

The vulnerability assessment of the mobile infrastructure is presented in Chapter 8. The framework proposed in Chapter 4 provides the outline for triangulating the information from Chapter 5 to Chapter 7. The criticality of the mobile infrastructure is summarised, the threats, vulnerabilities, impacts, and risks are assessed and evaluated. Some solutions arising from the data gathering phase of the research are presented. This chapter relates to the objective of conducting a vulnerability assessment of the mobile infrastructure.

Chapter 9 concludes the thesis. The conclusion provides the outcomes for the four primary objectives and the secondary objectives. Recommendations and suggestions for future research are provided. Following the conclusion, appendices provide additional information related to the technical content, research instrumentation, and the administrative process of the study.

1.7 Research Output from the Thesis

This section presents the main research output from this thesis. There are other outputs from this thesis such as internal seminar series and presentations, and other outputs that are related to the thesis; a full list is given in Appendix A. The main conference, journal, and book chapter outputs are:

1. van Niekerk, B., and Maharaj, M.S. (2009a) "The Future Roles of EW in IW," *Aardvark Roost Big Crow Conference*, Pretoria, 25-26 August.
2. van Niekerk, B., and Maharaj, M.S. (2009b) "Information Operations Education for South Africa," *3rd Annual Teaching and Learning Conference*, Durban, 21-23 September, pp. 206-224.
3. van Niekerk, B., and Maharaj, M.S. (2009c) "The Future Roles of Electronic Warfare in the Information Warfare Spectrum," *Journal of Information Warfare* 8(3), pp. 1-13.
4. van Niekerk, B., and Maharaj, M.S. (2010a) "Information as a Strategic Asset in an Asymmetric Unconventional Conflict," *International Conference on Information Management and Evaluation*, Cape Town, 25-26 March, pp. 413-421.

5. van Niekerk, B., and Maharaj, M.S. (2010b) "Mobile Security from an Information Warfare Perspective," *9th Information Security South Africa Conference*, Sandton, 2-4 August.
6. van Niekerk, B., and Maharaj, M.S. (2010c) "Weaponisation of the Net," *12th Annual Conference on World Wide Web Applications (ZA-WWW 2010)*, Durban, 21-23 September.
7. Pillay, K., van Niekerk, B., and Maharaj, M.S. (2010) "Web 2.0 and its Implications for the Military," *Workshop on the Uses of ICT in Warfare and the Safeguarding of Peace*, Bela-Bela, 11 October, pp. 50-57.
8. van Niekerk, B., and Maharaj, M.S. (2011a) "Infrastructure Vulnerability Analysis from and Information Warfare Perspective," *South African Computer Lecturer's Association (SACLA 2011) Conference*, Ballito, 6-8 July, pp. 76-85.
9. van Niekerk, B., Ramluckan, T., and Maharaj, M.S. (2011) "Web 2.0 as an Attack Vector Against Strategic Security," *5th Military Information and Communications Symposium of South Africa (MICSSA 2011)*, Pretoria, 18-21 July 2011.
10. van Niekerk, B., Pillay, K., and Maharaj, M.S., (2011) "Analysing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective," *International Journal of Communications*, vol. 5, pp. 1406-1416.
11. van Niekerk, B., and Maharaj, M.S., (2011b) "Mobile Malware Trends," *Business Management Conference*, 28-29 September, Durban.
12. van Niekerk, B., and Maharaj, M.S., (2011c) "Relevance of Information Warfare Models to Critical Infrastructure Protection," *Scientia Militaria* 39(2), pp. 99-122.
13. van Niekerk, B., and Maharaj, M.S., (2011d) "The Information Warfare Life Cycle Model," *South African Journal of Information Management* 13(1), available online at: http://www.sajim.co.za/index.php/SAJIM/article/view/476
14. van Niekerk, B., and Maharaj, M.S., (c. 2012) "A South African Perspective on Information Warfare," book chapter in Ventre, D., in press.

1.8 Writing Conventions

This section provides a summary of the writing conventions in the thesis. Due to the number of acronyms, those that are seldom used will be typed in full the first time they are used in each chapter for the reader's convenience. Due to the number of publications, it will be indicated at the beginning of the section if a previous version of the content was published, and the relevant publication.

1.9 Conclusion

Information warfare methods may be used to attack information infrastructures of organisations and nations. New technologies provide new targets and threats related to IW. As the mobile infrastructure is prominent in modern society, it may be targeted by IW attacks to achieve various objectives. However, there is no consolidated information about IW attacks on the mobile infrastructure, except for isolated reports and research proposing specific attacks. Consolidated information for South Africa is also scarce. A framework to assess the vulnerabilities of information infrastructures from an IW perspective is also needed.

The objectives of the study are therefore to propose the vulnerability assessment framework, and gather information to provide a consolidated view of IW, with a particular focus on South Africa and the mobile infrastructure. The gathered information will be used to provide an indication of the criticality of the mobile infrastructure in South Africa, and be used to apply the proposed framework in assessing the vulnerability a generic mobile infrastructure in South Africa. Multiple research methods will be used: interviews, a workshop, trend and incident analysis through document analysis, a questionnaire-based survey, computer simulations and mathematical calculations, and deskwork.

Chapter 2. Literature Review

2.1 Introduction

This chapter presents the literature review and background for information warfare, critical infrastructure protection, vulnerability and risk management, and the structure of the technologies and infrastructures that will be considered in this dissertation. The focus of the background theory will be the models describing these various concepts as related to the dissertation. In some cases adaptations of models are proposed; these will be employed in Chapter 4 to develop the new IW and vulnerability assessment models.

A funnel approach will be adopted for the literature review; Section 2.2 discusses the relationships between information, data and knowledge. This flows into the information concept, where the models and constructs will be discussed in Section 2.3. More detailed discussions of the IW functional areas most relevant to the dissertation, namely network warfare, electronic warfare, and critical infrastructure protection are provided in Sections 2.4 to 2.6, respectively. Section 2.7 discuses vulnerability and risk management, which is a key component of critical infrastructure protection. After this funnel approach, Section 2.8 provides the background to the relevant technologies and infrastructures that will be discussed in the dissertation. Figure 2.1 illustrates the flow of the literature review and the relationships between the concepts and sections.

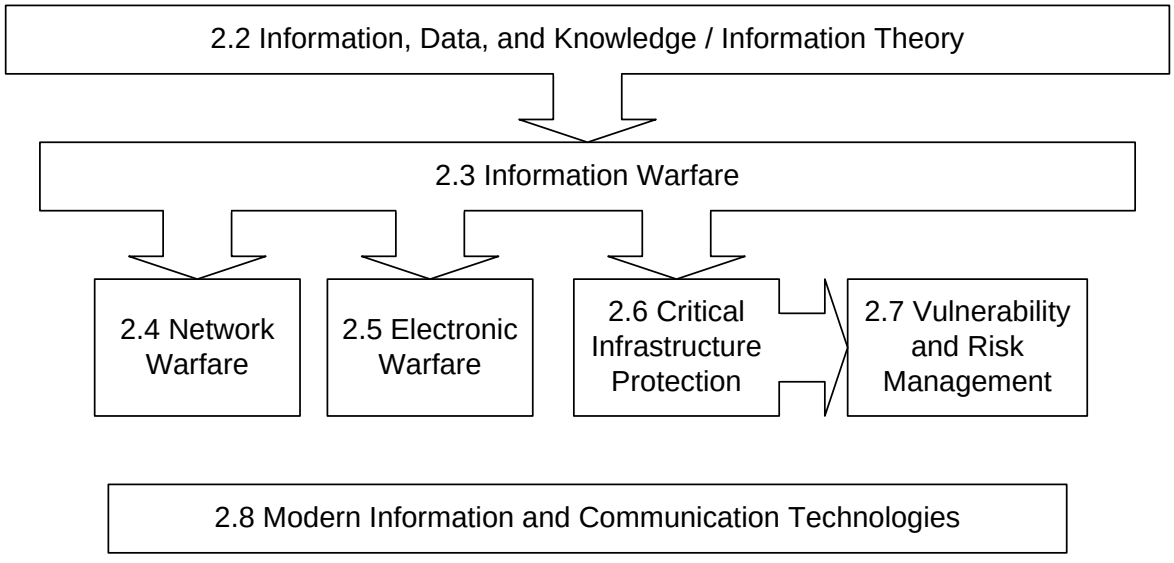


Figure 2.1: The Flow of the Literature Review

Possible sources were identified by searching online for specific key words and phrases; online journals, conferences, and academic databases, book sellers, and general search engines were used to identify books, reports, articles, and specialised subject directories. The search strategy used follows one that is recommended by the University of California Berkeley Library (2009), where distinctive words, synonyms, and equivalent terms were used for searching. For example, the terms information warfare, network warfare, and cyber-warfare are commonly used interchangeably.

The types of sources used include books, major research reports, and journal or conference papers. A core set of books, namely Denning (1999), Hutchinson and Warren (2001), Jones, Kovacich, and Luzwick (2002), and Waltz (1998) are used throughout the literature review, particularly in Sections 2.3 and 2.4, which form the basis of the IW background. Other sources are then used when discussing and providing contrasting view points. Appendix B provides a concept matrix of the major sources used. The literature for specific incidents will be presented in Chapter 5; the sources for these incidents are news articles, vendor reports, and blogs, and will therefore be considered as secondary data. Some incidents will be mentioned in this chapter to illustrated concepts.

2.2 Information, Data, and Knowledge / Information Theory

This section discusses the relationship between information, data and knowledge, and aspects of information theory that are relevant to the dissertation. Various aspects of this section have been published in van Niekerk & Maharaj (2010a).

Hutchinson and Warren (2001) describe the relationships of knowledge, information and data as follows: data is analogous with a thing (such as an event or object) in that it describes the different states of the object or event and consists of the attributes of the object or event. Knowledge is likewise associated with an agent; it is analogous to a set of interacting mind models which influences the interpretation of the data, but can also be influenced by the data, during an event. Knowledge can only be possessed by an intelligent being; usually a human, but could also be possessed by an animal or intelligent machine. Information is the data that has been filtered by the agent through their personal biases formed by experience and perception. Figure 2.2 shows these relationships.

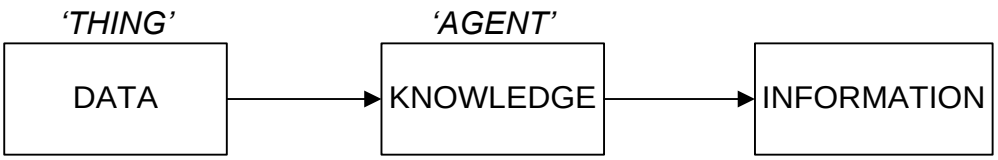


Figure 2.2: The Relationship between Data, Information and Knowledge, adapted from (Hutchinson, 2002)

Waltz (1998) describes the data fusion model, shown in Figure 2.3. Data, in the form of measurements and observations, is processed to create or form information by placing it in context, indexing and organising it. Knowledge is then developed by detecting patterns and relationships amongst the information; this allows the information and data to be understood, explained, and modelled. These models could also possibly be used to predict future behaviour of the entity or process being observed. Wisdom can then be considered as the effective application of knowledge to implement planning and actions to achieve objectives.

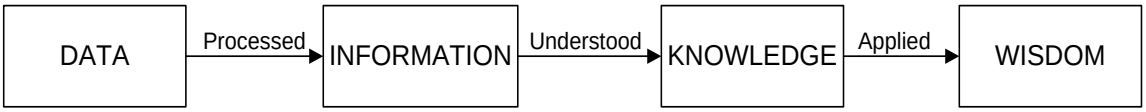


Figure 2.3: Data Fusion Model, adapted from (Waltz, 1998)

An extended model may be derived from the two models discussed above: data is collected and processed; and filtered by *a priori* knowledge (the agent in Figure 2.2) in the form of experience and perception to produce information. The information is analysed and understood to create additional knowledge (*a posteriori* knowledge), which provides wisdom when applied effectively, and can be used as *a priori* knowledge in future analyses. The model also accounts for external influences, such as media and peer opinions that may influence perception and the processing of data and information. These relationships are shown in Figure 2.4.

Another interpretation is that data is comprised of the bits and bytes that form the basis of digital communication systems, whereas information is the data presented in a format understandable to humans, such as image, text or video. Knowledge is then the modelling of information in order to understand trends and possibly predict behaviour of certain systems (Waltz, 1998).

Shannon (1948) developed a mathematical theory of communication; the theorem indicated that the data carrying capacity of a communications channel was limited by the bandwidth of the channel, and the interference, known as noise, that is present on the channel. The following equation was derived to calculate the capacity of a communications channel with noise:

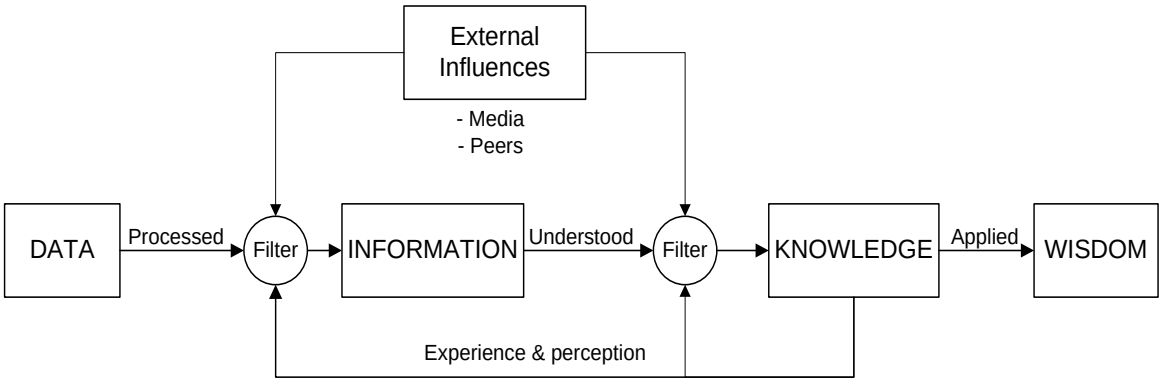


Figure 2.4: The Extended Model for Information Relationships

$$C = W \log_2(SNR) \qquad \textbf{2.1}$$

The capacity, *C*, is measured in bits, *W* is the bandwidth of the communications channel, and *SNR* is the ratio of the signal strength to the noise strength. This mathematical theory goes on to derive the entropy of information; Taub and Schilling (1991) describe the entropy as the average amount of information transmitted over a message interval. The equation for entropy is (Shannon, 1948; Taub & Schilling, 1991):

$$H = \sum_{k=1}^{M} p_k \log_2 \frac{1}{p_k} \qquad \textbf{2.2}$$

The entropy is denoted by *H*, *M* is the total number of possible messages, and p_k is the probability that message m_k is transmitted (Shannon, 1948; Taub & Schilling, 1991). Borden (1999) uses the following conceptual model to illustrate entropy:

Paul Revere considered an attack that came from the sea equally probable as an attack by land; therefore the $p_{land} = p_{sea} = 0.5$. If we calculate the entropy of this using Equation 2.2, we get $H = 1$. Borden equates this to one bit of uncertainty. A lookout was told that if the attack came by sea, he was to show two lanterns or one lantern if the attack was by land. When he showed two lanterns, $p_{sea} = 1$ and $p_{land} = 0$. Again using Equation 2.2, we get $H = 1$; Borden equates this to one bit of information was received. In this case the signal by the lanterns was the data, and the decoding of the data using knowledge resulted in the information that the attack was by sea.

Entropy is related to noise in a communications channel through the concept of mutual information (Waltz, 1998); that the information transmitted is what is received. In digital communications the binary bits or other symbols that are transmitted as electrical signals. The noise interferes with these

signals, which results in some of the bits or symbols being incorrectly interpreted by the receiver; this is equivalent to the wrong message being received compared to what was transmitted. The more bits or symbols received in error, the lower the probability that the transmitted message will be received; this will therefore affect the mutual information. In an IW environment, an attacker may intentionally interfere with the transmitted information, thereby reducing the mutual information, to deny the recipient the information.

As the world has become information-centric, there has been a drive to understand how to determine the value of information, and how to manage information; from this the field of Knowledge Management arose (Prusak, 2001). A method of calculating the value of information based on its capital utility is presented in Waltz (1998):

$$I_v = A_t - A_n - L_t + L_n - \sum_{n=1}^{7} I_n, \qquad \textbf{2.3}$$

where:

- I_v is the information value;
- A_t are the assets derived from the information at the time of arrival;
- A_n are the assets should the information not have arrived;
- L_t are the liabilities derived from the information at the time of arrival;
- L_n are the liabilities should the information not have arrived;
- I_n is the total cost of the information;
- I_1 is the cost for generating information;
- I_2 is the cost to format information;
- I_3 is the cost to reformat information;
- I_4 is the cost for information duplication;
- I_5 is the cost for information dissemination;
- I_6 is the cost for information storage; and,
- I_7 is the cost for information retrieval and usage.

As information assets have value to the owner, competitors will attempt to maximise the value for their own objectives, and possibly minimise the value of the information assets for other actors (Denning, 1999). This competition surrounding information and its use leads to the concept of IW, discussed in Section 2.3. The value of the information may also be used in calculations of risk, which are discussed in Section 2.7.

2.3 Information Warfare

Information Warfare is a relatively new concept, first gaining prominence during the early 1990's (Kopp, 2000), and the first recognised paper considering the topic was published in China in 1985 (Adams, 1998). Whilst most of the methods and tactics encompassed by IW are old, they have been amalgamated under a single concept that is still evolving; consequently there is no standard definition for IW. Two underlying principles that will always hold true regarding IW is that information has value (Denning, 1999) and that the information itself, as well as the systems that transport and store it, are both weapons and targets, (Hutchinson & Warren, 2001). Information warfare as a concept has also undergone a transition to information operations (IO); which encompasses IW and the relevant supporting functions (United States Air Force, 1998).

This section discusses the theories and models of IW, and the constituents that make up the broader concept of IW. The models discussed are relevant to the proposal of the new IW model in Chapter 4. A previous version of this section was initially published in van Niekerk and Maharaj (2011c).

2.3.1 Definitions

As the term suggests, the fundamental component in IW is information; it is both a weapon and a target that needs to be protected, and can be used to gain a strategic or competitive advantage over a competitor or adversary. As the concepts of IW and IO are still evolving, it is difficult to provide precise definitions; those provided by each organisation or nation reflects their specific perspectives. As such, a number of definitions from various sources are presented:

- "Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks," United States Joint Chiefs of Staff (1996a).
- "Actions taken to affect adversary information and information systems while defending one's own information and information systems," Joint Chiefs of Staff (1998, pp. I-1).
- "Information warfare is combat operations in a high-tech battlefield environment in which both sides use information-technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information," Baocun and Fei (1997, p. 328).
- "Offensive and defensive operations against information resources of a "win-lose" nature. It is conducted because information resources have value to people. Offensive operations aim

to increase this value for the offence while decreasing it for the defence. Defensive operations seek to counter potential losses in value," Denning (1999, p. 21)

- "All actions taken to defend the military's information-based processes, information systems and communications networks and to destroy, neutralise or exploit the enemy's similar capabilities within the physical, information and cognitive domains," Brazzoli (2007, p. 219).
- Jones, Kovacich, and Luzwick (2002:24) use the same definition as the Joint Chiefs of Staff (1998, pp. I-1); however, specific definitions for defensive and offensive information warfare are provided: defensive information warfare "is the ability to protect and defend" the information environment while offensive information warfare aims to make an adversary "bend to the will of the attacker".

The fact that IW consists of actions to attack and defend information and related systems and processes are mentioned by the majority of the definitions presented above. Denning (1999), however, specifically mentions the fact that information has value; and Brazzoli (2007), defines three domains in which these actions may be taken: the physical, information and cognitive; the importance of which will be discussed in Section 2.3.3. The definitions by Brazzoli (2007) and Baocun and Fei (1997) restrict IW to the military, however the two definitions by the Joint Chiefs of Staff only refer to an adversary; yet the 1996 definition mentions information superiority, which Hutchinson and Warren (2001) also relate to the corporate sphere; this will be discussed further in Section 2.3.3.

From the definitions presented above, a new definition is proposed, which will be used for the purposes of this dissertation:

Information warfare is actions taken to attack, protect, or exploit information and its supporting systems and processes in the physical, information, and cognitive domains in order to achieve tactical, operational, and/or strategic objectives.

2.3.2 Models

This section discusses various models for IW; these models will be used to develop the new IW framework. Section 2.3.2.1 describes defensive concepts, Section 2.3.2.2 discusses offensive concepts, and Section 2.3.2.3 describes potential target types. Section 2.3.2.4 introduces some mathematical models for completeness.

2.3.2.1 Defensive Models

The "CIA Model" or "CIA Triad" (Denning, 1999; Hutchinson & Warren, 2001) illustrates three aspects of information (and information infrastructure services) that need to be maintained; they are:

- Confidentiality: only those who should have access to sensitive information or knowledge of the functioning, operations or characteristics of infrastructures;
- Integrity: only authorised persons should be able to alter information or systems settings that could affect the infrastructure;
- Availability: the information and its supporting infrastructure should be available when required.

Parker (2002) expands the CIA Triad, proposing three additional attributes: possession or control, authenticity, and utility. Parker states that the loss of possession and/or control of information or the information systems does not necessarily breach confidentiality, unless the information has actually been read. Authenticity is the correct attribution of information to a field in a database or a source, and authenticity is compromised should this be incorrect; an attacker my intentionally subvert authenticity by claiming to be a legitimate user. Utility is the usefulness of the information; it is argued that should a decryption key be lost, all aspects of information are preserved, yet it cannot be used. Wylder (2004) states that there is a consideration that availability should be replaced with authenticity as availability is related to business continuity planning. However, the availability of information can be attacked, as will be discussed in Section 2.3.2.2; therefore it will remain as part of the CIA Triad for the purposes of this dissertation. It can be argued that the extended attributes are subsets of the original CIA Triad; possession and control may be considered as a special case of confidentiality as the information has been accessed in some form, then confidentiality has been breached. The availability may also be breached should the rightful owner also have lost physical control of the information or information systems. Authenticity may be considered as a subset of integrity, as incorrect attribution reduces the quality of the information. It can be argued that should the utility of the information be breached, then so is the availability, as it needs to be available before it can be utilised; utility is a subset of availability.

Other attributes proposed include authentication, non-repudiation (Denning, 1999; Joint Chiefs of Staff, 1998; Waltz, 1998), and restoration (Waltz, 1998). Authentication attempts to ensure that only authorised persons have access to relevant restricted information or infrastructure, or the ability to make alterations to them (Waltz, 1998). Non-repudiation is intended to provide proof of

participation (Joint Chiefs of Staff, 1998); which attempts ensures a false denial may not call integrity into question. Restoration provides the ability for information and infrastructures operations to continue should a disturbance occur (Waltz, 1998). These factors may be considered as controls used to preserve the attributes of the CIA Triad: authentication seeks to maintain confidentiality and integrity, non-repudiation protects integrity, and restoration aims to preserve availability. The CIA Triad and related attributes that are discussed above are the same for both IW and general information security perspectives, and have been described as the industry standard for information security (Whitman & Mattord, 2010).

Poisel (2004) also discusses three attributes: relevancy, accuracy, and timeliness. Wylder (2004) also considers accuracy, which is analogous to integrity in that inaccurate information will have poor integrity. Timeliness is analogous to availability in that a delay in the receipt of the information breaches the availability for a period of time (Defense Science Board, 1996). Relevancy may impact on both integrity and availability in that the requested information is irrelevant and therefore has low integrity, and the required information is unavailable. Should the information be extra and irrelevant, then it has no affect on the integrity or availability.

From the discussions above it can be seen that the CIA Triad constitutes the fundamental attributes of information and infrastructures; the extensions proposed may be considered as subsets of or controls for the three attributes described by the CIA Triad (van Niekerk & Maharaj, 2011c), as shown below:

- Confidentiality
    - Possession
    - Control
- Integrity
    - Authenticity
    - Relevancy
    - Accuracy
    - Non-repudiation
- Availability
    - Timeliness
    - Utility.

2.3.2.2 Offensive Models

Waltz (1998) describes a number of strategies can be used to attack information: disruption of access to the information or information service, corruption of the information, and exploitation of the information. Borden (1999) and Kopp (2000) provide a similar model, however they divide the disruption strategy into two subsets: deny and degrade. Similarly, the United States Air Force (1998) divides disruption into denial/loss and destruction, which also implies the use of the physical domain to conduct IW; this will be discussed in Section 2.3.3. In addition, exploit is termed as compromise, and corrupt as deceive/corrupt, which implies the human vulnerability to deception. Pfleeger and Pfleeger (2003) divide corruption into fabrication and modification, and term disrupt as interrupt, and exploit as intercept.

Hutchinson and Warren (2001) provide a far more intricate model, with six strategies:

- Deny and/or disrupt access to data.
- Destroy data.
- Steal data.
- Manipulate data.
- Alter the context in which the data is viewed.
- Change the perceptions of people towards the data.

This model divides disrupt into disrupt, deny, and destroy; corrupt into manipulate, alter perception, and change context, and exploit is termed steal. This model again implies human vulnerabilities through the tactic of altering the perception of the target. The models discussed above are compared in Table 2.1.

From the comparison, it can be see that Waltz's model describes the 'fundamental' strategies, and the other models provide subsets of these strategies. The strategies described by Waltz also directly oppose or attack the CIA Triad discussed in Section 2.3.2.1; for this reason this will be the primary offensive model adopted for use in the dissertation.

The Defense Science Board (1996) provides a high-level taxonomy for IW which also relates offensive strategies to the CIA Triad, and also considers the time taken to detect the attack; this model is illustrated in Table 2.2, where *t* denotes the unit of time, which can vary from microseconds to years; the criticality of *t* needs to be determined for each case.

Table 2.1: Comparison of Information Warfare Attack Strategies (van Niekerk & Maharaj, 2011c)

Waltz (1998)	Borden (1999) and Kopp (2000)	Hutchinson & Warren (2001)	Pfleeger & Pfleeger (2003)	USAF (1998)
Disrupt	Degrade Deny	Disrupt Deny Destroy	Interrupt	Deny/loss Destroy
Corrupt	Corrupt	Manipulate Alter perception Change context	Modify Fabricate	Deceive/corrupt
Exploit	Exploit	Steal	Intercept	Compromise

Table 2.2: A Top-Level Taxonomy for Information Warfare, adapted from Defense Science Board (1996)

Confidentiality	Compromise of information or information service	Detected on occurrence
		Detected after *t* units of time
		Undetected
Integrity	Unauthorised change in data	Detected on occurrence
		Detected after *t* units of time
		Undetected
	Insertion of false data from a correct source	Detected on occurrence
		Detected after *t* units of time
		Undetected
	Insertion of false data from a incorrect source	Detected on occurrence
		Detected after *t* units of time
		Undetected
Availability	Loss of information or information service	Detected on occurrence
		Detected after *t* units of time
		Undetected
	Delay of an information service or in receipt of information	Detected on occurrence
		Detected after *t* units of time
		Undetected

The United States Air Force (1998) relates the various strategies discussed above to specific threats that may be employed to conduct an attack; this is illustrated in Table 2.3. These threats are still relevant; the candidate added network overload to the denial/loss column, and malware insertion to the destruction column to account for aggressive worms spreading through networks, network denial-of-service attacks, and the Stuxnet malware that can target industrial controllers (Fisher & Roberts, 2011).

Table 2.3: Information Warfare Threats, adapted from the United States Air Force (1998)

Compromise	Deception/ Corruption	Denial/ Loss	Destruction
Malicious code	Malicious code	Malicious code	Malicious code
System intrusion	System intrusion	System intrusion	Bombs
Psychological operations	Military deception	Lasers	Directed energy weapons
Intelligence collection	Spoofing	Physical attack	Lasers
Technology transfer	Imitation	Electro-magnetic pulse	Physical attack
Software bugs		Malware insertion	Electro-magnetic pulse
		System overload	Nuclear, biological & chemical warfare
		Radio frequency jamming	Malware insertion
		Network overload	

2.3.2.3 Targets

Potential targets for exploitation or attack in an information system are described by Denning (1999) and Hutchinson and Warren (2001):

- *Data storage*, such as disk drives and computer or human memories, which can have their contents corrupted or can be physically damaged or destroyed;
- *Transporters*, such as humans and telecommunication systems, may have their performance degraded by a denial of service attack, or may be intercepted to exploit the information;
- *Sensors and Input Devices*, such as cameras and human input devices, which could be destroyed or fed false signals;
- *Recorders, Writers, and Output Devices*, such as printers and disk writers, which can have the output stream of data corrupted;
- *Processors*, such as microprocessors and humans, which also include software, may be corrupted by altering the logic, or be subjected to degradation or destruction.

The Joint Chiefs of Staff (1998) identified the following areas as being vulnerable to attack: information, human factors, links, and nodes. The links and nodes of networks and telecommunications are particularly susceptible to attack, as many are easily identifiable and physically accessible. Human factors may include emotions, which make them susceptible to threats; they are also susceptible to disease and fatigue.

2.3.2.4 Mathematical Models

A model developed independently by Borden (1999) and Kopp (2000), subsequently called the Borden-Kopp Model by Kopp (2000); is the primary model of IW that has a mathematical background. It is based on Shannon's Information Theorem (Shannon, 1948) which is discussed in Section 2.2. The Borden-Kopp model relates Shannon's Theorem to IW through the fact that decisions are made on information (as described in the Paul Revere example in Section 2.2), and IW intends to degrade or protect and improve the efficiency of decision making (Borden, 1999). This relates to the *SNR* term in Equation 2.1, where an attacker may seek to increase the noise (the variable *N*) to degrade efficiency, and the defender will attempt to reduce the noise while improving the message or signal (the variable *S*). To follow on from the Paul Revere example, assume that the attacking English forces used deception and only sent an advance party by sea, whilst the main force would attack by land at a later stage. The lookout would have signalled the attack by sea, however that information is incorrect due to the noise introduced by the attackers. Even if the lookout signalled a land attack at a later stage, two contradictory sets of information would have been transmitted, which degrades the efficiency of the decision making.

2.3.3 Information Warfare Domains, Arenas and Constructs

Information warfare may be conducted in different domains and arenas, and may be constructed differently according to national perspectives. The categorisation of IW discussed in this section will be used to develop the new IW framework. Section 2.3.3.1 discusses the domains of operation, the arenas or spheres are described in Section 2.3.3.2. Section 2.3.3.3 discusses the various IW constructs, and Sections 2.3.3.4 to 2.3.3.9 describe certain components in more detail.

2.3.3.1 Information Warfare Domains

The definition of IW provided by the South African National Defence Force (SANDF) states that IW can be conducted in the "physical, information and cognitive domains" (Brazzoli, 2007); Cronin and Crawford (1999) provide the same categories with different wording. Waltz (1998) extends this model by dividing the cognitive domain into perception and will. Various information systems models also break information systems down into analogous categories: Laudon and Laudon (2004) divide information systems into hardware, software and persware (human assets), Lehman and Quilling (2009) have people, processes, software, data, and hardware as categories, while O'Brien and Marakas (2008) replaces processes with networks. Table 2.4 compares various IW and information systems models. From the comparison, it can be seen that the distinction of physical, information and cognitive domains is the most fundamental model, which will be used throughout

the dissertation. The purpose of these distinctions is to categorise the domains according to broad principles; namely the human thought, intangible information assets, and the tangible hardware assets. These three fundamental domains may then have sub-domains, such as will, perception, data, and software. For the purposes of this dissertation, three main domains (cognitive, information, and physical) will be used, with their relevant sub-domains.

Table 2.4: Comparison of Information Warfare and Information Systems Models, adapted from van Niekerk and Maharaj (2011c)

Brazzoli (2007)	Cronin & Crawford (1999)	Waltz (1998)	Lehmann & Quilling (2009)	O'Brien & Marakas (2008)	Laudon & Laudon (2004)
Cognitive	Psychic	Will / Perception	People	People	Persware
Information	Soft	Information	Processes / Software / Data	Software / Networks / Data Stores	Software
Physical	Physical	Physical	Hardware	Hardware	Hardware

2.3.3.2 Information Warfare Spheres or Arenas

The term information warfare has significant military connotations; its origin was in military thought as can be seen by the definitions presented above. However, it is also applicable to other spheres: this was implied above by terms such as political warfare and economic information warfare. Schwartau (1996) divides IW into personal, corporate and global spheres. Global information warfare may incorporate military IW as well as competition and IW in the international economic and political spheres, and large-scale social information warfare. Waltz (1998) describes IW at national, corporate and personal levels. Cronin and Crawford (1999) discuss it in military, corporate/economic, community/social, and personal spheres. There may be overlaps in many of the terms; aggressive competition amongst multi-national corporations may constitute both global and corporate information warfare. For each of these spheres, IW may still be conducted in the physical, information and cognitive domains, for example physical theft of documents, arson, and theft of laptop computers may be the methods used.

Busuttil and Warren (2002) summarise the differences between military and corporate views of IW: the military has well-defined national boundaries, whereas corporations often operate internationally and may have websites or information assets hosted outside of their physical boundaries, and therefore do not well-defined boundaries for IW. The military may also escalate IW to include physical destruction, whereas corporations will more likely limit themselves to computer-based attacks. The actors for the military viewpoint are listed as well-defined organised groups, and the actors for the corporate perspective are described as not well-defined. However, activity by 'rogue' groups advocating for transparency, such as Wikileaks and the hacker group Anonymous publically releasing military and government information (Bronstein, 2010; Walker, 2010), indicate that potential attackers are not well-defined for government or military perspectives either.

The importance of these spheres is that it illustrates the extension of IW beyond the military sphere; this also implies there may be a blurring in the distinction of military and civilian systems, which will be discussed under the trend analysis in Chapter 5.

2.3.3.3 Information Warfare Constructs

Six functional areas or pillars of IW are identified by Brazzoli (2007) and Théron (2008), which are also shown in Figure 2.5, and discussed further in Sections 2.3.3.4 to 2.3.3.9:

- Command and control warfare (C2W), which protects the ability to effectively command and control (C2) forces whilst attempting to hinder an oppositions' command and control abilities;
- Intelligence-based warfare (IBW), attempts to maximise the intelligence gathering, assessment and dissemination capabilities and degrade those of the opposition;
- Information infrastructure warfare (IIW), where the aim is to protect the information infrastructure whilst attacking or exploiting the opposition's;
- Electronic warfare (EW), prevents the opposition's use of the electromagnetic spectrum, whilst preserving its availability for friendly use;
- Network warfare (NW), protects the information networks and attacks or exploits the oppositions information networks; and
- Psychological operations (PSYOP), which are planned and co-ordinated activities to influence the emotions, reasoning and behaviour of an audience to further the objectives.

These can then be grouped into two domains; the application domain, comprising of command and control warfare, intelligence-based warfare and information infrastructure warfare, and the enabling

domain comprising of electronic warfare, network warfare and PSYOPs (Brazzoli, 2007; Théron, 2008). The pillars in the application domain can be considered to be the targets which are affected; and the enabling domain is where activities are performed to create effects in the application domain, and can be considered to be the weapons which attack or defend the pillars in the application domain, analogous to a sword and shield of old. It should be noted that the definitions given above (and Figure 2.5) are the perspective of the South African National Defence Force.

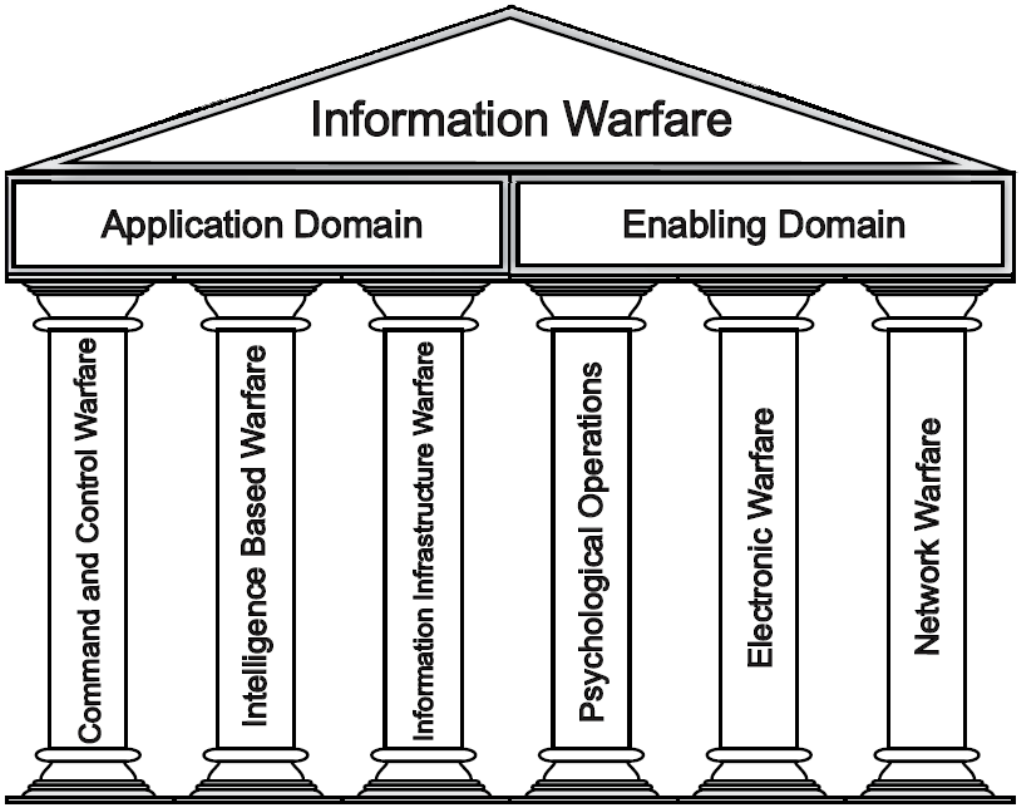


Figure 2.5: The Functional Areas of Information Warfare, adapted from van Niekerk and Maharaj (2009c)

Libicki (1995) proposes seven categories of IW, which are also discussed in Waltz (1998). The definitions of various terms may differ slightly from those above:

- Command and control warfare: attacking and defending command and control capabilities, this relates to the chain of command;
- Intelligence-based warfare: the collection, exploitation, protection, dissemination and analysis of information for use in warfare and competition;
- Electronic warfare: "Communications combat in the realms of the physical transfer of information (radioelectronic) and the abstract formats of information (cryptographic)";

- Psychological operations: actions taken against the human mind;
- Hacker warfare: combat over the global information infrastructure;
- Economic information warfare: the attempts to control economic activity by controlling information and the relevant information systems;
- Cyber-warfare: "Futuristic forms of terrorism, fully simulated combat, and reality control".

The Indian military also defines seven pillars (Chatterji, 2008; Ventre, 2009). Definitions are only provided where there is a difference from the South African description.

- Command and control warfare;
- Intelligence-based warfare;
- Electronic Warfare;
- Psychological warfare: the doctrine specifically mentions that psychological warfare is conducted through the mass media to influence public opinion; the use of information technologies to conduct subtle psychological actions is also mentioned (Ventre, 2009).
- Cyber-warfare: the attacking of computer systems;
- Network centric warfare: the networking of military components. The doctrine clearly distinguishes between network centric warfare and cyber-warfare, whereas other doctrines combine the two.
- Economic information warfare: the use of information as to destabilise a nation's economy. Ventre (2009) notes that this forms part of the military IW doctrine, which implies that operations in the economic sphere may be controlled by the military.

The Chinese publications on IW also mention seven pillars: electronic warfare, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, computer warfare, and command and control warfare (Mulvenon, 1998). These theories also appear to have a greater emphasis on non-technological aspects of IW, particularly social implications or physical means to achieve the same results; this is due to the fact that the perceived enemy is considered to be technologically superior (Mulvenon, 1998; PuFeng, 1997; Rawnsley, 2005). This thinking also appears to view IW as a form of unconventional (or guerilla) warfare rather than a force multiplier (as some Western nations do) (Mulvenon, 1998); and advocates pre-emptive strikes to disrupt logistics and communications via computer warfare (Rawnsley, 2005) or physical means. This view by the Chinese theorists still appears to be valid, and was discussed by Ventre (2009).

Arquilla and Ronfeldt (1997) identify four forms of IW: netwar, political warfare, economic warfare, and cyber-war as a form of command and control warfare. Political warfare is the use of political power, policy and diplomacy to achieve objectives (Waltz, 1998); netwar is the use of networked societies and populations to conduct IW through the media, politics, diplomacy, propaganda and psychological operations, political and cultural subversion, and the promotion of political dissention via computer networks (Waltz, 1998).

The United States Air Force provides an information operations construct, which illustrates the military components of IW as it was viewed in the United States, and the extension of IW to information operations. Figure 2.6 is an adaptation of this construct, which has been extended to the corporate environment where OPSEC denotes operations security and TRANSEC denotes transmissions security. Table 2.5 combines the three pillars of the enabling domain as discussed above with the construct shown in Figure 2.6. Table 2.6 relates the IW functional areas to the various domains.

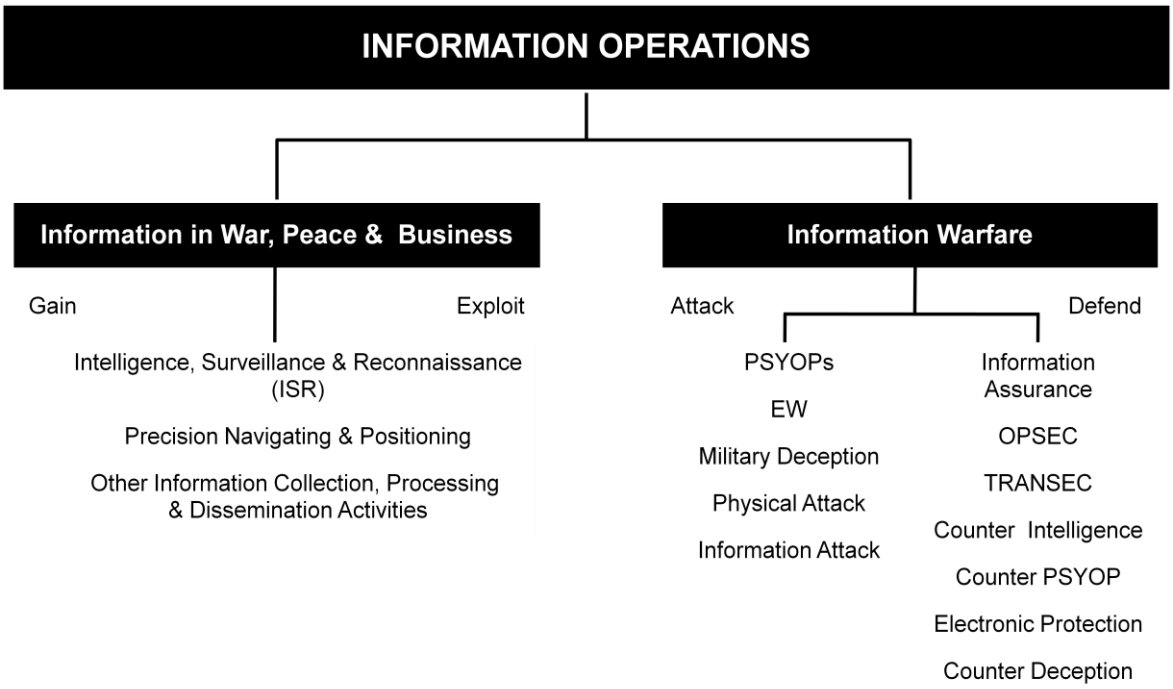


Figure 2.6: The Information Operations Construct, Adapted from (USAF, 1998)

Table 2.5: **Information Warfare Tactics and Tools for the Enabling Domain, adapted from Smith & Knight (2005) and van Niekerk and Maharaj (2009c).**

	EW	NW	PSYOPs
Disrupt / Deny / Destroy	Radio Frequency Jamming Anti-Radiation Missile Low Observability Technology	Denial of Service Attack Physical Destruction Delete Information Firewalls	Disrupt and deny communications and media broadcasts via EW, NW and physical destruction
Exploit	Signals Intelligence Communications Intelligence Electronic Intelligence Identification Friend of Foe	Sniffers Scanners Backdoors Intrusion Detection Systems	Release and distribute condemning information Counter Propaganda Perception Management
Corrupt	Chaff Flares Low Observability Technology	Honey pots Honey nets Root-kits Malware	Provide information out of context Counter Propaganda Propaganda Perception Management

Table 2.6: Domains of IW, adapted from Waltz (1998)

Conflict sphere	Examples
National	Network warfare Economic warfare Political warfare Command and control warfare
Corporate	Network-based espionage, sabotage, and source intelligence Insider espionage or sabotage Precision physical attack on information systems Destruction of media Notebook and computer theft Exploitation and analysis of competitor products and former employees Capture and analysis of competitor trash Arson and other non-precision attacks on information systems
Personal	e-commerce fraud Identity theft, impersonation, spoofing, e-mail harassment, spamming Wiretapping and mobile phone intercepts Bank card impersonation, band and credit card theft, "shoulder surfing" and PIN capture Telephone harassment Theft of personal information from databases and other information stores Computer destruction

From the discussion above, a new model was developed which incorporates the six functional areas of the South African construct as shown in Figure 2.5, and the various domains and spheres described above. The model also illustrates the relationship between the functional areas and domains, and is shown in Figure 2.7.

Figure 2.7: The Relationship between the IW Functional Areas and IW Spheres

The functional areas are important as they distinguish between the ultimate objectives of IW; there may also be subtle differences in how each functional area relates to the different spheres. For the purposes of this dissertation, the six functional areas proposed by the SANDF will be used; economic IW (as proposed by some theorists) will be considered as the application of the various functional areas to the economic sphere. Sections 2.3.3.4 to 2.3.3.9 describe the six pillars of the South African construct in more detail.

2.3.3.4 Command and Control Warfare

The US Department of Defense defines command and control warfare (C2W) as:

"C2W is the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions" (Joint Chiefs of Staff, 1996b, p. V).

Wik (2002) describes command and control warfare as "a subset of information warfare and is an application in military operations that specifically attacks and defends the command and control systems." From the definitions above, the links between command and control warfare and the other functional areas described in Figure 2.5 and Figure 2.6 are apparent. One of the primary ways of affecting command and control, or management in a corporate environment, is to attack the decision cycle, shown in Figure 2.8. This is the standard model for the decision cycle is the observe, orient, decide, and act (OODA) loop (Waltz, 1998); Figure 2.8 also illustrates how the different forms of information, as discussed in Section 2.2, integrate into the decision cycle. In order to gain

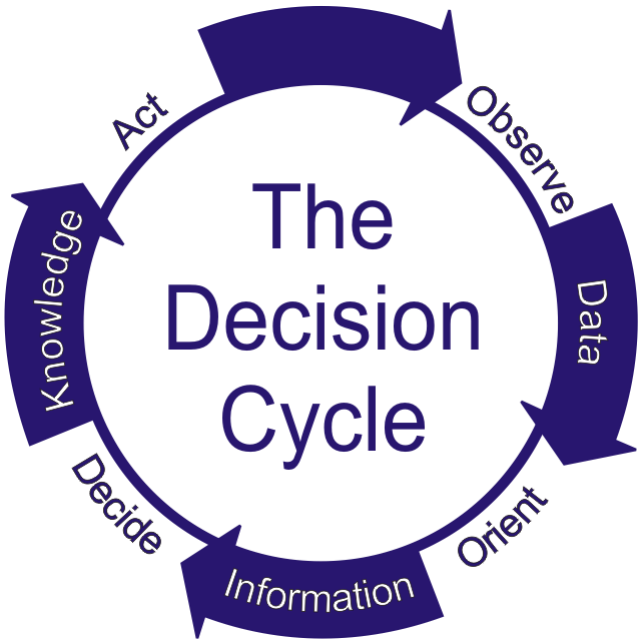


Figure 2.8: The OODA Loop Decision Cycle, adapted from Jones, Kovacich and Luzwick (2002)

information superiority, one needs to have a shorter or more efficient decision cycle than that of any competitors.

2.3.3.5 Intelligence-based Warfare

Intelligence-based warfare encompasses the gathering and dissemination of intelligence, protecting friendly intelligence processes, and disrupting the intelligence processes of an adversary. Intelligence may be collected from various sources:

- Open-sources intelligence – this usually comes from information found in the public sphere, such as from the broadcast and print media, publications, and websites (Denning, 1999; Waltz, 1998);
- Network intelligence (NETINT) – this is the gathering of intelligence from computer networks, and may involve analysis and monitoring of the network and traffic on the network, the interception of messages and system intrusions and exploitation (Waltz, 1998);
- Signals intelligence (SIGINT) – this is the gathering of intelligence from broadcast signals (Denning, 1999; Waltz, 1998), and comprises of:
    - Electronic intelligence (ELINT) – this is intelligence gained from the physical characteristics of signals, or "externals". An order of battle can be generated by analysing the various types of emitted signals (Adamy, 2011; Waltz, 1998); and

    - Communications intelligence (COMINT) – this is the interception of the message, or "internals" that the signal is carrying (Adamy, 2011; Waltz, 1998);
- Human intelligence – this is intelligence from human sources (Denning, 1999; Waltz, 1998);
- Imagery intelligence – this is the intelligence from images, particularly those from satellites and reconnaissance aircraft, and may include either still images or video (Denning, 1999; Waltz, 1998).

Other forms of intelligence are competitive intelligence, which is the legal collection of corporate information, possibly by a competitor for use in strategic planning. A more aggressive version is industrial espionage, which may use covert or illegal methods for acquiring the information. Economic intelligence is the legal gathering of national economic information by other states or organisations; economic espionage is more aggressive and uses covert and possibly illegal methods to gather the intelligence (Denning, 1999).

Waltz (1998) describes the intelligence cycle as consisting of the collection of data from one or more of the sources described above; the data is then distributed for processing, where it is indexed, organised, and translated if required. After processing, the data is analysed, after which an intelligence report can be produced and then disseminated to the required users to act upon.

To protect against an adversary collecting intelligence against an organisation or operations, the signals emissions should be controlled, called emission control (EMCON), and operational security should be employed be reduce the transparency of operations. Transmissions security, primarily encryption, can be employed to maintain the confidentiality of communications. Deception may be employed to actively affect the integrity of the adversary's intelligence collection efforts.

2.3.3.6 Information Infrastructure Warfare

Information infrastructure warfare is the defence of friendly information infrastructure, and the exploitation and attacking of the adversary's information infrastructure; the energy infrastructure, upon which the information infrastructure is dependent to function, is included in this form of IW (Brazzoli, 2007). At a strategic or national level, this is strongly related to strategic information warfare (SIW), see Section 2.3.4, and the defence is related to critical infrastructure protection (CIP), discussed in Section 2.6.

2.3.3.7 Psychological Operations

Psychological operations can be defined as planned operations "designed to convey selected information and indicators to foreign leaders and audiences to influence their emotions, motives, objective reasoning, and ultimately their behaviour to favour friendly objectives" (United States Air Force, 1998).

Psychological operations are closely related to perception management, which also seeks to influence the emotions, reasoning, decisions, and behaviour of the target audience (Denning, 1999). Psychological operations can be seen as using more aggressive tactics, and therefore are offensive, whereas perception management may be more subtle and can be considered defensive (Denning, 1999; Ramluckan & van Niekerk, 2009a). Both PSYOP and perception management are based on the truth, whereas propaganda may involve deception and distortion (Ward, 2003). The message to be conveyed by the PSYOP or perception management needs to be carefully constructed to be culturally correct for the intended target audience, and the media for delivery needs to be chosen to maximise the reception by the target audience (Waltz, 1998). The message may be delivered through actions (*ibid*.) as well as print or broadcast media (Cox, 1997), and also the Internet through web pages (Hutchinson & Warren, 2001).

Figure 2.9 illustrates a message flow process that describes the process used in PSYOPs. The sender of the message will construct the message in such a way that it coerces, deters or provides incentives to the target audience with regards to a specific behaviour or action (Cox, 1997). The message is delivered via the instrument of power (IOP), such as the delivery methods mentioned above, which then create a phenomenon that is observed, interpreted and internalised by the target audience, who would react according to whether they support or oppose the message; the sender can then re-evaluate the message by assessing this reaction (*ibid.*).

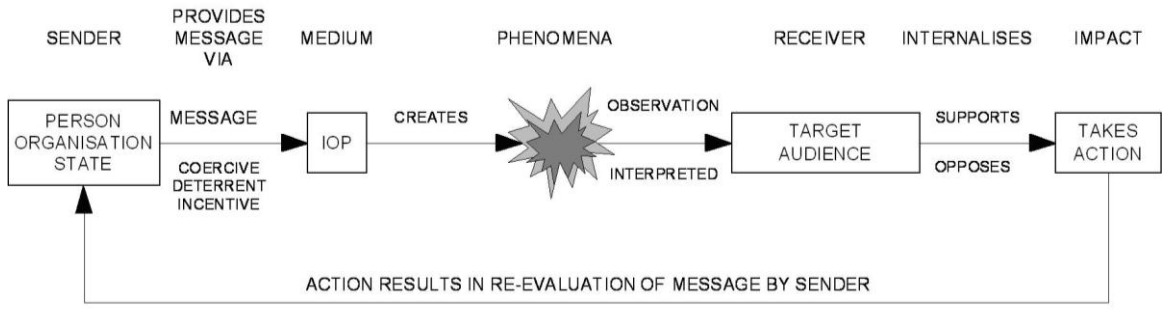


Figure 2.9: Message Flow Diagram, adapted from Cox (1997), Ramluckan and van Niekerk (2009a) (2009b)

The media has traditionally been an effective instrument of power as it shapes public attitudes and can influence operations (Department of the Army, 2001). An example is the US forces withdrawing from Somalia due to public pressure after televised images of the bodies of US servicemen was broadcast; this has subsequently become known as "The CNN Effect" (Taylor, 2002).

2.3.3.8 Network Warfare

Network warfare is the based on the attacking, defending and exploitation of information networks; in particular computer networks. This will be discussed in more detail in Section 2.4.

2.3.3.9 Electronic Warfare

Electronic warfare is the based on denying an adversary the use of the electro-magnetic spectrum, whilst preserving its use for one's own use. This will be discussed in more detail in Section 2.5.

2.3.4 Strategic Information Warfare

Strategic information warfare can be defined as the intersection of strategic warfare and IW (Molander, Riddile, & Wilson, 1996; Molander, Wilson, Mussington, & Mesic, 1998). Command and control warfare is typically tactical battlefield management, and is primarily concerned with the military and physical domains; conventional warfare extends this to the economic, political and possibly the social domains; SIW however, may attack a national homeland without the use of military, political or economic actions (Molander, Riddile, & Wilson, 1996). Libicki (2009) considers IW to be strategic when it is the primary method of warfare or competition; when IW is secondary and supporting other activities it is then considered as operational information warfare.

There are a number of defining features in SIW which add to the complexities when assessing SIW; these are illustrated in Table 2.7. The low entry cost to enter the SIW arena may result in many actors, from nations to organised crime, and possibly even individuals, as all that is needed is a personal computer (Molander, Riddile, & Wilson, 1996). Due to the nature of SIW and network warfare, there is a great deal of uncertainty: lack of strategic intelligence and difficulties in warning and assessments results in difficulties in determining potential threats, infrastructure vulnerabilities and knowing if an attack is occurring, who the perpetrator is and what the current or possible future damage will be (*ibid.*). An added difficulty for the subject of the attack is that the traditional boundaries of the various agencies become blurred, resulting in uncertainties regarding the responsibilities of the various agencies before, during and after an attack (*ibid.*). Some of these

features are relevant to other forms of IW, in particular network warfare which may be used to conduct SIW; network warfare will be discussed in more detail in Section 2.4. The concept of a Minimum Essential Information Infrastructure (MEII) was proposed to mitigate the effects of such an attack (Anderson, *et al*., 1999). This concept is a framework to aid the identification and management of possible vulnerabilities in critical information infrastructures (CII) to ensure a minimum level of functionality to provide continuity of operations (Anderson, *et al*., 1999). This concept will be discussed in more detail in Section 2.7.2.1.

Table 2.7: The SIW Environment, adapted from (Molander, Wilson, Mussington, & Mesic, 1998)

Defining Features	Implications	Dimensions
Low entry cost	Potential for many actors in the SIW environment	Number of offensive SIW actors
No or little strategic intelligence on possible threats	Identity and capabilities of actors and potential adversaries may be unclear	Unknown number of offensive SIW players, including identity
Tactical warning difficult	May not know an attack is occurring	Tactical warning capability
Attack assessment difficult	May not know perpetrator or targets	Attack assessment capability, including perpetrator identity
Damage assessment difficult	May not know the full implications of the attack	Damage assessment capability
Blurring of traditional boundaries	Responsibility allocation before, during or after an attack may be unclear	N/A
Uncertain weapons effects	Both the offensive and defensive actors may be uncertain about the effects of weapons	Uncertainty in weapons effects
Infrastructure vulnerabilities uncertain	National homelands may not be sanctuaries, vulnerable partners may make sustaining coalitions more difficult	Degree of SIW vulnerability

2.3.5 The Application of Information Warfare

Ventre (2009) contends that many confrontations on computer networks stem from tense political situations, and has developed a model to illustrate this shown in Figure 2.10. Whilst it was developed for the case of politically connected cyber-attacks it can be used to describe any situation where an IW attack has occurred. Some contexts results in potential adversaries and motivations, which results in an IW attack. This obviously has ramifications for the target, which reacts in an attempt to recover and gain protection from current and future attacks; which influences the context.

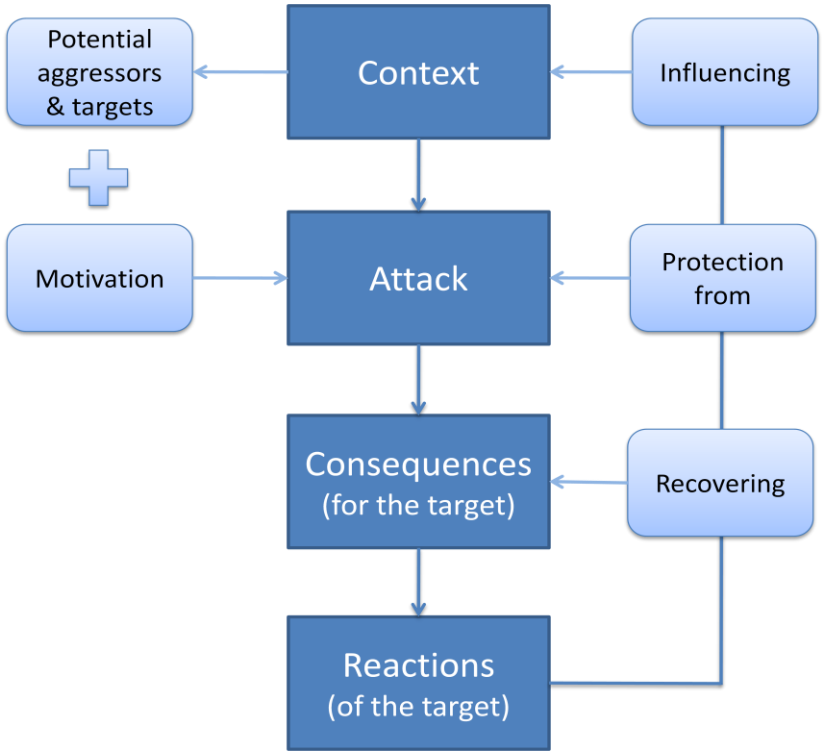


Figure 2.10: Information Warfare Cycle, adapted from Ventre (2009)

Wik (2002) mentions that the disciplines and capabilities that are relevant to command and control warfare may be employed to achieve IW objectives outside of the military command and control target set; and other less traditional methods may also be employed. From this he developed a process for information operations, which is illustrated in Figure 2.11. From the planning of the operations, the available tools are applied to the infrastructure and systems which modern society revolves around, particularly data and communications systems, the mass media, and other infrastructure in society (Wik, 2002). The affects created then impact on the humans themselves, resulting in altered or new thought processes and ultimately actions. This model fits in with the attack to reaction blocks in Figure 2.10.

Examples of IW objectives are: deterring war, supporting peace operations, exposing deception, affecting infrastructure, and the protection and defence of the information infrastructure (Wik, 2002). In terms of this dissertation, the objectives of affecting infrastructure and the protection and defence of the information infrastructure are the most relevant.

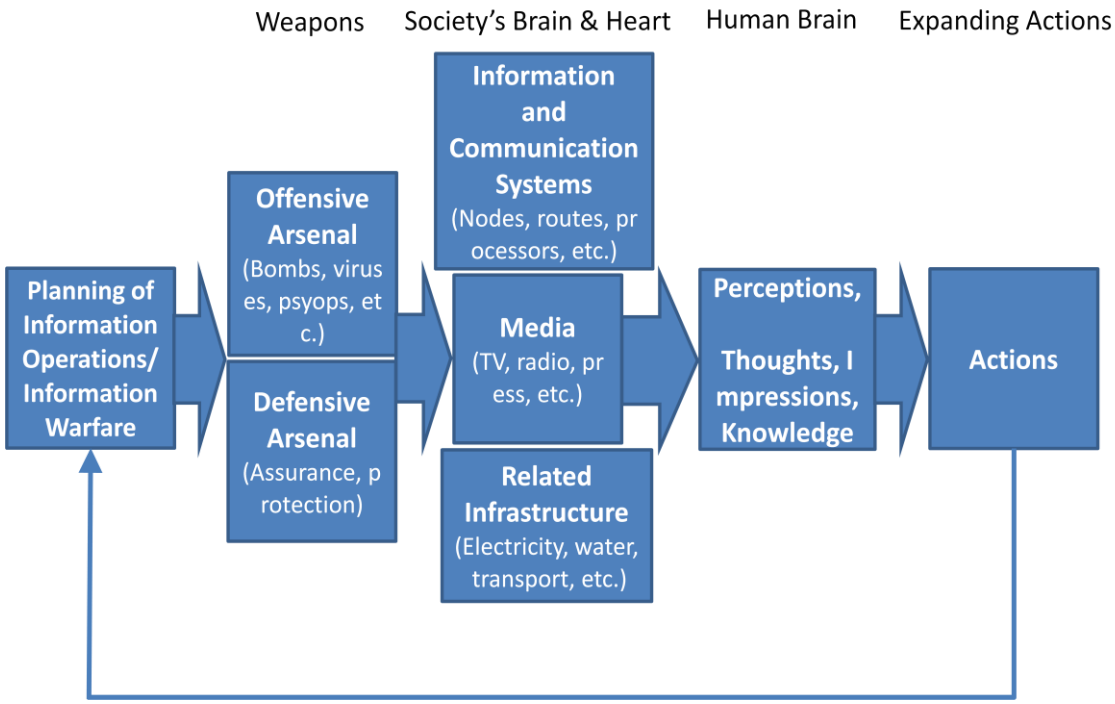


Figure 2.11: The Information Operations Process, adapted from Wik (2002)

Information warfare can be applied in six stages as two or more nations progress from a state of competition to war, and in post-hostility actions (Jones, Kovacich, & Luzwick, 2002), as illustrated in Figure 2.12. Intelligence gathering is ongoing, and probably the most common occurrence of IW; however the focus is shifting from the human spies of old to more technical methods, including surveillance satellites and recently "netspionage" or cyber-espionage (*ibid*.). An example of cyber-espionage is the system penetrations of multiple international organisations (Nakashima, 2011). As the competition becomes more aggressive, diplomatic pressure increases; modern technology provides additional means to project diplomatic pressure, particularly the mass media, and the Internet and social networks, where non-state actors could conceivably become involves through hacking and defacing websites (Hutchinson & Warren, 2001; Jones, Kovacich, & Luzwick, 2002).

The next stage is economic pressure, where traditionally embargoes have been employed; in future IW, it is possible that economic information of adversaries is intentionally targeted and affected. As tensions deepen, military posturing will begin, signifying heightened military alert levels and infrastructure protection, and an increase in propaganda and PSYOPs (Jones, Kovacich, & Luzwick, 2002). The next stage is actual combat, where command and control warfare and tactical IW is apparent on the battlefield in addition to the strategic information

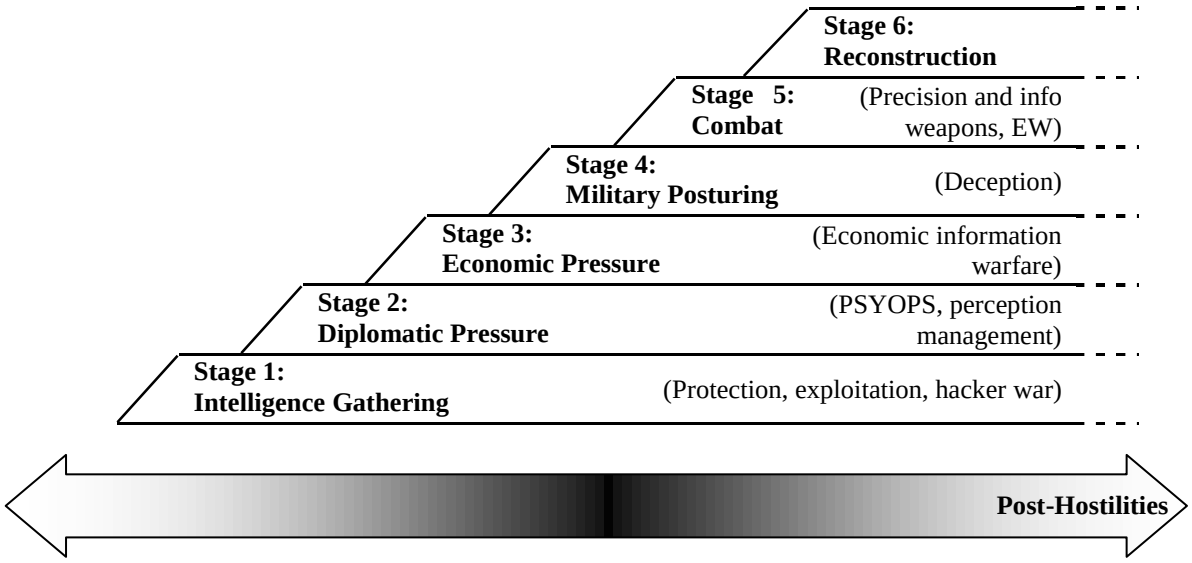


Figure 2.12: The Stages of Information Warfare, adapted from Jones, Kovacich, and Luzwick (2002) and Waltz (1998)

operations. After combat has ended, reconstruction occurs; where IW could be employed to support peace-keeping operations (*ibid*.).

2.4 Network Warfare

Network warfare is the computer-based aspect of IW, and it many go under many names, such as cyber-warfare, computer-based operations and sometimes hacker warfare. The majority of IW texts focus on this aspect of IW (Denning, 1999; Hutchinson & Warren, 2001; Jones, Kovacich, & Luzwick, 2002). Computer network warfare can be divided into three components: computer network attack, computer network defence, and computer network support, as illustrated in Figure 2.13.

Another view breaks computer network operations, as it is termed in the United States, into computer network defence, computer network attack, and computer network exploitation (Hayden, 2010). Computer network exploitation deals with the penetration of information systems in order to steal information (*ibid*.); for the purposes of this dissertation, computer network exploitation will be considered as part of network warfare attack.

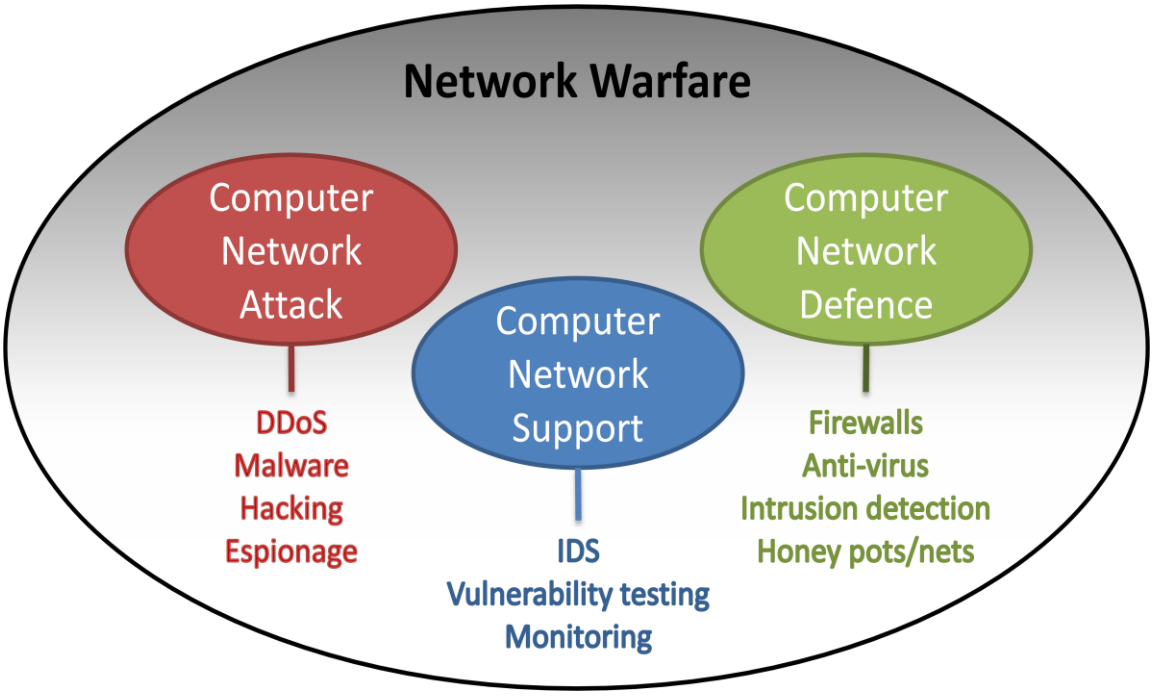


Figure 2.13: Network Warfare Components

2.4.1 Network Warfare Attack

Computer network attack covers those activities which seek to exploit, corrupt, degrade or deny the performance of networks or the various components that constitute the network. This may be accomplished through various tactics, which are either active or passive. Active attacks include: denial-of-service (DoS) attacks; the introduction of malware and backdoors; system penetration; and various other activities. Passive attacks are more difficult to detect, and usually include the monitoring of networks in order to retrieve more information about that network (Thion, 2008). The availability of hacking tools and malicious code on the World Wide Web provides ready-made IW weapons to any nation or group seeking to obtain an IW capability (Jones, Kovacich, & Luzwick, 2002). The following paragraphs discuss types of attacks.

A denial-of service attack is when a target is flooded with false requests, overloading the gateway or network so that legitimate traffic is severely hampered or is prevented altogether (Peltier, Peltier, & Blackley, 2005). When the attack originates from multiple machines it is known as a distributed denial of service (DDoS) attack (*ibid*.).

Viruses are a type of malicious software which requires another program of file to propagate. They may include the following:

- Boot viruses, which infect the boot sector of a disk and executes every time the system is turned on, and may infect any removable disk that is inserted into a drive (Denning, 1999).
- Macro viruses, which are contained in the macros of Microsoft Office documents (Denning, 1999; Hutchinson & Warren, 2001).
- Program viruses are contained in, or infect, executable files, primarily of programs (Denning, 1999).

Worms are self-replicating and actively seek to spread to other systems via the network, the intent being to infect the network (Hutchinson & Warren, 2001; Waltz, 1998). Rabbits are also independent and self-replicating, but do not spread to other systems; it replicates continuously exhausting the resources of the infected system (SpyOps, Technolytics Institute, and Intelomics, c. 2008). Waltz (1998) gives this definition to bacteria, whereas (SpyOps, Technolytics Institute, and Intelomics, c. 2008) differentiate the two; they agree that the bacterium exhausts computer resources, yet mention that it specifically attaches itself to the operating system. A Trojan, or Trojan Horse, appears to perform a legitimate function, however it contains additional hidden malicious functions (Hutchinson & Warren, 2001; Waltz, 1998). Backdoors are inserted code fragments or programs that provide a covert means of accessing the system after the initial penetration or infection (SpyOps, Technolytics Institute, and Intelomics, c. 2008), and may be used in conjunction with Trojans (Waltz, 1998). Logic bombs are pieces of code that are inserted into software to trigger potentially malicious activity when certain conditions are met (*ibid*.).

Two modern versions of malicious code are Rootkits and malware that creates networks of systems controlled by the attacker, called Botnets. Rootkits are a collection of tools that can be used to mask intrusion and gain administrator-level access to computers, networks and related systems (SANS Institute, 2010); they may also mask the running of illegitimate programs or processes, and possibly take control of a system (Poulsen, 2003). In 2005 Sony used a rootkit for to hide software for copyright protection of its CDs. This use was not intended to be malicious; however it was discovered that the rootkit created vulnerabilities that could be exploiting by attackers (BBC, 2005). Botnets are a network of software bots (short for robot), which run autonomously (SpyOps, Technolytics Institute, and Intelomics, c. 2008). Malicious variants may seize control of computers (these are then called zombies), and the network can be used for conducting DDoS attacks or committing other cyber-crimes (Ajoku, 2009), they may also be used for the distribution of spam emails. For the purposes of this thesis, all forms of viruses, worms, and other malicious code or software will be encompassed by the generic term malware.

A man-in-the middle attack is where an eavesdropper manages to intercept communications (particularly those that are encrypted) between two parties; the attacker receives each message sent and then transmits it to the intended recipient, and then receivers and relays the replies. This type of attack is most commonly used against secure websites, particularly e-commerce sites in order to compromise the client's credit card details (Whitman & Mattord, 2010). A modern variation is the man-in-the browser attack, which is facilitated through the use of a Trojan, and is effectively a man-in-the-middle attack between the user and the security mechanisms of the web browser application (Gühring, 2006). These attacks are capable of modifying information on the fly, so no fraudulent activity is readily detectable (*ibid*.). These attacks could also conceivably be used to gain information required to logon to websites or servers that contain other forms of sensitive information. Cross-Site scripting is a popular attack vector against both the average user and organisational networks; this can be used for stealing user sessions, injecting malicious content, and to compromise usernames and passwords (Dhanjani, Rios, & Hardin, 2009). The attacker inserts malicious code into a legitimate dynamic web page; this can be a hyperlink which loads or redirects the user to malicious content (Janczewski & Colarik, 2008; Lawton, 2007). Cross-site request forgery is when an attacker compromises a legitimate user's computer and uses it to send requests to web-sites or organisation intranets for which the user has legitimate authentication (Lawton, 2007). This allows the attacker to pose as the legitimate user and conduct malicious acts once access is gained to the web sites. Cross-site scripting and cross-site request forgeries are particularly relevant to social networks (*ibid*.); cross-site scripting has been used to attack both YouTube (Barnett, 2010) and Twitter (Twitter, 2010).

Phishing attacks utilise spam emails to coerce or trick users to go to fake banking sites and enter their online banking details; a modification on this is the chat-in-the-middle attack, where a fake technical support instant messaging chat window is used to trick the user into providing account information. These attacks primarily target online banking to gain access to the victim's finances (RSA FraudAction Research Labs, 2009).

Coleman (2008a) describes three components of cyber-weapons: there needs to be a delivery vehicle (also called an attack vector), a security breaching mechanism, and the payload. Delivery may be manual (from a hacker), through an email or webpage, or from hardware (such as a universal serial bus (USB) drive). The weapon then needs to exploit vulnerabilities in the system that is to be infected, and then needs to continue to avoid and protection mechanisms, such as anti-

virus software and firewalls that may be in place. Once the system is infected the malicious content, or payload, is activated.

Figure 2.14 shows a network warfare attack process; information is required regarding the interfaces to reach the target network, and information about the target network itself, particularly the vulnerabilities that could potentially be exploited (Jones, Kovacich, & Luzwick, 2002). In this figure GII denotes the global information infrastructure and NII denotes the national information infrastructure. Once the system has been penetrated, the attacker may accomplish the objectives of the attack, and possibly identify additional networks that could be targeted; the attack then proceeds to these new targets. Usually backdoors are left so that the systems and networks may be easily penetrated at a later stage as required (*ibid.*). A distributed denial of service attack may not require the level of planning indicated in this process; all that is required is that the target is flooded with illegitimate data streams to reduce its performance; therefore all that is required is preliminary scanning to determine the IP range of the target.

Due to the prevalence of wireless technologies, there are a number of attacks that arose from weaknesses in the implementation. These include jamming, Wardriving and related attacks for WLAN; and Bluejacking, sniffing, and DoS attacks on Bluetooth networks. These attacks will be described in more detail in Section 2.8.2.

2.4.2 Network Warfare Defence

Computer network defence are those measures taken to mitigate attacks against the computer networks. These usually incorporate conventional information security measures, such as the use of encryption, anti-virus programs, firewalls, and intrusion detection systems (Denning, 1999; Hutchinson & Warren, 2001). Honey pots and honey nets may also be used; these are fake systems or networks that are used to entice an attacker into penetrating them so their attack methods can be monitored and analysed while reducing the risk of any sensitive information being compromised (Jones, Kovacich, & Luzwick, 2002). Other procedural and physical security measures are also incorporated, such as video surveillance, access controls and audits (Denning, 1999; Hutchinson & Warren, 2001; Jones, Kovacich, & Luzwick, 2002). As with network warfare attack, the available hacker tools can be used to conduct penetration testing of networks infrastructures to identify technical vulnerabilities (Jones, Kovacich, & Luzwick, 2002).

Figure 2.14: Network Warfare Attack Process, adapted from (Jones, Kovacich, & Luzwick, 2002)

The various security measures, also called controls or countermeasures, have strengths and limitations. Firewalls act as a gateway between private or trusted and public or untrusted networks by performing packet filtering based on a set of rules; certain protocols can be blocked and only the necessary protocols and their relevant ports are left open (Whitman & Mattord, 2010). The limitation of firewalls is that they do not check what the packets contain; therefore what appear to be legitimate packets to the firewall may still transfer malicious code or sensitive information (Pfleeger & Pfleeger, 2003). Firewalls also do not protect against DoS attacks (Whitman & Mattord, 2010). Sinkholes and Black Hole filtering can be used to defend against DoS attacks.

Sinkholes redirect and trap malicious traffic from a DoS attack to protect the target and allow defenders to monitor and analyse the traffic (Glenn, 2003; Jeong, 2007). Black hole filtering allows traffic to be redirected to a different IP address; this technique is useful when the unavailability of a website is less harmful than traffic hindering the organisational network. It is implemented by reconfiguring the network perimeter routers to redirect the traffic at an organisational or service provider level (Glenn, 2003).

Intrusion detection systems (IDS) monitor the network or system and report on potential malicious activity; a signature-based IDS compares activity against known attack patterns, and a behaviour-based IDS builds a model of acceptable or normal behaviour, and reports on activity that does not correspond to the model (Pfleeger & Pfleeger, 2003). A protocol-anomaly IDS is a type of behaviour-based IDS that tests for anomalies in network or data-transfer protocols (Das, 2002). Host-based IDSs (based on a system) can also check the system log files and file integrity (Gollmann, 2011). An improperly configured IDS may result in a flood of false alarms, or not detect attacks (Whitman & Mattord, 2010); behaviour-based IDSs are particularly susceptible to false alarms. Gollman (2011) also suggests that an attacker may intentionally create alarms on network IDS, resulting in the network administrator's email account being flooded with warnings. Finding the balance of the sensitivity of the IDS may be difficult (Pfleeger & Pfleeger, 2003). An advanced IDS may have built in protection mechanisms that can reconfigure network devices to block the attack, or blocking the network connection; the IDS can therefore provide some protection against a DoS attack (Whitman & Mattord, 2010). A firewall and an IDS can complement each other well; the firewall blocks specified traffic and ports, and the IDS monitors the traffic that is allowed through (Pfleeger & Pfleeger, 2003). Anti-virus software is a form of IDS; the software scans files and processes to check for malicious code, and remove any infection that is discovered (Denning, 1999). Anti-virus software, and signature-based IDSs, may be limited to detecting malicious code and attacks that are encoded into the signature database (*ibid*.); this makes it imperative to ensure that the signature databases are updated regularly. Some sophisticated attacks use multiple methods; therefore multiple signatures will be required to counter these threats (Das, 2002). Rootkits, with their ability to mask intrusions and infections, may also be able to subvert the scans performed by anti-virus tools, however most modern anti-virus tools have some anti-rootkit capability.

Encryption scrambles the original plaintext into unreadable cipher text through the use of a key and algorithms; the aim of encryption is to protect confidentiality (Whitman & Mattord, 2010). Public-

key cryptography and digital signatures provide for a mechanism that provides authenticity, non-repudiation and integrity checks (*ibid*.). However, the integrity checks performed can only indicate that what was sent arrived at the destination without alteration; it cannot determine the accuracy of the information. Encryption schemes also assume that the end-points are secure; if a system or end-user is compromised, the source will be recognised as legitimate, however the communications as a whole is illegitimate. Public-key cryptography is susceptible to man-in-the-middle attacks (*ibid*.), as discussed in Section 2.4.1. It is also possible to use virtual private networks, which are essentially encrypted tunnels between two trusted networks, allowing users to access a trusted private network over a public or untrusted network (Gollmann, 2011; Pfleeger & Pfleeger, 2003). Vulnerabilities in the implementation of devices for virtual private networks may circumvent the secure communication channels they are intended to provide; in one instance general web browser security was undermined (US-CERT, 2009).

A concept that is applicable to both information security and network warfare defence is defence-in-depth; a range of countermeasures are implemented that will provide protection in the physical, information, and cognitive domains (Jones, Kovacich, & Luzwick, 2002). These measures typically attempt to prevent intrusion, detect any intrusion that has occurred, minimise the impact of the intrusion, recover from any damage or loss (Jones, Kovacich, & Luzwick, 2002; Peltier, Peltier, & Blackley, 2005), and possibly respond to the attack (Hutchinson & Warren, 2001; Jones, Kovacich, & Luzwick, 2002). Defence-in-depth usually contains layers of controls such as those discussed above in order to protect various aspects of the networks (Pfleeger & Pfleeger, 2003); for example firewalls provide gateway protection, anti-virus software protects against malicious code, and encryption protects confidentiality. Figure 2.15 illustrates this concept; in the figure ConOps denotes concept of operations, and BDA denotes battle damage assessment.

A defensive concept in the networked world is the air-gap or air wall. This physically and electronically separates critical systems from those that are connected to the Internet (Festa, 1998); with the use of wireless it should also electromagnetically separate the networks using electromagnetic shielding. This is primarily used to separate sensitive networks (such as high-security military networks) and industrial control networks from the normal network that is connected to the Internet (Festa, 1998). The concept behind this is that it will prevent an attacker from gaining electronic access to those critical systems. However, the Stuxnet worm of 2010 managed to circumvent air-gaps (Fisher & Roberts, 2011); which illustrates that this method is not infallible.

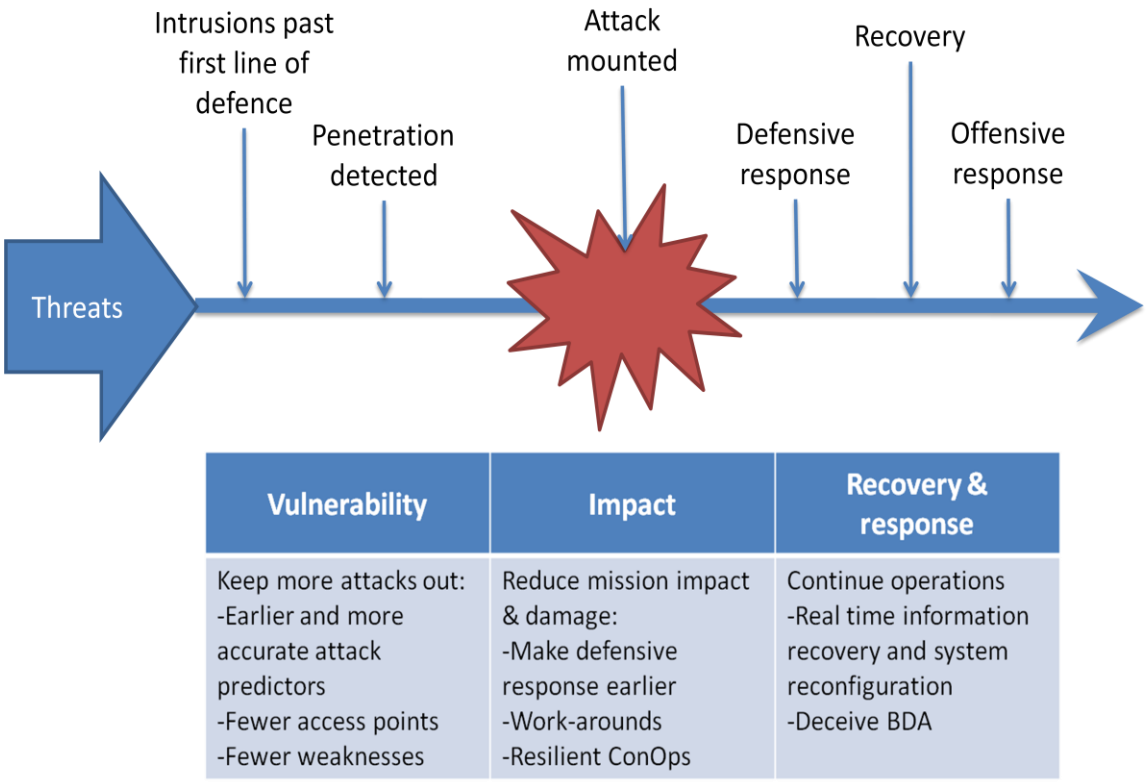


Figure 2.15: Network Warfare Defence, adapted from (Jones, Kovacich, & Luzwick, 2002)

2.4.3 Computer Network Support

Some of the defensive countermeasures taken may also fall under computer network support. This term was used by Smith and Knight (2005), and denotes normal maintenance of network and computer components and applications. Applying security patches and ensuring anti-virus applications are updated, conducting vulnerability and risk assessments, and creating benchmarks for normal network and system performance and behaviour may fall into this category (Smith & Knight, 2005).

2.4.4 Network Warfare Framework

Veerasamy and Eloff (2009) proposed a network warfare framework that incorporates all the concepts discussed in this section; this can be seen in Figure 2.16. In addition, the figure includes factors that may constrain the use of network warfare and the intended target sectors as discussed in Section 2.3.5. The syntactic level denotes the structured organisation of the networks, and the semantic level denotes the meaning of the received data (Veerasamy & Eloff, 2009), and could be

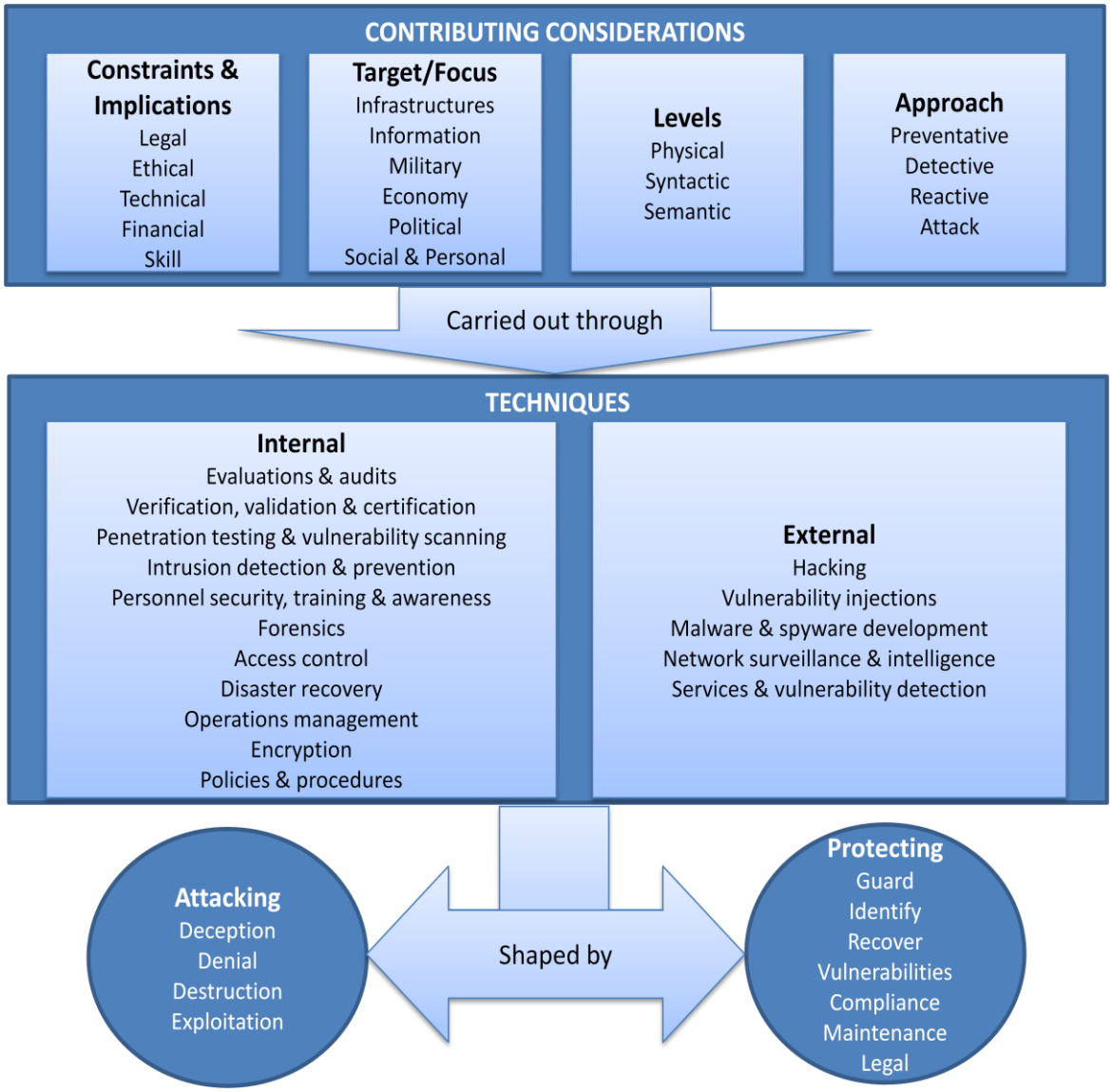


Figure 2.16: Network Warfare Framework, adapted from Veerasamy and Eloff (2009)

partly related to the cognitive domain as it involves trust. Many of the techniques and objectives have been discussed previously.

2.4.5 Cyber-Conflict Spectrum

Adkins (2001) distinguishes the various forms of network warfare in what is called the cyber-conflict spectrum. The various forms are:

- Cyber-crime;
- Hacktivism;

- Cyber-espionage;
- Cyber-terrorism; and
- Cyber-warfare.

Cyber-crime is the illegal accessing of computer systems primarily for personal gain or entertainment, or in an extreme case to affect other persons; hacktivism is the use of network warfare techniques for social disobedience and protest (Adkins, 2001; Arquilla & Ronfeldt, 2001; Jones, Kovacich, & Luzwick, 2002). Cyber-terrorism, however, has the intention of creating fear and possible physical destruction through the network warfare attacks; they may also employ network warfare or cyber-crime to generate funds for terrorist activities (Adkins, 2001; Veerasamy, 2009a). Cyber-espionage was mentioned in Section 2.3.3.5 as network intelligence (NETINT), which attempts to penetrate systems with the primary goal of gathering information (Adkins, 2001); this may take the form of industrial or corporate espionage as well as espionage between nation states (Schwartau, 1996). Cyber-warfare is possibly the most aggressive form of network warfare, where the intent is to drastically affect the opponents' information infrastructure (Adkins, 2001; Arquilla & Ronfeldt, 1997).

2.5 Electronic Warfare

Electronic warfare is the use of electromagnetic (EM) energy to disrupt or deny an adversaries use or the EM spectrum (EMS), and ensure the availability of the EM spectrum for one's own use. Electronic warfare can be subdivided into three components: electronic attack, electronic protection and electronic support (see Figure 2.17). Each of these components may be applied to two areas: radar and communications. For the purposes of this dissertation, the focus will be on communications electronic warfare.

Sections 2.5.1 to 2.5.3 discuss the three components of electronic warfare in more detail. Sections 2.5.4 and 2.5.5 discuss signals interception and jamming in more detail.

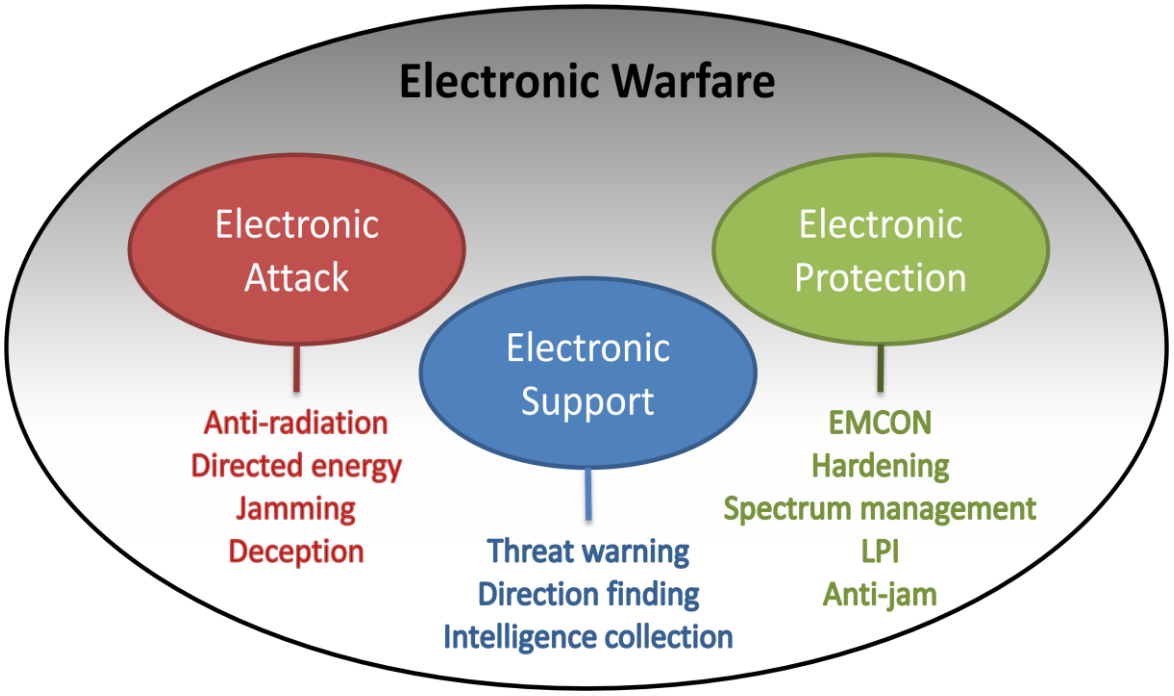


Figure 2.17: Electronic Warfare Components, adapted from (Joint Chiefs of Staff, 2007)

2.5.1 Electronic Attack

This was previously known as electronic countermeasures, and is the "use of EM energy, directed energy or anti-radiation weapons to attack personnel, facilities or equipment with the intent of degrading, neutralising, or destroying enemy combat capability" (Joint Chiefs of Staff, 2007). This constitutes jamming, which affects the timeliness and availability of information; deception, which targets the integrity or accuracy of the information; and directed energy, which is similar to jamming, however it attempts to permanently damage or destroy communications equipment (Poisel, 2004). Anti-radiation missiles and decoys (flares and chaff) also fall into this category (Joint Chiefs of Staff, 2007), in that they seek to deceive and destroy threats; however these are usually employed against radar and optical systems.

2.5.2 Electronic Support

Actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localise sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations (Joint Chiefs of Staff, 2007). This may include threat warning on aircraft, direction finding, SIGINT, ELINT, COMINT and measurement and signature intelligence. Electronic support acts against the

confidentiality of the information, either by attempting to identify the source, or the transmitted information itself. Adamy (2011), however, distinguishes between SIGINT and electronic support in that SIGINT is at a strategic level and focuses purely on intelligence gathering and timeliness is not critical; whereas electronic support is at a tactical level and is used for targeting information, and the timeliness of information is critical.

2.5.3 Electronic Protection

This was formerly known as electronic counter-countermeasures, and is defined as "actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of EMS that degrade, neutralise, or destroy friendly combat capability (Joint Chiefs of Staff, 2007). Examples of electronic protection are screening of communications from detection and jamming, which includes low probability of intercept (LPI) and anti-jam communications, emissions control, and spectrum management (Poisel, 2004). Equipment may also be hardened against directed energy through shielding (Joint Chiefs of Staff, 2007). Other forms of electronic protection are encryption (Poisel, 2004) and low-observability technology (commonly called stealth).

2.5.4 Signal Detection and Interception

In order to exploit a communications signal, its presence first needs to be detected, then the emitter located through direction finding in order to optimise detection, and then it may be possible to demodulate the signal in an attempt to retrieve its contents; this process is shown in Figure 2.18. The process of detecting the presence of signals to provide an image of the electromagnetic environment is SIGINT, and the interception of signals to access the contents is COMINT.

Figure 2.18: Process to Exploit Communications

The probability of intercept is defined as the electronic warfare system will detect the presence, and some parameters, of a particular signal from the time the signal first reaches the electronic warfare systems locations and before it is too late to complete the interception. Spread-spectrum communications are classified as LPI due to the fact that their characteristics make them very difficult to intercept (Adamy, 2009). Frequency hopping signals are only present at a specific frequency for a very short time period before they hop to another frequency; this makes interception

difficult as the electronic warfare system will need to track the hops (Adamy, 2009; Poisel, 2004). Direct-spread communications, such as those found in 3G mobile phone communications, often have the signal energy distributed over such a wide frequency bandwidth that the spread signal strength is below the background noise, making them difficult to detect and intercept (Adamy, 2009; Poisel, 2004). Adamy (2004) and Nicholson (1998) provide in depth discussion on the requirements and probability of detecting various signal types.

There are three basic search strategies when attempting to detect the presence of signals: a general search, where there is no prior knowledge of signal presence, and every possible frequency and direction needs to be considered without any priority. A directed search is possible when some characteristics are known, such as the frequency range, or possible direction from which the signal could be arriving; then any signals that fall within the search criteria are given priority over other signals. A sequentially qualified search measures specific parameters of possible signals in a sequential order; depending on each step the signal may be assigned a priority to determine the amount of effort that will be employed to further analyse the signal (Adamy, 2009).

The location of the emitters can then be located with some precision, depending on the technique used. Multiple direction finding stations could be used to triangulate the emitter location, more stations usually result in a greater degree of accuracy; the mobility of the direction finders and target also affects accuracy. Adamy (2009) provides more detail on location techniques and accuracy.

The interception of the signal attempts to demodulate the signal to access the data contained within; however as the information is usually encrypted, the interception may not be practical unless the encryption can be broken while knowledge of the information carried by the signal is still of some worth to the interceptor (Adamy, 2009). As mentioned above, the characteristics of spread-spectrum communications hinder interception of the information; this depends on the length of the pseudo-random sequence used for the spreading, as longer codes are more secure (*ibid*.). Adamy (2009) discusses this in more detail.

2.5.4.1 Mathematical Calculations for Detection of Radio Communications

This section will describe how to calculate if a signal can be detected for a given sensitivity of an intercepting antenna, and the maximum range at which a transmitted signal can be detected. The equations presented are in a form taken from Adamy (2009); other sources such as Nicholson (1998) and Poisel (2004) provide more in-depth equations that will not be required for this

dissertation. These equations are presented as they will be used in Chapter 7 to determine the maximum range that communications can be intercepted as to determine the effectiveness of an electronic warfare threat.

The first step is to calculate the signal strength at the receiving intercept antenna; the received signal power is related to the power that it was originally transmitted at, the gains of the transmitting and receiving antennas (in the direction of the intercept receiver), and the loss in power that the signal experiences during transmission. This can be calculated by:

$$P_R = P_T + G_T - L + G_R \quad \textbf{2.4}$$

Where P_R is the received signal strength in dBm, P_T is the transmitted power in dBm, G_T is the gain of the transmitting antenna in dB, L is the propagation loss in dB, and G_R is the gain of the receiving antenna in dB.

Two forms of propagation loss (L) will be considered, for line of sight and two-ray propagation. Two-ray propagation occurs when the distance between the transmitting and receiving antennas is such that there are reflections from the ground in addition to the main signal. To determine which form of loss will occur, the Fresnel Zone needs to be calculated; if the distance between the antennas is greater than the Fresnel Zone, then two-ray propagation occurs. The Fresnel Zone is affected by antenna heights and the frequency of the signal. The formula for calculating the Fresnel Zone is:

$$FZ = \frac{f \times h_T \times h_R}{24000} \quad \textbf{2.5}$$

Where FZ is the Fresnel Zone distance in kilometres, f is the transmitted frequency in MHz, h_T is the height of the transmitting antenna in metres, and h_R is the height of the receiving antenna in metres. The constant terms in Equations 2.5 to 2.7 are due to the fact that radio waves propagate spherically, In Equation 2.6 the speed of light (3×10^8 m/s) is also taken into account. The loss from line of sight propagation is a function of the distance between the two antennas and the signal frequency; this is calculated as:

$$L = 32.44 + 20\log_{10} d + 20\log_{10} f \quad \textbf{2.6}$$

where d is the distance between the two antennas in kilometres, and the other variables have been described before. The loss from two-ray propagation is a function of the distance, and the height of the antennas; this is calculated as:

$$L = 120+40\log_{10} d - 20\log_{10} h_T - 20\log_{10} h_R \quad \textbf{2.7}$$

If the received power is greater than the intercepting antenna's sensitivity, S (in dBm), then the signal can be successfully intercepted. Therefore, to calculate the maximum range a signal can be intercepted for a given sensitivity, the received power, P_R, should be replaced by the sensitivity, S, and then solve for the distance, d. The formula to calculate maximum distance at which the signal can be successfully intercepted for line of sight propagation is then:

$$20\log_{10} d = P_T + G_T + G_R - 32.44 - 20\log_{10} f - S \quad \textbf{2.8}$$

The equivalent formula for two-ray propagation becomes:

$$40\log_{10} d = P_T + G_T + G_R - 120 + 20\log_{10} h_T + 20\log_{10} h_R - S \quad \textbf{2.9}$$

2.5.5 Jamming of Radio Communications

As communications plays a vital part on the modern battlefield, the ability to hamper an adversary's communications can decide the outcome of a battle or campaign. From a safety and security perspective, the ability to jam the communications of criminal elements prevents them from sending out a warning about an impending takedown, and could also hamper the ability to employ explosive devices using a RF-controlled detonator. As mentioned earlier, electronic warfare is related to either radar systems or communication systems; the primary difference in relation to jamming is that the transmitter and receiver are co-located, whereas in communications the transmitter and receiver are in different locations (Adamy, 2009).

The primary jamming missions employed by ground forces on the battlefield are planned jamming, where the jamming missions are integrated with fire support missions and friendly communications windows. This includes on-call jamming, where jamming is employed as required, usually against reinforcements. Electronic masking is the use of jamming to hide friendly communications by interfering with potential listening posts that the enemy may have deployed. Standard operating procedures (SOP) jamming is when a target is jammed upon recognition, usually when it is not possible to determine the minimum power required, so maximum power is used (Department of the Army, 1992).

The most common method of analysing the effectiveness of a jammer is the jammer-to-signal ratio (JSR), which is usually expressed in decibels. Jamming is essentially the intentional introduction of noise into a communications channel to result in reception errors. The stronger the jamming in

relation to the communications signal, the more errors and the less likely the receiver will be able to recover the transmitted information. The jamming-to-signal ratio (in decibels) is determined by subtracting the power of the signal at the receiver from the power of the jamming at the receiver. The received powers are calculated from the transmitting power, the loss due to the channel, and the gain of the receiving antenna in the direction of the signal or jamming. A general formula for calculating the JSR is (Adamy, 2009):

$$JSR = ERP_j - ERP_s - L_j + L_s + G_{rj} - G_r \quad \textbf{2.10}$$

Where ERP_j is the effective radiated power of the jammer (in dBm), ERP_s is the effective radiated power of the desired signal transmitter (in dBm), L_j is the propagation loss from the jammer to the receiver (in dB), L_s in the propagation loss of the desired signal (in dB), G_{rj} is the gain of the receiver in the direction of the jammer (in dBi), and G_r is the gain of the receiver in the direction of the desired transmitter (in dBi). The channel loss follows the same rules for line of sight and two-ray propagation as in Section 2.5.4.1.

There is some difference in jamming analogue signals to digital signals. Generally, a high JSR, in the region of 10dB, is required to effectively jam analogue signals, with 100% duty cycle (i.e. continuously jammed). In the case of digital signals, the jammer attacks the digital modulation to make the signal unreadable by the demodulator; here a quantifiable measurement of jammer performance can be used: the bit error rate (BER), also known as the probability of error (P_e). Generally, only 20% to 33% of a digital signal needs to be unreadable for it to be useless, however error correction codes may reduce the jammer performance (Adamy, 2009; Poisel, 2004). It should be noted that a BER of 50% is the worst achievable, as anything lower makes the signal more coherent (Adamy, 2009). This is equivalent to reducing the mutual information by increasing the noise levels (as described in Section 2.2), thereby introducing errors in the digital communications signal.

The probability of bit error for a basic binary phase shift key (BPSK) modulated signal in an additive white Gaussian noise (AWGN) channel is $P_e = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$, where E_b is the bit energy and N_0 is the power spectral density of the Gaussian noise. From this the equation for BER for BPSK under conditions of intentional jamming can be derived (Poisel, 2004):

$$P_e = \mathrm{Q}\left(\sqrt{\frac{2E_b}{N_0 + J_0}}\right) = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{E_b}{N_0 + J_0}}\right) \quad \textbf{2.11}$$

where J_0 is the energy of the jamming signal. In general, J_0 is much larger then N_0, so the equation can be simplified to:

$$P_e \approx \mathrm{Q}\left(\sqrt{\frac{2E_b}{J_0}}\right) = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{E_b}{J_0}}\right) \quad \textbf{2.12}$$

For Equations 2.11 and 2.12, the equality $Q(x) = \frac{1}{2}\mathrm{erfc}\left(\frac{x}{\sqrt{2}}\right)$ (Nicholson, 1998) is used.

If the jammer does not have enough power to jam the entire message, partial-message jamming, also called pulse jamming (Adamy, 2009), can be employed. The concept is that if the power is concentrated on a specific part of a message, that part will be destroyed, and if enough of the message is destroyed, then the message as a whole can be destroyed. A simple tactic for partial message jamming is to transmit band-limited white Gaussian noise with a power spectral density of J_0/ρ for a time period ρ, and to transmit nothing for the remainder of the time. The parameter ρ is known as the duty factor of the jammer. As partial-message jamming creates blocks of errors, and some error correcting codes which can correct blocks of erroneous data, it may not be effective (*ibid.*).

Other jamming strategies include (Poisel, 2004):

- Broadband jamming: where a large frequency spectrum is jammed;
- Partial band jamming: where the jamming energy is focussed on specific channels of the frequency band;
- Narrowband jamming: where the jamming energy is focussed on a small portion of the frequency band;
- Multi-tone jamming: the jamming energy is focussed on certain specific frequencies; and
- Single-tone jamming: the jamming energy is focussed on a single frequency.

These strategies are particularly useful against spread-spectrum communications, which have inherent anti-jamming features; an example of such technology is the CDMA employed in 3G mobile communications, and frequency-hopping radios (Adamy, 2009; Poisel, 2004). The performance of the various types of spread spectrum communications are derived in Adamy (2009) and Poisel (2004) for each of the jamming strategies mentioned above. For the purposes of this

dissertation, a basic description of direct-spread CDMA (DS-CDMA) communications, such as those used in 3G mobile networks will be presented here.

In spread-spectrum communications, the signal is distributed over a wider frequency range, as the name suggests. This is done by the means of a pseudo-random sequence, which spreads the data signal with bit rate R_b to a rate that is equal to the chip rate of the sequence, R_c (Adamy, 2009; Poisel, 2004). When this signal is transmitted, the interference is introduced (as indicated by the dashed line in Figure 2.19); at the receiver, the received signal is de-spread using the same pseudo-random sequence, however as the interference has not been spread, the de-spreading process now does so, thereby reducing the spectral density of the interference (Adamy, 2009; Poisel, 2004).

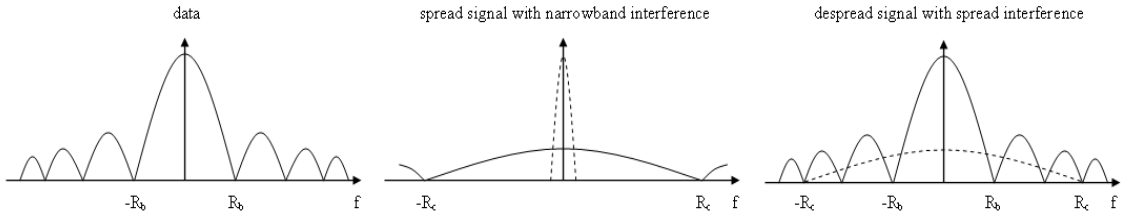


Figure 2.19: The Effects of Spreading on Interference, adapted from (Nicholson, 1998)

This advantage over interference is known as the processing gain, G_p, and is a function of the rate of the pseudo-noise sequence divided by the original data rate, which is equivalent to the bandwidth of the spread signal divided by the bandwidth of the original signal; this can be calculated as, (Poisel, 2004):

$$\mathrm{G_p} = \frac{\mathrm{R_c}}{\mathrm{R_b}} = \frac{\mathrm{W_{ss}}}{\mathrm{W}} \qquad \textbf{2.13}$$

where W is the original (non-spread) bandwidth and W_{ss} is the spread bandwidth. Due to the spreading of the interference, in this case the jamming signal, it first needs to overcome the jamming margin, which is calculated as (Blahut, 1990):

$$jamming\ margin = \left(G_p\right)_{dB} - \left(SNR_{req}\right)_{dB} \qquad \textbf{2.14}$$

which is the difference of the processing gain (in dB) and the minimum required SNR (in dB) for the receiver to detect the desired signal. This results in a probability of bit error of (Blahut, 1990):

$$P_e \approx \mathrm{Q}\left(\sqrt{\frac{2G_p}{JSR}}\right) = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{G_p}{JSR}}\right) \qquad \textbf{2.15}$$

Figure 2.20 compares the theoretical performance of spread-spectrum communications signals against those of a common binary phase shift key (BPSK) communication system; the spread spectrum signal is not as badly affected by the jamming.

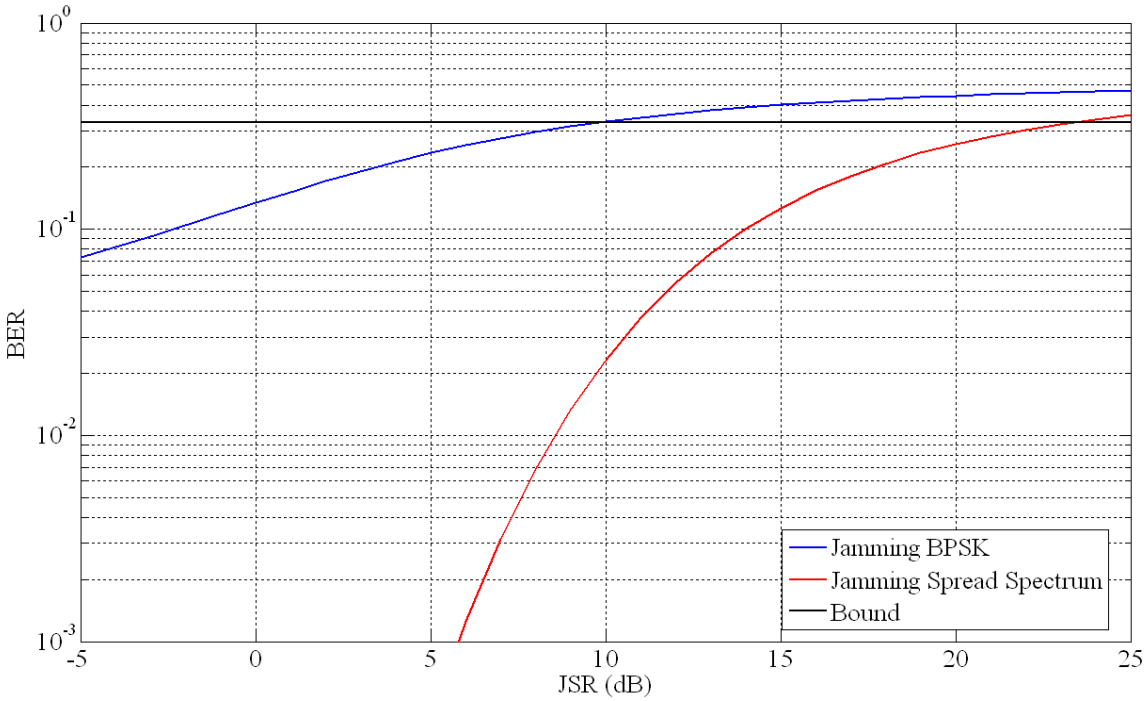


Figure 2.20: Comparing Theoretical Jammer Performance against Spread-Spectrum and Conventional Communications Signals

For the case where multiple users are present on a channel, such as for mobile communications, correlated jamming may be used to improve the performance of the jammer. Correlated jamming results when the jammer has some knowledge of the target signals, and can adjust the ERP of the jamming accordingly (Shafiee & Ulukus, 2009). This information about the target signal may be gained from SIGINT, as discussed in Section 2.5.4. Such a method of gaining information is proposed by Yao and Poor (2001), where an expectation-maximisation algorithm is used to estimate the spreading sequence of mobile CDMA systems in order to eavesdrop of the signals. Simulations in Chapter 7 will be done to illustrate potential limitations of this concept.

The BER equations (Equations 2.11 to 2.15) may be used to describe the theoretical performance of communication systems under jamming; these equations were used in the simulation presented in

Section 7.6 and generate Figure 2.20. For the purposes of the dissertation, the dB equations (Equations 2.5 to 2.10) will be used to estimate the maximum distance for which jamming and signal interception is effective; this will be presented in Section 7.5.

2.6 Critical Infrastructure Protection

This section will discuss critical infrastructures and the need for their protection. Section 2.6.1 defines critical infrastructure, and Section 2.6.2 discusses their inter-dependencies. As this dissertation focuses on information infrastructure, Section 2.6.3 will discuss critical information infrastructures in more detail. Section 2.6.4 will explicitly relate critical infrastructure protection and IW.

2.6.1 Defining Critical Infrastructures

A critical infrastructure is one that is vital to the well-being and functioning of a nation, society, or an organisation. A disturbance of such an infrastructure may result in severe degradation or cessation of operational capabilities or service delivery (Department of Homeland Security, 2009; Macaulay, 2008). The US Presidential Directive 63 of 1998 defines critical infrastructure as "those physical and cyber-based systems essential to the minimum operation of the economy and government" (Moteff & Parfomack, 2004). The Department of Homeland Security in the United States considers critical infrastructures as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof" (Department of Homeland Security, 2010).

As can be seen, the definition of critical infrastructure may have subtle differences according to organisational or national perspectives, similar to the variations in the definitions of IW.

The Presidents Commission for Critical Infrastructure Protection in the United States identified five main critical infrastructure sectors, namely (Ware, 1998):

- Information and communications,
- Banking and finance,
- Energy (electrical power, oil and gas),
- Physical distribution, and
- Vital human services.

The Department of Homeland Security expands the concept of critical infrastructures to critical infrastructures and key resources (CIKR), where the key resources may be defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government" (Department of Homeland Security, 2010). This has also resulted in a re-organisation of the main sectors (Department of Homeland Security, 2010). Table 2.8 compares the critical infrastructure sector groupings described above with those of Nickolov (2005) and Macaulay (2008).

Table 2.8: Comparison of Critical Infrastructure Sectors

Ware (1998)	Department of Homeland Security (2010)	Nickolov (2005)	Macaulay (2008)
Information and communications	Agriculture and food	Electricity, fuel and water supply	Banking and finance
Banking and finance	Banking and finance	Transportation and communication systems	Energy
Energy (electrical power, oil and gas)	Chemical	Food supply and waste management	Information and communications
Physical distribution	Commercial facilities	Finance and insurance	Health care
Vital human services	Communications	Information and telecommunications networks	Food supply
	Critical manufacturing	Military and defence systems and civil protection	Water supply
	Dams	Emergency, health and rescue services	Transportation
	Defence industrial base	Public agencies, administration and legal systems	Safety and Security
	Emergency services	Media, major research establishments, etc	Government
	Energy		Manufacturing
	Government		
	Healthcare and public health		
	Information technology		
	National monuments and icons		
	Nuclear reactors, materials and waste		
	Postal and shipping		
	Transportation systems		
	Water		

As can be seen, the five sectors described by Ware (1998) have been divided into their components by the Department of Homeland Security. An interesting addition is the classification of national monuments and icons as a critical infrastructure or key resource. This is related to the will component of IW as discussed in Section 2.3.3; the destruction or damaging of these monuments may affect the morale and will of the public. The Department of Homeland Security specifically mentions the psychological consequences of an attack on, or using, the CIKR (Department of Homeland Security, 2010). Grobler, Jansen van Vuuren, and Zaaiman (2011) also recognise the psychological relevance in the South African situation. This potential psychological impact is also evident from user frustration due to non-attack related service outages. Both Nickolov (2005) and Macaulay (2008) provide extended versions of the five sectors; as occurred with South Africa's mobile networks (Mtshali, 2011) and wide-spread BlackBerry services (Press Association, 2011) in 2011. Macauly compares the sectors and subsectors of the United States, Canada and the European Union to arrive at the "harmonised CI sectors" presented in Table 2.8. Table 2.9 provides a re-working of the models to include six sectors and their components or key resources. The original five sectors described by Ware (1998) were kept with their components as indicated in the other three models. The military and defence was added as a sixth sector as their infrastructure is generally separate from the others.

Table 2.9: Critical Infrastructure Sectors and Their Components

Energy	Information & communications	Physical distribution	Financial & economic systems	Essential services	Military and defence
Power stations Electric distribution Fuel distribution Water (for cooling and hydro-electric schemes)	Telecommuni-cations Information technologies Satellite Service providers Media and broadcast Military communications	Roads Railways Airports Harbours Postal services Related services Mass transportation	Industry Manufacturing Mining Commerce Banking Defence industrial base	Government Legal Healthcare Emergency and rescue services Law enforcement Waste management Water supply Food supply and agriculture National monuments	Armouries Barracks Air bases Naval bases Military communications Defence industrial base

As these infrastructures are critical to the well-being of a nation, they need to be protected from intentional attacks which could potentially damage the social well-being and economic stability of a nation.

2.6.2 Critical Infrastructure Interdependencies

There are interdependencies amongst the various infrastructure sectors; this is important when considering their protection as the dependencies and interdependencies of critical infrastructure sectors on each other may produce cascading effects that are far beyond the physical location of the incident, or the original sector that was disrupted (Department of Homeland Security, 2010).

Figure 2.21 and Table 2.10 illustrate the inter-dependencies of the sectors. As can be seen there is a very high reliance on the energy and information sectors, which is echoed by Ware (1998) and Nickolov (2005); large disturbances of these sectors will result in severe disruptions in the financial sector and some vital services, and to a lesser degree the physical distribution sector. Banking and finance can be considered to be indirectly depended upon by the other sectors, as a disruption will not immediately result in noticeable affects in the information, energy or physical distribution sectors.

The energy sector requires some degree of communications infrastructure for its control systems, and physical distribution for the delivery of fuel for the power stations; the finance and economy may also affect the supply of fuel due to mining industry or imports being affected. The information and communications requires energy to operate, physical distribution to facilitate maintenance and repairs, and the finances to fund the functioning and maintenance of the systems. The physical distribution sector requires energy and communications to operate airports and sea-ports and rail systems, and to a certain degree the traffic lights on the roads. The financial and economic sector is heavily reliant on the energy to run its systems, and the communications to exchange information; it does have some dependency on the physical distribution system to transport goods and raw materials. Essential services are dependent on all sectors except the military. The military is reliant on the physical distribution systems for deployments, it generally has its own communications systems, and has some capability for its own power generation, however fuel is still required; it has some reliance on industry for equipment supply, and on essential services for food, water and governance.

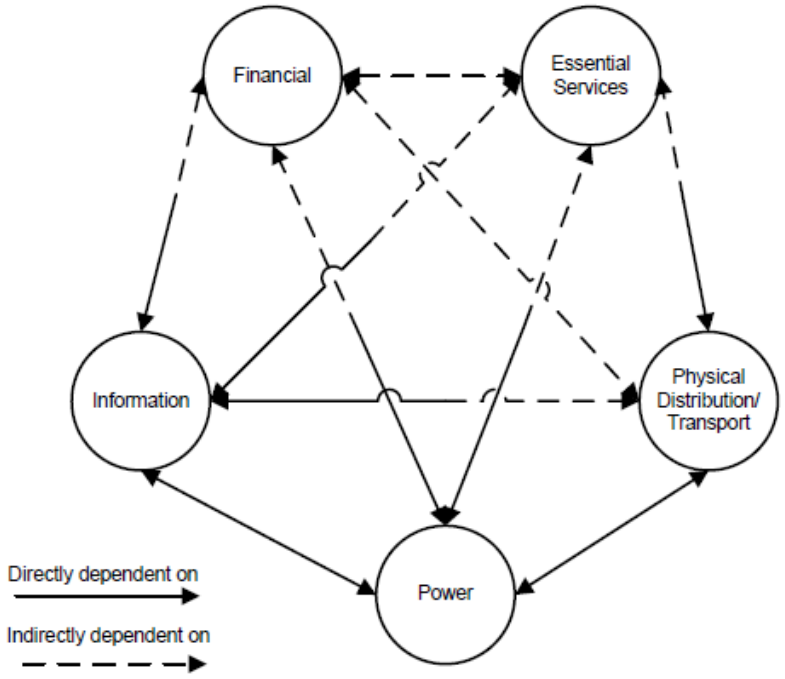


Figure 2.21: Infrastructure Interdependencies, (van Niekerk & Maharaj, 2011c)

Table 2.10: Interdependencies of Critical Infrastructure Sectors

Sector: \ Dependent on:	Energy	Information & communications	Physical distribution	Financial & economic	Essential Services	Military & defence
Energy		Medium	Medium	Medium	Low	Low
Information & communications	High		Medium	Medium	Low	Low
Physical distribution	High	Medium		High	Low	Low
Financial & economic	High	High	Medium		Low	Low
Essential Services	High	High	High	High		Low
Military & defence	Medium	Low	High	Medium	Medium	

2.6.3 Critical Information Infrastructure Protection

There are three concepts of interconnected and inter-dependent information infrastructures, as described below (Dudgeon, 2008; Jones, Kovacich, & Luzwick, 2002):

- Global information infrastructure (GII): this is the global connections and links between the information infrastructures of nations. It comprises of the interconnections of all telecommunications systems, networks and related devices. Examples of these may include undersea fibre-optic cables.
- National information infrastructure (NII): this is the information infrastructure contained within a nation. It comprises of the telecommunications, networks and related devices within a nation. Most of the infrastructure may be in private hands; especially as most of the mobile phone and Internet service providers are private corporations.
- Defence information infrastructure (DII): this is the information and communications infrastructure used for military and defence purposes. Whilst it forms part of the national information infrastructure, much of it is separate from the public and private infrastructure. It incorporates the command and control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) systems that the military and defence department uses.

Busutill and Warren (2002) also suggest two additional infrastructure levels: the organisational information infrastructure (OII) and the personal information infrastructure. Critical information infrastructure (CII) can be described as including "telecommunications, computers/ software, Internet, satellites, fibre optics, etc. The term is also used for the totality of interconnected computers and their critical information flows" (Wenger, Metzger, & Dunn, 2002). Combining this definition with the definitions of critical infrastructure in Section 2.6.1, the CII can therefore be seen as the information systems within the NII, DII, or OII which is essential to its operations.

2.6.4 Critical Infrastructure Protection and Information Warfare

On a day-to-day basis, infrastructures generally experience disturbances that may degrade performance or results in interruptions or outages of services; examples of this may include road accidents, daily criminal activity, or transients and component failures on a power or communications grid (Ware, 1998). This has been termed "infrastructure noise", after the concept of engineering noise, which interferes with audio and electronic signals (*ibid*.). Such disturbances can be expected in the everyday operation of infrastructures, and measures are put in place to mitigate

and respond to such incidents (*ibid*.). These disturbances effectively form the noise floor; this concept is relevant to CIP and IW in that a deliberate attack needs to be distinguished from the everyday noise floor in order to respond effectively (*ibid*.).

The network warfare attack process, shown in Figure 2.14, is also applicable to information infrastructure warfare; the process can be followed to gain access and plant malicious code and backdoors. Rather than steal information, infrastructure control processes could be modified in order to create disturbances such as altering the output of a generator. An example of this is the Stuxnet worm, which altered the code for industrial controllers; this is reported to have caused physical damage to an Iranian nuclear processing facility (Fisher & Roberts, 2011).

When considering IW threats to the CII at a national level, there are characteristics that separate these threats from the more common nuisance hacker attacks (Anderson, *et al*., 1999). The IW attacks are more likely to form part of a larger operation to achieve an objective, which may include conventional economic, political and military actions (*ibid*.). The ability to predict the impact of an IW attack is important for the attacker; if the impact is less than expected the entire operation may fail, or if the impact is far worse, the retaliation by the target may be extreme (*ibid*.). In relation to IW, the nuisance attacks may form part of the infrastructure noise; however it is possible that these attacks are part of a larger, co-ordinated effort. The main example that has been used to illustrate an attack on a critical infrastructure occurred in 2000 in Australia when a disgruntled former employee wirelessly accessed the control systems of the sewerage system and release sewerage into the public waterways (Abrams & Weiss, 2008). This example illustrates the concept of nuisance attacks, where the perpetrator was only doing enough, hoping to be rehired. The Stuxnet worm is a possible example of an attack by a nation, as it is rumoured that it was developed specifically to damage the Iranian nuclear facility in order to hinder its completion (Fisher & Roberts, 2011).

From the interdependencies discussed in Section 2.6.2 and the concept of infrastructure noise, it is possible to model a number of critical infrastructures as an information or communications network. Electrical power is distributed via an electrical waveform with a voltage and current; it is susceptible to disturbances which create spikes or dips in the voltage. This is equivalent to the noise that a communications signal experiences. The electrical power signals are converted to the voltages that are supplied to the end-users; this is analogous to the antenna processing in a wireless communications system. The physical distribution infrastructure may similarly be modelled on a digital communications system; the vehicles can be seen as bits or packets, bridges are gateways, and intersections can be seen as routers or switches. Humans with their capacity to store, process,

and gather information through the use of their memory, mind, and senses, primarily use the physical distribution infrastructure to travel; therefore it can be seen as a system for transporting information (van Niekerk & Maharaj, 2011c).

Physical attacks on these infrastructures can be modelled as IW attacks; destroying or severely damaging a bridge will deny its availability. This will have implications for the entire infrastructure as traffic increases over other bridges in the area, degrading their performance. Intentionally introducing high voltage spikes into the power grid may damage infrastructure components, denying their availability and impacting on the integrity of the infrastructure; end-user equipment may also be damaged or destroyed (van Niekerk & Maharaj, 2011c). As mentioned above, an Iranian nuclear facility was reported to have sustained damage due to an infection by the Stuxnet worm (Fisher & Roberts, 2011).

2.7 Risk and Vulnerability Management

In order to defend against IW attacks, one needs to know where potential vulnerabilities are in order to better protect them (Hefer & Theron, 2009). The vulnerabilities are identified and documented through a process known as a vulnerability assessment (Whitman & Mattord, 2010). Whilst the dissertation is to focus on the vulnerability of infrastructures, risk and threats also need to be taken into account, as they are all related, as shown in Figure 2.22. The figure illustrates the "Information Security Lifecycle," which illustrates that other analyses need to be conducted to determine risk, threats and possible impacts.

Vulnerabilities can be defined as weaknesses or faults in a system, design, procedure, implementation or security mechanism that exposes information or the supporting systems to an attack (Pfleeger & Pfleeger, 2003; Whitman & Mattord, 2010). A threat is an entity, set of circumstances or occurrence that has the potential to cause harm, loss or otherwise breach security (Pfleeger & Pfleeger, 2003; Whitman & Mattord, 2010). Mechanisms used to address vulnerabilities are known as controls or countermeasures. A consequence, or impact, is the effect of an incident, and it reflects the level, duration and nature of the loss resulting from the incident (Department of Homeland Security, 2009).

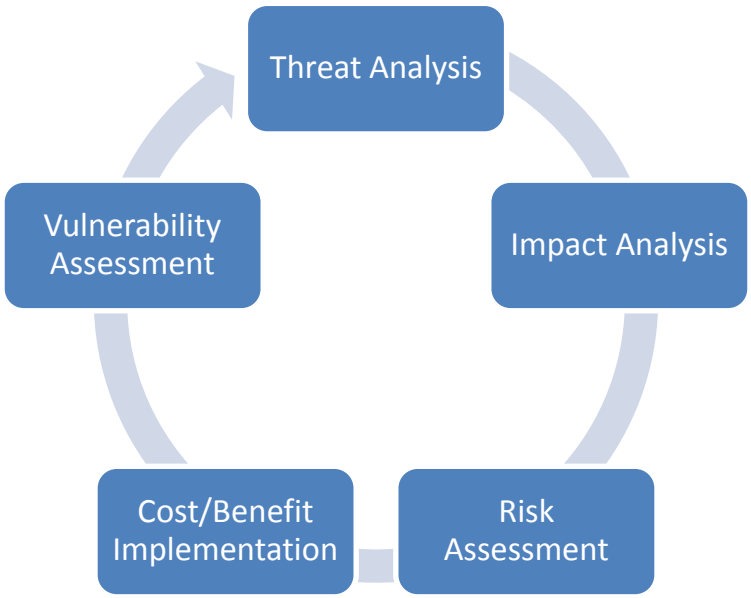


Figure 2.22: The Information Security Lifecycle, adapted from Peltier, Peltier and Blackley (2005)

Pfleeger and Pfleeger (2003) define risk as the possibility for harm to occur; however there are a number of variations of this, which will be discussed later. It is virtually impossible to prevent all risk or vulnerabilities; a defender will have to successfully protect all possible vulnerabilities, whereas an attacker only needs to expose and exploit a single vulnerability. In addition, protecting all systems from all risks may become prohibitively expensive; therefore there is a certain amount (or nature) of risk that an organisation is willing to accept, known as risk tolerance (Whitman & Mattord, 2010). Usually after a risk assessment has been conducted only the risks and associated vulnerabilities that do not fall into the acceptable range have controls applied. For those risks that are mitigated via controls, the remaining risk to the asset after the control has been applied is known as residual risk (*ibid*.).

As mentioned above, there are variations on the definition of risk. One of the more common calculations to determine risk is that it is the product of the probability of an incident occurring (i.e. the probability of a threat exploiting a vulnerability) and the magnitude of the impact or loss (Boehm, 1991), as illustrated in Equation 2.16.

$$\text{Risk} = P_{\text{incident}} \times |\text{Impact}| \qquad \textbf{2.16}$$

As an example, if there is a 50% chance that a computer will be infected by a virus (P_{virus} = 0.5) in a period of a year, and the total cost as a result of the infection occurring would be R2000, then the

risk can be calculated as R1000. The total cost of the infection may include the salary of the employees who are idle waiting for the virus to be removed, the loss due to the delay of a project, and the cost of the virus removal itself. The impact or loss may be measured as an actual monetary value, if it is available; however in some instances it may not be possible to assign or predict the actual monetary loss.

The $P_{incident}$ term in Equation 2.17 may be expanded to include the contributions of the threats, vulnerabilities, and controls, as illustrated by Equation 2.17 (Wik, 2002):

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability}}{\text{Countermeasure}} \times \text{Impact} \qquad \textbf{2.17}$$

Risk may also be determined by using a Risk Matrix (Habegger, 2008), shown in Table 2.11. Risk again is determined by the probability and potential impact, however ranked values are used; this method may be useful when it is impossible to accurately determine a figure for the probability or potential loss.

Table 2.11: Risk Rating Matrix

Impact	**Probability**		
	Low	*Medium*	*High*
Low	1	2	3
Medium	4	5	6
High	7	8	9

A variation on this is used by Anderson *et al*. (1999), shown in Table 2.12.

Table 2.12: Vulnerability Distinctions (Anderson, 1999)

	Damage Potential	
	Limited	**Serious**
Easy to fix	Type 1 (easy/limited)	Type 2 (easy/serious)
Difficult to fix	Type 3 (difficult/limited)	Type 4 (difficult/serious)

There are two approaches to assessing the vulnerabilities; the first is as part of the risk assessment as described above. The second approach regards vulnerability as a combination of risk analysis and emergency management evaluation, where the vulnerability is the collective results of risks and the ability of an organisation, nation, society, or local municipal authority to cope with and survive external and internal emergency or crisis situations (Wenger, Metzger, & Dunn, 2002).

2.7.1 Vulnerability and Risk Assessment Techniques

There are a number of techniques and methodologies to conduct risk and vulnerability assessment. This section provides a summary of the techniques that are relevant to this dissertation; the majority of techniques are taken from Habegger (2008), who provides a more extensive list. These techniques will be used when developing and proposing the new framework in Chapter 5, and implementing the framework in Chapter 8. Aspects of this section were previously published in van Niekerk and Maharaj (2011a).

2.7.1.1 Risk Matrices

The risk rating matrix is shown in Table 2.11 above. A slight variation of this is the risk level matrix, illustrated in Table 2.13. An example of a qualitative risk matrix is shown in Table 2.14.

Table 2.13: Risk Level Matrix, Adapted from (Wenger, Metzger, & Dunn, 2002)

Impact	**Probability**		
	Low (0.1)	*Medium (0.5)*	*High (1.0)*
Low (10)	Low (0.1x10=1)	Low (0.5x10=5)	Low (1x10=10)
Medium (50)	Low (0.1x50=5)	Medium (0.5x50=25)	Medium (1x50=50)
High (100)	Low (0.1x100=10)	Medium (0.5x100=50)	High (1x100=100)
Key:	High >50-100	Medium >10-50	Low >1-10

Table 2.14: Qualitative Risk Matrix

Impact	**Probability**				
	Very Low	*Low*	*Medium*	*High*	*Very High*
Very High	Medium	High	High	Very High	Very High
High	Low	Medium	High	High	Very High
Medium	Low	Low	Medium	High	High
Low	Very Low	Low	Low	Medium	High
Very Low	Very Low	Very Low	Low	Low	Medium

2.7.1.2 Delphi Technique

The Delphi Technique is an information-gathering technique which is used to reach a consensus of experts on a subject. This technique aids in reducing bias in data and prevents any one person from

having a strong influence on the outcome, as the subject experts participate anonymously. Thoughts on the subject in question are solicited by means of a questionnaire. The responses of the participants are summarized and then re-circulated or further comment in order to achieve consensus, which may be reached in several rounds (Habegger, 2008). The follow-up interviews may also be used to gain deeper insight into previous responses. Expert assessment and interviews may be used to assess critical infrastructure (Wenger, Metzger, & Dunn, 2002); this technique may be employed in this role. The interviews may also be conducted via electronic means, such as email and instant messengers; this is known as the E-Delphi technique (Lindqvist & Nordanger, 2007).

2.7.1.3 Focus Groups

Focus groups can be considered as a group interview, consisting of an open-ended, structured discussion with a representative group. Focus groups explicitly use group interaction as part of the technique; people are encouraged to talk to one another and may ask questions, exchange anecdotes, and comment on each participant's experiences and points of view. One or more interviews with small groups of participants are conducted (Habegger, 2008). This is another technique that may be used to gain expert assessment of critical infrastructures.

2.7.1.4 Simulation

Simulation use models that translate uncertainties that are specified at a detailed level into their potential impact on processes or systems; usually computer models and estimates of risk are used to conduct the simulation (Habegger, 2008).

2.7.1.5 Monte-Carlo Simulation

Monte-Carlo simulations are a type of “what-if” simulation that measures the effects of uncertainty on a process or system through the use of random numbers. Traditional “what-if” simulations reveal what is possible, whereas a Monte-Carlo simulation reveals what is probable (Habegger, 2008).

2.7.1.6 Trend Analysis

Trend analysis is an analytical technique that attempts to forecast future outcomes based on historical results. It is a method for predicting the variance from a baseline parameter by using collected data from earlier periods, and projects how much a parameter might diverge from the baseline at some future point assuming no changes are made and the underlying patterns from the previous periods will continue to exist in the future (Habegger, 2008).

2.7.1.7 PESTEL

PESTEL is an analytical tool used to systematically analyse an organisation's environment and to structure identified factors for specified categories. The PESTEL framework uses six different categories of factors that may affect the organisation under consideration: Political, Economic, Societal, Technological, Environmental/Ecological, and Legal factors (Habegger, 2008).

2.7.1.8 Strengths, Weaknesses, Opportunities, Threats (SWOT) Analysis

A SWOT assessment structures information and generates strategic planning alternatives by analysing both internal and external factors that influence an organisation. The organisation's strengths and weaknesses form the internal factors, while opportunities and threats constitute the external factors (Habegger, 2008).

2.7.1.9 The Threats-Vulnerabilities-Assets Worksheet

A Threats-Vulnerabilities-Assets (TVA) worksheet is used at the beginning of a risk assessment process in order to identify and list the vulnerabilities that associate specific threats with assets (Whitman & Mattord, 2010). A threat may have multiple associated vulnerabilities for an asset. While this worksheet considers assets, it could be easily adapted to consider an infrastructure, and is a useful tool to present the vulnerabilities and their associated threats.

2.7.1.10 Graph Theory Analysis

Graph theory may be used to analyse networks and infrastructures; it is useful in identifying critical nodes, and possible singularities of choke points; destruction of these nodes may result in segmentation or failure of a network or infrastructure. Lewis (2004) discusses the model-based vulnerability analysis (MBVA), where an infrastructure is represented as a graph; once the critical nodes are identified they are analysed using fault-tree and event-tree analysis. The critical nodes are identified by performing a scale-free network test. A network is scale-free if the node distribution for each degree of node (a node degree is the number of edges that connect to it) is approximated by $degree^{-p}$, where $p > 1$. For scale-free networks the critical nodes are the one of the highest degree; if the network is not scale-free then it may be a small world network, where there are critical clusters or neighbourhoods of nodes of high degree (Lewis, 2004).

Shake, Hazzard, and Marquis (1999) model links in fibre-optic network as an electronic resistive circuit, where each edge has a vulnerability value. The overall vulnerability value between two nodes may then be calculated as one would calculate the value of the equivalent resistance; the vulnerability of links in series is the sum of their individual vulnerabilities, while the vulnerability

of links in parallel is the product of the individual values divided by the sum of the individual values (Shake, Hazzard, & Marquis, 1999).

2.7.2 Frameworks and Processes

This section provides an overview of selected frameworks that have been proposed to analyse vulnerabilities and risk. These frameworks are relevant to the development of the new vulnerability assessment framework, proposed in Chapter 4. Aspects of this section were previously published in van Niekerk and Maharaj (2011a).

2.7.2.1 Minimum Essential Information Infrastructure (MEII) Process

The Minimum Essential Information Infrastructure (MEII) process was proposed by Anderson *et al*. (1999). The concept is based upon the Minimum Essential Emergency Communication Network established to ensure emergency messages could be received by nuclear forces in the United States during the Cold War. The MEII, however, was proposed as an answer to the threat of a cyber-based attack on the information infrastructure of the United States. Due to a number of concerns, it was deemed impractical to develop a static or fixed portion of the infrastructure that was hardened or protected against all forms of attack, especially due to the speed with which computer, networking, and communication technology was advancing. The MEII was therefore developed as a process, which can be applied to portions or local elements within a larger infrastructure (Anderson, *et al*., 1999).

The MEII process is as follows:

1. Identify the critical information functions which are essential for the unit or infrastructure element to successfully complete its objectives or mission.
2. Determine the information systems that are essential to accomplish the information functions.
3. Identify vulnerabilities for each information system. The system vulnerabilities that the MEII process identifies are categorised in Table 2.15.
4. Identify techniques that can be used to mitigate each of the identified vulnerabilities. Table 2.16 shows a list of security techniques and their impact on each of the vulnerabilities.
5. Implement the security techniques.
6. Simulate a variety of threat scenarios to assess the robustness of the security techniques that were selected.

Table 2.15: System Vulnerabilities, adapted from Anderson *et al*. (1999)

Vulnerability	A system or process:
Inherent Design/Architecture	
Uniqueness	That is unique and may be less likely to have been thoroughly tested and perfected.
Singularity	Representing a single point of failure, or even acting as a "lightning rod" for attacks.
Centralisation	In which all decisions, data, and control must pass through a central node or process.
Separability	That is easily isolated from the rest of the system.
Homogeneity	In which a flaw may be widely replicated in multiple identical instances.
Behavioural Complexity	
Sensitivity	That is especially sensitive to variations in user input or abnormal use-an attribute that can be exploited.
Predictability	Having external behaviour that is predictable; attackers can know the results their actions will have.
Adaptability and Manipulation	
Rigidity	That cannot be easily changed in response to an attack, or made to adapt automatically under attack.
Malleability	That is easily modifiable.
Gullibility	That is easy to fool.
Operation/Configuration	
Capacity limits	Near capacity limits that may be vulnerable to DoS attacks.
Lack of recoverability	Requiring inordinate time or effort to recover operation relative to requirements.
Lack of self-awareness	That is unable to monitor its' own use.
Difficulty of management	That is difficult to maintain, so known flaws may not be found or fixed.
Complacency and co-optability	With poor administrative procedures, insufficient screening of operators, etc.
Indirect/Non-physical Exposure	
Electronic accessibility	For which remote access provides an attack opening.
Transparency	That allows the attacker to gain information about it.
Direct/Physical Exposure	
Physical accessibility	In which attackers can get close enough to a system to do physical damage.
Electromagnetic susceptibility	In which attackers can get close enough to use radiated energy to disable a system.
Supporting Facilities/Infrastructures	
Dependency	That depends on information feeds, power, etc.

Table 2.16: The Impact of Security Controls on Vulnerabilities, adapted from Anderson *et al*. (1999)

Key:

- Addresses vulnerability directly
- Addresses vulnerability indirectly
- Not applicable
- May incur vulnerability indirectly
- May incur vulnerability directly

Vulnerability Attributes		*Security Techniques*: Heterogeneity	Static resource allocation	Dynamic resource allocation	Redundancy	Resilience / robustness	Rapid recovery & reconstitution	Deception	Segmentation / decentralisation / quarantine	Immunologic identification	Self-organisation & collective behaviour	Personnel management	Centralised management of information resources	Threat warning response structure
Inherent design architecture	Uniqueness													
	Singularity													
	Centralisation													
	Separability													
	Homogeneity													
Behav-ioural complex-ity	Sensitivity													
	Predictability													
Adaptability & manipulation	Rigidity													
	Malleability													
	Gullibility													
Operation & configuration	Capacity limits													
	Lack of recoverability													
	Lack of self-awareness													
	Difficulty of management													
	Complacency & co-optability													
Indirect exposure	Electronic accessibility													
	Transparency													
Direct exposure	Physical accessibility													
	Electromagnetic accessibility													
Dependency on supporting facilities														

The vulnerabilities identified, shown in Table 2.15, are sub-divided into categories: the design and architecture of the infrastructure, the behavioural complexity, the adaptability and ability to manipulate the infrastructure, the operation and configuration of the infrastructure, indirect and direct exposure, and the dependency on other infrastructures.

The MEII framework provides generic vulnerabilities that may be applied to most infrastructures; however, due to the rapid evolution of information systems, this framework can be considered a bit dated. While the majority of vulnerabilities listed are still applicable, there are some additional aspects and alterations to those listed due to the evolving technology. The convergence of communications technologies, such as mobile phones, online applications (particularly social networks) and processing power may introduce new vulnerabilities or impact on those that are already identified in the framework. Due to the rise of mobility and wireless technologies, there will now be an overlap between the electronic accessibility listed under indirect exposure and electromagnetic accessibility listed under direct exposure.

The MEII framework provides a guide to categories where vulnerabilities may exist. Some may constitute an entire vulnerability; such as operating close to the capacity limit. Others, such as electronic accessibility, may encompass a range of technical vulnerabilities that reside in the applications or protocols that are used to facilitate the electronic access. The framework also provides suggestions for mitigating the vulnerabilities. However, there is less focus on the specific nature of the threats, and again there is not a single rating for the overall vulnerability of an infrastructure. The centralisation vulnerability can be illustrated through the wide-spread international outages of BlackBerry services due to the failure of centralised components (Press Association, 2011).

2.7.2.2 National Institute of Standards and Technology (NIST) Framework

The NIST framework is comprehensive, and is the standard for the United States Federal Government (Elky, 2006). The framework may also be incorporated into the system design lifecycle (Stoneburner, Goguen, & Feringa, 2002).

This framework consists of nine steps (Stoneburner, Goguen, & Feringa, 2002):

1. Characterise the system
2. Identify threats
3. Identify vulnerabilities
4. Analyse controls

5. Likelihood determination
6. Analyse impacts (loss of confidentiality, integrity, or availability)
7. Determine risk
8. Recommend controls
9. Document results

As mentioned, the NIST framework is a comprehensive process and details various sources that may be used to identify potential threats and vulnerabilities, such as attack history, intelligence reports, vendor notifications and the mass media (Stoneburner, Goguen, & Feringa, 2002). Other than using sources for vulnerability identification, the only other method suggested is the use of automated network analysis tools, and does not provide much detail on other forms of information infrastructures.

2.7.2.3 Facilitated Risk Analysis and Assessment Process (FRAAP)

This is a framework developed by Peltier (2005). It is primarily a quantitative assessment, however it does not aim to precisely quantify the risks as the documentation and consumption of time to do so is seen as too large, and exact estimates of the potential impacts are not required to determine if a control is required (Peltier, 2005). During the process brainstorming and open sources are used to identify the threats and their potential impacts to broadly categorise the risks, and possible controls that could be implemented (*ibid*.). The brainstorming focuses on the threats to the confidentiality, integrity and availability of information resources, and considers each process, system or operations individually. These assessments make use of risk matrices and worksheets (*ibid*.). There is also a pre-FRAAP phase, where a pre-screening is done to identify systems and processes that are required to undergo the risk assessment. The post-FRAAP phase involves the reporting and documenting the outcomes of the process, specifically the identified threats, associated risk levels, controls and responsible parties (*ibid*.).

The FRAAP framework has a variation which allows for assessing infrastructure risk, and a separate variation allows for the assessment of vulnerabilities (Peltier, 2005). The infrastructure variation focuses on threats and impacts to the infrastructure; and the vulnerability variation does not make provision for how the vulnerabilities are to be identified.

2.7.2.4 Factor Analysis of Information Risk (FAIR)

Jones (2005) developed this framework, which combines multiple factors to calculate risk. The FAIR framework utilises the risk matrix to determine the value of each level as shown in Table 2.17. Each variable is represented by a five-point scale, generally ranging from very high to very low. The framework provides definitions for the terms illustrated in the table; some may differ slightly from those discussed previously. The definitions provided by Jones (2005) are:

- Risk – the probable frequency and probable magnitude of future loss;
- Loss event frequency – the probable frequency that a threat will cause harm to an asset in a given timeframe;
- Threat event frequency – the probable frequency that a threat will act against an asset in a given timeframe;
- Vulnerability – the probability that an asset will succumb to a threat action that has been made;
- Contact frequency – the probable frequency that a threat will come into contact with an asset in a given timeframe;
- Action frequency – the probability that a threat will act against an asset should contact occur;
- Control strength – the ability of a control to prevent or deter a threat action;
- Threat capability – the probable level of force that a threat is able to apply against an asset;
- Probable loss magnitude – this is the estimated loss resulting from a threat action against an asset;
- Primary loss factors – this is the probable loss as a direct result of a threat action, and is comprised of threat loss factors and asset loss factors;
- Threat loss factors – considers the location of the threat (an internal or external threat) and the type of action that may be performed, such as misuse, modification or denial;
- Asset loss factors – this is comprised of volume (the more assets at risk, the higher the loss magnitude) and the value and liability for each asset, such as the sensitivity of the information, legal or regulatory implications, loss of image and competitive advantage, and the cost of the asset itself.
- Secondary loss factors – these are losses that occur indirectly from an incident, and are comprised of organisational loss factors and external loss factors;

- Organisational loss factors – these factors are internal losses such as liability with regards to due diligence, and the response to the incident (including remediation, containment and recovery);
- External loss factors – these are indirect losses due to influence by the media, stakeholders, competitors and legal ramifications.

The threat event frequency is determined by applying the risk matrix to the contact frequency and action frequency; the vulnerability is determined by the control strength and the threat capability. The loss event frequency can then be determined by applying the results of the vulnerability and threat event frequency to a threat matrix. The probable loss magnitude and risk are determined similarly. This framework has a detailed depth to determining risk and a consistent way of estimating loss, threats and vulnerability. This allows simple adaptation of variables to the specific case of IW threats for specific assets. It does not however provide an overall vulnerability or risk figure for an entire infrastructure.

Table 2.17: FAIR Constituents, adapted from Jones (2005)

Risk							
Loss Event Frequency			X	*Probable Loss Magnitude*			
Threat Event Frequency	X	Vulnerability		Primary Loss Factors	X	Secondary Loss Factors	
• Contact frequency • Action frequency		• Control strength • Threat capability		• Asset loss factors • Threat loss factors		• Organisational loss factors • External loss factors	

2.7.2.5 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

The OCTAVE framework was developed at Carnegie Mellon University, and uses a workshop-based approach for the analysis. The framework's structure is outlined as (Software Engineering Institute, 2003):

- Planning
- Phase 1: Organisational view
    - Assets
    - Threats
    - Current practices
    - Organisational vulnerabilities

    - Security requirements
- Phase 2: Technological view
    - Technological vulnerabilities
- Phase 3: Strategy and plan development
    - Risks
    - Protection strategy
    - Mitigation plans

During implementation, the framework consists of eight processes, as outlined below (Software Engineering Institute, 2003):

- Phase 1: Organisational view
    - Process 1: Identify senior management knowledge
    - Process 2: Identify operational area management knowledge
    - Process 3: Identify staff knowledge
    - Process 4: Create threat profiles
- Phase 2: Technological view
    - Process 5: Indentify key components
    - Process 6: Evaluate selected components
- Phase 3: Strategy and plan development
    - Process 7: Conduct risk analysis
    - Process 8: Develop protection strategy
        - Workshop A: Protection strategy development
        - Workshop B: Protection strategy selection

The OCTAVE framework is primarily an organisational information security risk assessment; however some information infrastructure assessments are conducted under the second phase and when creating threat profiles. However, like the NIST framework, this seems limited to using automated tools to assess computer networks, and does not cater for larger information infrastructures.

2.7.2.6 Tool-driven Assessments

Risk Watch is a tool that uses a database of expert knowledge to guide the user through the risk assessment and report on compliance and provide advice on managing risks (Elky, 2006). The database also includes statistical data to support quantitative assessment (*ibid*.). The Consultative,

Objective and Bi-Functional Risk Analysis process focuses on a business approach to risk assessments, and also utilises knowledge bases and templates to aid the user (*ibid.*).

2.7.2.7 Summary of Frameworks

Of the frameworks discussed, the most suitable for consideration for adapting to a scalable framework for infrastructure vulnerability and risk assessments with regards to IW threats are the MEII and FAIR frameworks due to their structure and scope. The MEII framework is especially suitable as it was designed as a vulnerability assessment for infrastructure elements; due to the rapidly evolving landscape of information systems the framework may be considered as being dated, however the generic vulnerabilities maintain its applicability. The OCTAVE and NIST frameworks may be useful for guiding high-level processes of the risk and vulnerability assessment. Tool driven assessments may in some cases be suitable for performing specific analysis of software components or existing organisational procedures. None of the frameworks appear to provide a single measure of the vulnerability of an entire infrastructure; but rather focus on individual elements or assets.

2.7.3 Relating Risk and Vulnerabilities to Critical Infrastructure Protection and Information Warfare

The definitions presented in Section 2.7 hold true for critical infrastructure protection and IW, however the calculations may have subtle differences and subcategories when dealing with CIP and IW. Consequences usually are divided into four categories: public health and safety; direct and indirect economic impact; psychological; and governance or mission impacts (Department of Homeland Security, 2009). When calculating the risk of an intentional hazard, vulnerability is measured as the likelihood that an attack is successful, given that it is attempted; the threat for an intentional hazard is the likelihood that an attack will be attempted by an adversary (Department of Homeland Security, 2009). An example is given for the case of a terrorist attack, where the threat is estimated based on the capabilities and intent of the terrorists (Department of Homeland Security, 2009), a similar estimation may be used for IW. Figure 2.23 shows the process suggested by the Department of Homeland Security (2009) for critical infrastructure protection; it can be seen that the third step is to assess risks.

Figure 2.23: Continuous Process for Critical Infrastructure Protection, adapted from Department of Homeland Security (2009).

To calculate the risk of an IW attack, it may be necessary to determine the economic consequences of the attack. Erbschloe (2001) provides a guide to the impacts over time for a single organisation, an industry sector, and a country or region for a cyber-attack. These impacts are summarised in Table 2.18. An attack on a specific information infrastructure is equivalent to an attack on an industry sector. It is conceivable that the impacts listed in Table 2.18 could have secondary effects, such as an increase in unemployment due to a decrease in the economic stability following the attack.

Table 2.18: Economic Impacts Over Time for a Cyber-Attack, adapted from Erbschloe (2001)

Target	Immediate Impact	Short-Term Impact	Long-Term Impact
Organisation	Damage to systems that require human intervention to repair or replace Business operations disrupted Cash flow and transactions delayed	Loss of contractual relationships or loss of retail sales Reputation negatively impacted Development of new business hindered	Market valuation declines Investor confidence eroded Stock price declines
Industry Sector	Supply chain systems damaged, requiring human intervention to repair or replace Sector production disrupted Cash flow and transactions delayed	Disruption of productivity in organisations that consume sector products Reputation of the sector negatively impacted Development of new business hindered	Investor confidence eroded Stock prices declines across the sector Market valuation declines across the sector
Country	National banking or commerce disrupted National industrial production disrupted Delay of military activity	International trade disrupted Reputation of the country's economy negatively impacted Military activity continually hindered	Investor confidence eroded Stock prices of companies within the country decline Market valuation of companies within the country decline

Vulnerability and risk assessments are generally considered as defensive measures as their objective is to identify potential problem areas and then mitigate the chance of an incident occurring; however, with sufficient information, it may be possible for an attacker to conduct vulnerability and risk assessments on a target infrastructure in order to plan the attack to maximise its impact. These

tools can therefore aid decision making in applying offensive resources to increase the effectiveness or likelihood of success of the attack.

2.8 Modern Information and Communications Technology

This section presents a background to modern information and communication technology. Section 2.8.1 describes the universal serial bus (USB). Wireless networking is described in Section 2.8.2, and Web 2.0 technologies are covered in Section 2.8.3. As the focus of the dissertation is on the mobile phone infrastructure, Section 2.8.4 will provide a description of this infrastructure in some details. Section 2.8.5 will describe cloud computing.

2.8.1 Universal Serial Bus

USB provides for high data transfer rates to and from devices; USB 2.0 allows for transfer rates up to 480Mb/s (60MB/s) (Compaq, *et al*., 2000), and USB 3.0 allows for a theoretical data transfer of up to 5Gb/s (Perenson, 2010). This, and other technological advancements, has resulted in the introduction of mass storage devices that are physically smaller than the old 3.5" magnetic discs or a CD, yet can hold significantly more data. The most common flash drives can hold 2GB up to 32GB of data. USB is also used to connect external hard-drives, which can contain terabytes of data. This is a risk as large amounts of information could be compromised by copying should an attacker gain physical access. Also the autorun capabilities of these devices makes then ideal for a vector to spread malware; the Win32/Autorun worm was one of the most common malware types in 2010 (Microsoft Corporation, 2011a).

2.8.2 Wireless Networking

Wireless networking for local area networks (WLAN) is governed by the Institute for Electrical and Electronic Engineers (IEEE) 802.11 standards, which define the media access control (MAC) and physical layers. The variations of the standards may have different levels of security and data transfer rates; the IEEE 802.11b variant had transfer rates of 11 Mbps, whereas the IEEE 802.11g version has a theoretical transfer rate of 54 Mbps (Smyth, McLoone, & McCanny, 2006). WLAN usually operates on a frequency range of 2.4GHz to 2.48GHz (Nichols & Lekkas, 2002). A security issue with wireless is that it is very difficult to constrain wireless signals, making it possible to physically connect to the network without physically being on an organisation's property. It is also easier to disrupt (i.e. jam) or eavesdrop on wireless connections than it would be on a physical line. Shielding is the most effective way of constraining wireless signals to physical boundaries; however

it may become prohibitively expensive for large buildings. There are various security mechanisms such as wired equivalent privacy (WEP), Wi-Fi protected access (WPA), and restricting MAC addresses that may connect to the access point; however a determined and sophisticated attacker may still be able to circumvent these (Whitman & Mattord, 2010).

Bluetooth is designed as a personal wireless network, primarily to connect two devices or a device to a peripheral; such as a mobile phone to a head-set. Bluetooth specifications are governed by the IEEE 802.15 working group and the Bluetooth special interest group (Dwivedi, Clark, & Thiel, 2010). Bluetooth also operates at a frequency of 2.4GHz (Nichols & Lekkas, 2002), and has three power classes: power class 1 is used for access devices, and has a maximum output power of 100mW; peripheral devices such as keyboards fall under power class 2, with a maximum of 2.5mW output power; power class 3 has a maximum output power of 1mW, and is used for devices such as headsets (Dwivedi, Clark, & Thiel, 2010). Early versions of Bluetooth had transmission rates of up to 400Kbps (Nichols & Lekkas, 2002), however more modern Bluetooth versions can achieve up to 1Mbps (Dwivedi, Clark, & Thiel, 2010). Bluetooth access points and devices can form ad-hoc networks. Piconets are where two or more devices organise themselves dynamically; a scatternet is where two or more piconets where a device acts as a slave in one piconet, and a master in a second piconet (*ibid*.).

Both WLAN and Bluetooth can be jammed and intercepted due to the fact that they are based on radio waves; therefore the electronic warfare jamming and detection discussed in Section 2.5 are applicable. In addition to traditional jamming which targets the physical layer, there are vulnerabilities in the media access control (MAC) layer which allows attackers to manipulate the management and control frames (Motorola, 2010). Like wired networks, the wireless networks are also susceptible to man-in-the-middle attacks. Wardriving is the process of driving through an area with a laptop of other device that scans for open wireless access points, or ones which have not been sufficiently secured (Whitman & Mattord, 2010). Warwalking is a similar concept, where the travelling is done on foot; warchalking is where those scanning for wireless networks leave marks indicating the location of the open or unsecured wireless access point (*ibid*.). Attacks on Bluetooth include Bluejacking, where an attacker exploits Bluetooth pairing to send illegitimate messages or access data on the targeted device; BlueChop, which is a DoS attack on Bluetooth Piconets; and BlueDump, which is used to sniff key exchanges between devices by spoofing the address of one of the devices (Dunham, 2009).

2.8.3 Web 2.0

In this section the background to the modern phenomenon of Web 2.0 and online 'social networking' will be provided. An earlier version of this section was published in Pillay, van Niekerk, and Maharaj (2010), and the content presented here was originally generated by the candidate.

The term web 2.0 covers a number of technologies, including online social networking, wikis, and blogs (O'Reilly, 2005). Web 2.0 is currently classified as the new media; where the new media can be defined as the incorporation of new information and communications technologies into the traditional media (Williams, Rice, & Rogers, 1988). Web 2.0 differs from the traditional web and media in that it focuses on user-generated content, collaboration, and the collective intelligence principle (O'Reilly, 2005). As such, it can be seen as a many-to-many communications, whereas web 1.0 is still considered as a one-to-many communications; these concepts are shown in Figure 2.24.

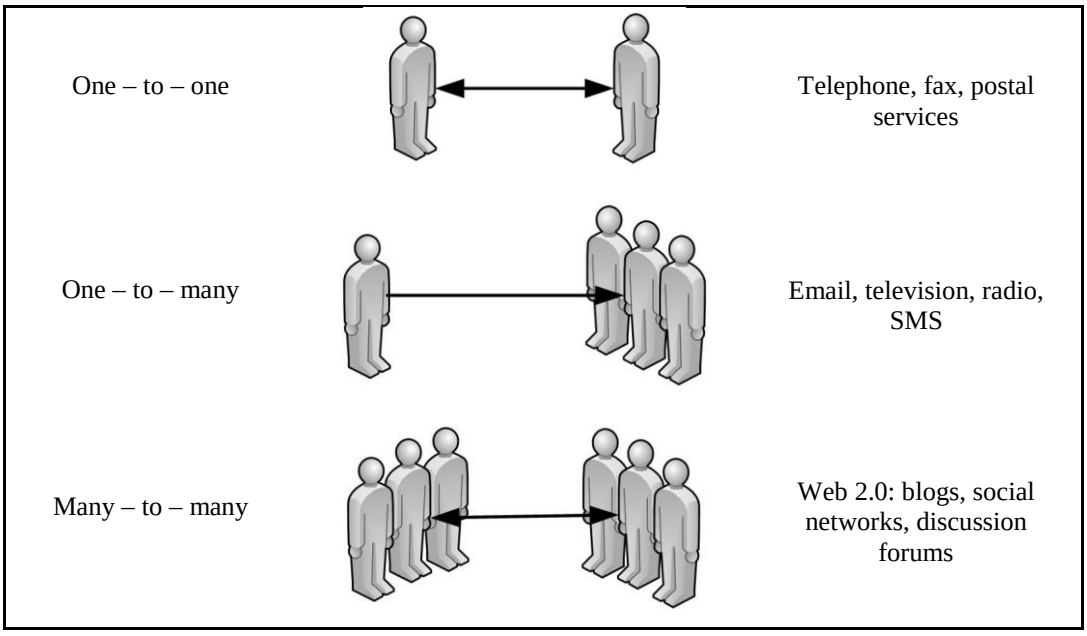


Figure 2.24: Modes of communication, Pillay, van Niekerk and Maharaj (2010)

Web 1.0 was different from the traditional media in that it provided content on demand; in the traditional media the audience were restricted to the broadcast times of what they wanted to view, whereas on the Internet the audience could go online and access the desired content when it suited them. A level of interaction was provided where the audience could provide feedback to the broadcasters via short message service (SMS), call-lines and email; on the web users were provided

with a space to comment on stories or items. Web 2.0 came to full strength when the users generated their own content, and comment on the content that others have shared online. As many mobile devices now have integrated social networking capabilities, users can access and share content on the move.

More technical vulnerabilities and threats are exhibited by Web 2.0 technologies compared to the traditional Web 1.0 sites due to the scripting requirements that provide the user with the ability to upload content (Lawton, 2007). Common threats in Web 2.0 are cross-site scripting, cross-site request forgery, and mobile worms (*ibid.*). YouTube was affected by a cross-site scripting attack that appeared to have targeted the singer Justin Bieber (Barnett, 2010), as was Twitter, where attackers used a cross-site scripting flaw to open unauthorised marketing pop-ups when the user's mouse cursor moved over a link (Twitter, 2010). Many Web 2.0 sites use applications that allow video and audio playing; these applications may also have vulnerabilities which can be exploited (Lawton, 2007). Davidson and Yoran (2007) suggest that users are coming to expect the same interactivity and collaborative ability in the workplace as Web 2.0 provides; however, Naraine (2009) states that users do not have the same restraint with personal information on Web 2.0 as they would when disclosing the information in person. These factors may result in Web 2.0 posing a risk regarding information leaks. The security implications of Web 2.0 will be discussed in more detail in Section 5.6.

2.8.4 Mobile Phone Infrastructure

This section will provide the background to the mobile phone infrastructure. Mobile phones have advanced from purely voice communications and short message services (SMS); they have the ability to transfer data and multimedia, and have additional connectivity options, such as USB, Bluetooth and WLAN. Section 2.8.4.1 describes the physical architecture of the mobile networks, Section 2.8.4.2 describes the wireless links, and Section 2.8.4.3 discusses the prevalence of mobile phones, with a focus on South Africa. The security concerns and IW aspects related to mobile communications will be introduced in Section 2.8.4.4, and discussed in more detail in Chapter 5.

2.8.4.1 Physical Infrastructure

The following description of the physical mobile phone infrastructure is an amalgamation from three sources: Enck, Traynor and La Porta (2005), Ojanpera and Prasad (1998), and Xenakis and Merakos (2006).

The devices themselves form mobile stations (MS), and they communicate to the base station (BS), or mobile phone tower, wirelessly. In South Africa this wireless link follows the Global System for Mobile Communications (GSM) standard and the Third Generation (3G) Wideband Code Division Multiple Access (WCDMA) standard, the other major 3G standard is known as CDMA2000 (Global Mobile Suppliers Association, 2010). The link from the mobile device to the base stations is known as the uplink, whereas the link from the base station to the device is known as the downlink. The reason the term cellular phone is commonly used is that the coverage area is divided into cells, each of which covered by a base station transceiver (BST). The mobile devices are free to roam within a cell, or into a different cell, at which time it will be handed over to the relevant base station.

The base station systems (BS) comprise of the BST, and the base station controller (BSC); multiple BSTs may connect to a single BSC (Ojanpera & Prasad, 1998; Xenakis & Merakos, 2006). The base stations connect to the mobile switching centre (MSC) via fibre-optic cable or wireless microwave data links between the BSC and MSC; the MSC connects the mobile phone infrastructure to the public switched telephone network (PSTN), which allows calls between the mobile devices and the fixed-line infrastructure (Enck, Traynor, McDaniel, & La Porta, 2005). The MSC is responsible for any circuit-switched services, such as voice calls, and connects to the core network and also provides a gateway to other network providers (Enck, Traynor, McDaniel, & La Porta, 2005; Xenakis & Merakos, 2006). The home location register (HLR) manages permanent information regarding the mobile users, including billing information (Enck, Traynor, McDaniel, & La Porta, 2005); the visitor location register (VLR) contains information related to the handling of the mobile station services (Xenakis & Merakos, 2006). The equipment identity register (EIR) contains information regarding the identity of the mobile equipment, and the authentication centre (AuC) contains security information for the subscribers' identity (*ibid.*).

There is little difference between the GSM and 3G network architectures as described by Ojanpera and Prasad (1998). The following descriptions cover the additional services such as short messages and data transfer for the GSM infrastructure. Short messages are routed via the short messaging service centre (SMSC); these may connect to external short message entities (ESME) which allow SMSs to be received from external locations, such as the web-based SMS services (Enck, Traynor, McDaniel, & La Porta, 2005). In simulations, Traynor *et al*. (2009) estimated that each HLR could operate with ten MSCs, and each MSC could control up to two hundred towers.

Data transfer was initially done through the global packet radio services (GPRS), which utilises the majority of the GSM infrastructure (Xenakis & Merakos, 2006). A serving GPRS support node (SGSN) is responsible for delivering the packets to and from the mobile station; a gateway GPRS support node (GGSN) provides external connection to the Internet and other data packet networks (*ibid*.).

The descriptions of the network architecture for the voice, SMS and GPRS services provide a picture of a generic mobile phone infrastructure, which is shown in Figure 2.25.

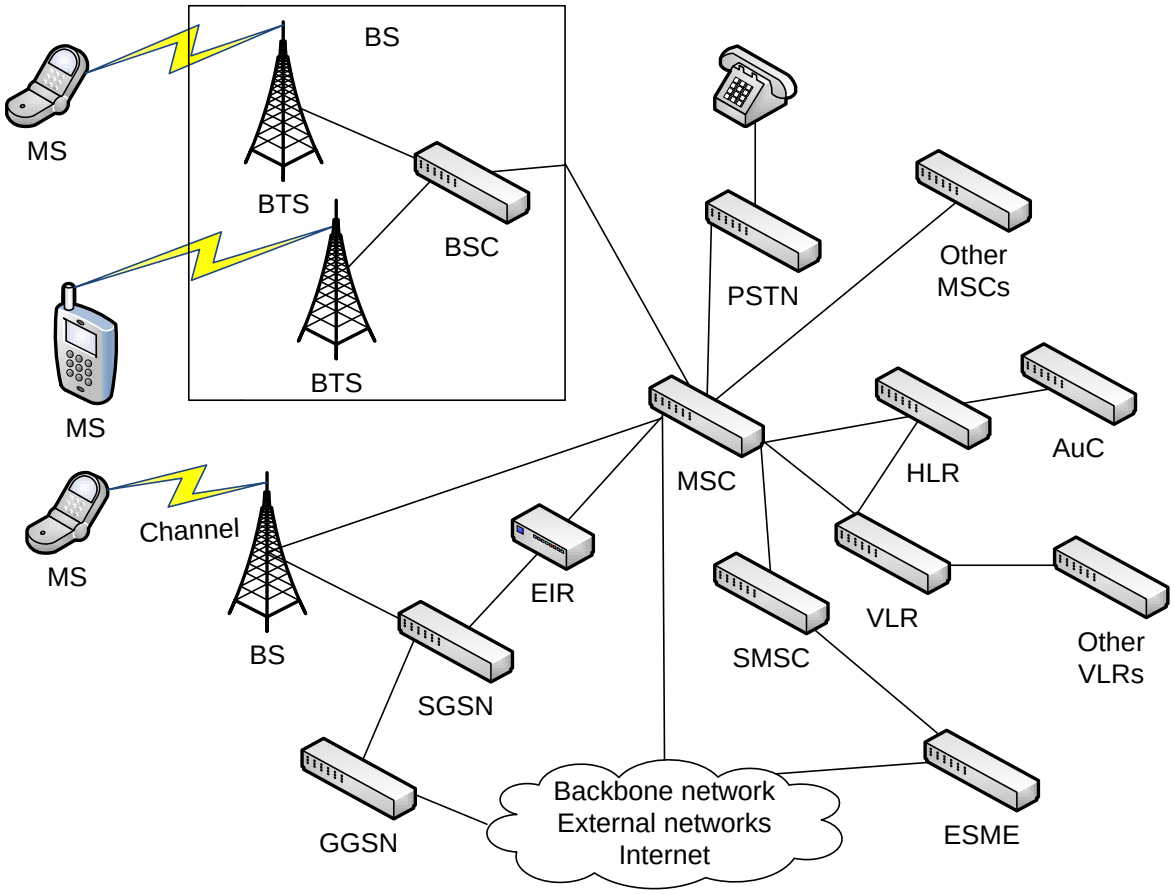


Figure 2.25: Mobile Phone Infrastructure

2.8.4.2 Wireless Physical Layer

The wireless physical layer in mobile phones provides the uplink from the device to the base station, and the downlink from the base station to the device. Two standards are used in South Africa: global system for mobile communications (GSM) and wideband code-division multiple-access (the abbreviation for the standard is WCDMA, whereas the abbreviation for general

wideband CMDA technology is W-CDMA), which is the deployed third generation (3G) standard in the country. The other major 3G standard is cdma2000.

GSM is a second generation (2G) mobile communications standard. It has four major operating frequencies: 850MHz, 900 MHz, 1800 MHz, and 1900 MHz, and uses 200 kHz channel (Ojanpera & Prasad, 1998). Multiple users are accommodated through time-division multiple-access, where each user or channel is allocated time slot to broadcast in (*ibid*.). GSM has evolved with the introduction of data services through GPRS, and data rates were increased through and enhanced data rated for GSM evolution (EDGE).

Both WCDMA and CDMA2000 uses DS-CDMA as discussed in Section 2.5.5, which is a form of LPI communications and has inherent noise-cancellation and anti-jam features. As WCDMA is the main standard used in South Africa, this will be focussed on. The spreading is performed with the aid of pseudo-noise sequences, which generate a series of chips. The digital signal is spread with the chips so that the signal is transmitted over a larger bandwidth than the original data signal would have required (Ojanpera & Prasad, 1998; Taub & Schilling, 1991). The correlation characteristics of the pseudo-noise sequences are also used to separate the users, as they have high auto-correlation and low cross-correlation. The same code is used for spreading and despreading; therefore any interference from other signals is cancelled due to the low-cross correlation (Ojanpera & Prasad, 1998; Taub & Schilling, 1991), as illustrated in Section 2.5.5. WCDMA uses Gold codes for the spreading sequence, and has possible chip rates of 4.096 Mcps (mega chips per second), 8.192 Mcps, and 16.384 Mcps for channel bandwidths of 5 MHz, 10 MHz, and 20 MHz, respectively (Ojanpera & Prasad, 1998).

For the purpose of simulating a mobile communications environment where multiple users are present, the environment will need to be described mathematically. Multi-user DS-CDMA communications can be described in matrix form as (Proakis, 2001; Verdu, 1998):

$$\mathbf{y}(i)=\mathbf{SAb}(i)+\mathbf{n}(i) \qquad \textbf{2.18}$$

where $\mathbf{y}(i)$ is the ith bit or symbol for each user, $\mathbf{S}$ is the spreading sequence for each user, $\mathbf{A}$ is a diagonal matrix with the amplitude of each user's signal, $\mathbf{b}(i)$ is the ith bit for each user, and $\mathbf{n}(i)$ is the noise or interference experienced by the ith bit of each user.

The output of a basic decorrelating multiuser detector can be described by (Proakis, 2001; Verdu, 1998):

$$r = Rb + n \quad (2.19)$$

where **r** is the bit stream that is the output of the matched filters for each user, **R** is a correlation matrix of all the spreading sequences described by **S**, **b** is the bits, and **n** is the interference. The purpose of the correlation matrix is to take into account interference between the signals; while the spreading sequences have low cross-correlation, there is still some interference. The simulations will be presented in Chapter 7.

The channels used for GSM and WCDMA are similar, and can be divided into two types: traffic channels and control channels (Enck, Traynor, McDaniel, & La Porta, 2005). The paging channel and random access channel are used to initiate voice and data services; devices are instructed by the base station to monitor a stand-alone dedicated control channel (SDCCH) which is used for authentication, enable encryption, and deliver SMS messages. Once the authentication is complete, a traffic channel is allocated for voice traffic. For the purposes of the dissertation, the SDCCH will be the primary channel considered in Chapter 7.

2.8.4.3 Prevalence of Mobile Phones

During the second quarter of 2010, it was reported that there were approximately 535 million WCDMA subscribers and approximately 4 billion GSM subscribers globally; this accounts for 89.7% of the approximately 4.933 billion mobile subscription worldwide (Global Mobile Suppliers Association, 2011a). In Africa there are approximately 350 million GSM subscribers and 20 million WCDMA subscribers (Global Mobile Suppliers Association, 2011b).

According to the State of the Cities Report (South African Cities Network, 2011b) 16% of households have access to both mobile phones and fixed line telecommunications; 67% only have access to mobile phones, 1% only has access to fixed line telecommunications, and 16% has no access. These figures are for 2009, and indicate a total of 83% of households have access to mobile phone, compared to 17% with access to fixed line telecommunications. The International Telecommunications Union (2011) estimates that there are 92.67 mobile subscriptions per 100 people in South Africa in 2009, compared to 8.62 fixed telephone lines per 100 inhabitants. This is a ratio of 10.75 mobile subscriptions per fixed line. There are an estimated 8.82 Internet users per 100 inhabitants in South Africa, and approximately 0.97 fixed broadband subscribers per 100 inhabitants, compared to 10.52 mobile broadband subscriptions per 100 inhabitants (International Telecommunications Union, 2011). This is a ratio of 10.85 mobile broadband subscriptions per fixed broadband subscriptions. These statistics illustrate the overwhelming prevalence of mobile

communications in South African society. The number of fixed line telecommunications has exhibited an annual decease from 2004 to 2009, whereas the mobile subscriptions have continued to grow (*ibid*.). This indicates that mobile communications are becoming more prevalent, to the detriment of the fixed line communications.

The prevalence of mobile phones may increase with the introduction of mobile commerce (m-commerce); online banking services use SMS for providing one-time codes, and mobile money such as M-Pesa has had huge success in Kenya (Aker & Mbiti, 2010). In addition, many development projects in Africa revolve around the innovative use of mobile phones and mobile applications; these projects include the health, education, and governance sectors (Aker & Mbiti, 2010). This additional functionality increases the importance of mobile communications in South Africa and elsewhere on the continent; it is possibly the backbone of the continent's telecommunications infrastructure.

2.8.4.4 The Mobile Infrastructure and Information Warfare and Security

This section relates aspects of IW to the mobile infrastructure. A previous version was published in van Niekerk and Maharaj (2010b). As electronic warfare targets the electro-magnetic spectrum, all wireless channels (particularly the physical layer) can be considered as falling under the auspices of electronic warfare. The infrastructure hardware and logical connections fall under network warfare, and the entire infrastructure will fall under information infrastructure warfare. Figure 2.26 shows a simplified mobile infrastructure and the relationships to these IW functional areas. It is also conceivable that the legitimate functionality of the mobile services may be used for malicious intent; in Kenya SMS services were used to distribute hate messages (Okeowo, 2008).

As with traditional computer-based systems and networks, mobile devices and infrastructures have security vulnerabilities and may be attacked. Modern mobile devices, in particular smartphones, are capable of being infected by malicious code or applications (Morales, 2009a); Fleizach *et al*. (2007) model the spreading of mobile worm infections using MMS and voice over IP. The simulations indicate that all mobile phones that could possibly be infected would be within a matter of minutes should there be no bandwidth constraints; taking bandwidth limitations into consideration the maximum number of infections could take up to 12 hours. This is attributed to the mobile infrastructure network reaching its processing capacity early in the malware propagation (Fleizach *et al*., 2007); this indicates that a DoS attack on the mobile infrastructure is possible. Enck *et al*. (2005) discusses and calculates the capacity of the logical control channels in order to illustrate the

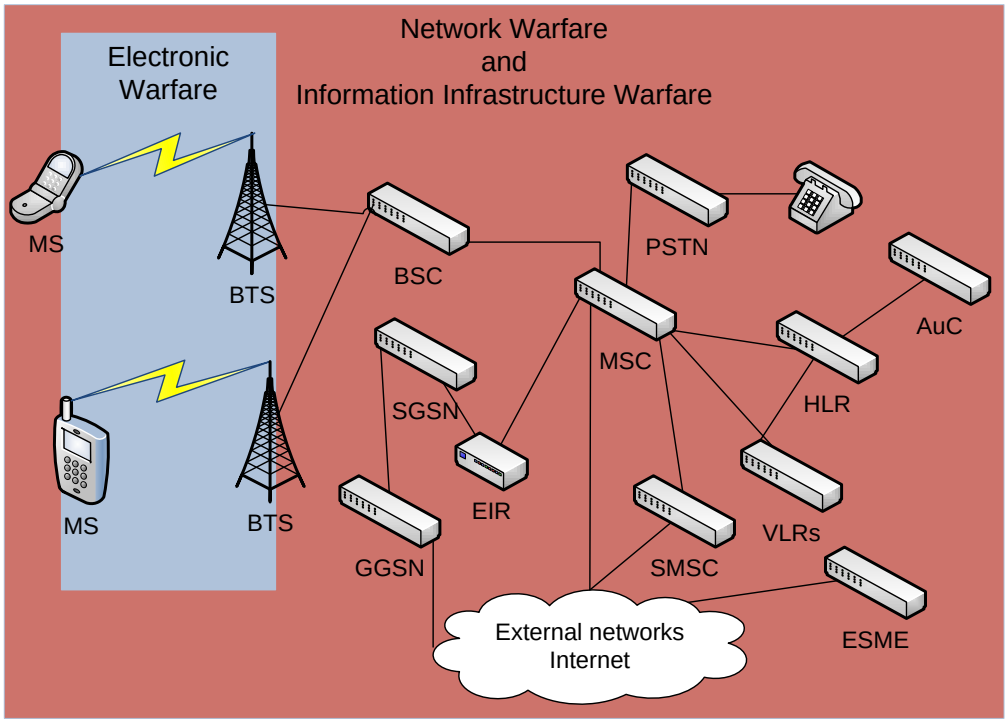


Figure 2.26: Relating the Information Warfare Functional Areas to the Mobile Infrastructure

possibility of using SMS services to perform a DoS attack on the mobile infrastructure; this is expanded in Traynor *et al*. (2009), who illustrate a possible DoS attack on the core mobile infrastructure.

The applications that run on mobile devices, as well as the communication capabilities may be attacked and the mobile device compromised (Dwivedi, Clark, & Thiel, 2010). It is also possible to eavesdrop on the wireless channels (Nohl & Paget, 2009), or attack the mobile infrastructure in order to eavesdrop, as occurred in Greece in 2004 (Prevelakis & Spinellis, 2007). The security and IW aspects of the mobile infrastructure will be discussed in greater detail in Chapter 5, and the simulations and calculations will be expanded to the South African situation in Chapter 7.

2.8.5 Cloud Computing

A previous version of this section was published in van Niekerk and Maharaj (2011a). A hypothetical situation using cloud computing services is used to initially validate the proposed vulnerability assessment framework in Chapter 4.

Cloud computing is "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources" (Information Systems Audit and Control Association, 2009).

The computing resources have the capability to be "rapidly provisioned and released with minimal management effort or service provider interaction" (Information Systems Audit and Control Association, 2009). The resource usage should be automatically monitored and controlled, with the ability to be "elastically provisioned" so that the client may increase or decrease usage at any time; the cloud services should be accessible from any location on various platforms, including smart mobile devices (*ibid*.).

The deployment models for cloud computing include public, private, community, and hybrid clouds. A public cloud is owned solely by the cloud service provider, and is made available to the general public or a large industry group. Multiple organisations with a shared interest may share cloud services thus forming a community cloud; it can reside on the premises of any of the organisations, or external to all of them. The management of the community cloud may be undertaken by one or more of the organisations or outsourced to a third party (Information Systems Audit and Control Association, 2009; Red Hat, 2010). A private cloud is operated for the sole purposes for a specific organisation; the management and hosting can be provided by the organisation itself, or a third party. A combination of two or more of the above cloud deployment models is known as a hybrid cloud. The two clouds remain separate entities but are bound together by a technology that is proprietary or standardised; this allows the porting of applications or data between the two clouds (Information Systems Audit and Control Association, 2009; Red Hat, 2010).

Cloud computing typically has three service models: software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). SaaS is the ability to use and access the cloud service provider's applications through an interface such as a web browser; these applications reside on the cloud infrastructure (Information Systems Audit and Control Association, 2009; Red Hat, 2010). Google Docs is an example of this. The client's control for SaaS is limited to user-specific application settings; the client does not have any control over storage, operating systems, or the underlying infrastructure (Red Hat, 2010). IaaS provides the client the ability to access and use computing resources, such as storage, processing, and networking, and allows the client to run operating systems and applications on the infrastructure. The IaaS model places the IT functions of an organisation into the hands of the service provider (Information Systems Audit and Control Association, 2009; Red Hat, 2010). Dropbox (http://www.dropbox.com) is an example of IaaS for storage. For the IaaS model, control over the operating system, applications, and storage is given to the client, but not control of the underlying cloud infrastructure (Red Hat, 2010). PaaS provides the

client the ability to deploy applications that have been either created or acquired by the client onto the cloud infrastructure through the use of tools and programming languages which are supported by the cloud service provider (Information Systems Audit and Control Association, 2009; Red Hat, 2010). The PaaS model gives the client control over the applications and possibly some control over the hosting environment configuration; as with SaaS the client does not have control over the underlying cloud infrastructure, operating system, or storage (Red Hat, 2010).

Amazon's Elastic Compute Cloud is one of the established cloud computing infrastructures; this is an example of the IaaS model, and provides scalable resources and load balancing. There are also PaaS and SaaS elements, where multiple operating systems and software applications for a web hosting, data basing, and development are available (Amazon, 2011). Microsoft's Windows Azure cloud is aimed at running and developing applications (Microsoft Corporation, 2011c); therefore this can be considered as following the PaaS model. IBM is another provider of cloud services (IBM, c. 2011), and in South Africa Teraco provides SaaS and IaaS cloud models (Teraco, 2011).

As cloud computing is a new technology there is an element of risk involved when deploying these services as part of an IT strategy. Confidentiality of information is a concern as the information is processed or stored by applications and infrastructure which the client has very little control over; the cloud service provider therefore responsible for the security and privacy of the information (Information Systems Audit and Control Association, 2009). In many cases, data from multiple clients may be stored together; if this is not controlled properly, it may result in an accidental data breach. Responsibility for maintaining the integrity of stored data (so that it is not altered accidentally or by unauthorised entities) also falls to the cloud service provider. Should a breach of the confidentiality or integrity of the data occur, there may be uncertainty regarding legal liability (Information Systems Audit and Control Association, 2009); the owner of the information is the client, however the storage and processing was outsourced to a third party (the cloud service provider). While the cloud provider is responsible for service delivery, the connectivity between the client and the provider may prove to be a weak point as it may be the subject of DoS attacks and attempts to intercept the information, and availability will also be reliant on the client's Internet service provider and the correct functioning of network gateways (*ibid*.). For those reliant on the cloud services, an outage may have severe impacts, such as when Amazon experienced outages of its cloud services in April 2011 (Brooks, 2011).

2.9 Chapter Summary

The chapter presented the background that is relevant to this study. Primarily, the models describing the IW constructs and taxonomies were discussed. Three areas of IW, namely network warfare, electronic warfare, and critical infrastructure protection, were described in more detail. The frameworks and methodologies for conducting risk and vulnerability assessments were described and discussed. The background to the information and communication technologies relevant to the study was presented; here the focus was on the mobile phone infrastructure as the primary case of the study considers that infrastructure. In some cases adaptations to models and frameworks were proposed; these will be used in Chapter 4, where the new IW and vulnerability assessment models are proposed.

Chapter 3. Methodology

3.1 Introduction

This chapter presents the research methodologies employed in conducting this study. The literature review is described and presented in Chapter 2. Multiple methodologies were employed; the data gathering and analysis methodologies are also relevant techniques for conducting vulnerability and risk assessments, as discussed in Section 2.7.1. The majority of the work for each methodology could be conducted in parallel; an advantage of this was that any potential delays in one methodological implementation did not affect other areas of research. During the study, multiple conference and journal papers were submitted; this provided a continuous feedback from the peer-review process and from the conference presentations themselves. Appendix A contains a list of publications that were generated from the research. The flow of the research is shown in Figure 3.1, and a description of the process and their relation to the objectives is provided below:

- The project was developed and designed from the initial concept, the research proposal was defended and ethical clearance was obtained.
- The primary literature review was conducted, which was an expansion of the initial literature review conducted for the research proposal. This provided the background to conduct the study.
- From the models reviewed in the literature, two new models were proposed: an IW incident model and a vulnerability assessment framework. This was an objective of the research in itself.
- A continuous literature review was conducted, which allowed for the ongoing analysis of trends and occurring incidents. This contributes to the vulnerability assessment by providing current trends in threats and provides information on possible vulnerabilities based on previous incidents.
- Interviews were conducted. The analysis of the interview responses was used to assist in designing the workshop objectives. These provided expert opinion on the criticality of the mobile infrastructure, general threat and vulnerability concerns, and specific concerns related to the mobile infrastructure and its use.
- Simulations and mathematical calculations were performed to analyse specific scenarios and expand on previous research; the simulations can visually represent the results. These are used to assess specific vulnerabilities, and contribute to the vulnerability assessment.

- The overall vulnerability assessment is based on the proposed framework, and performs the data-triangulation from the results of all the research methodologies. This is the objective of the research.
- Conclusions and recommendations are drawn from the gathered data and assessment.

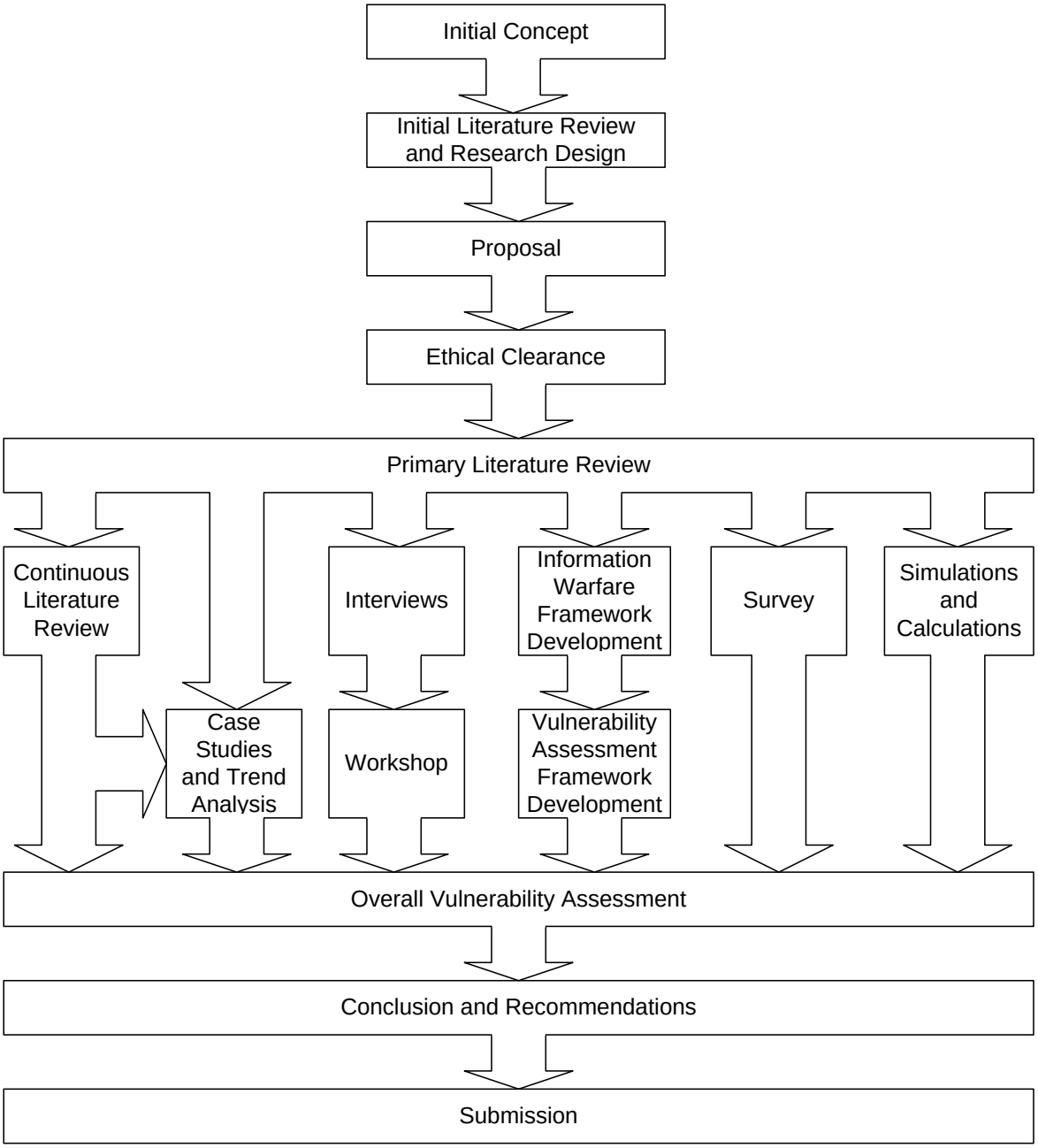


Figure 3.1: Flow of Dissertation Work

The multiple research methodologies are aimed at meeting the four primary objectives of the research study. The research methodologies described above relate to the main objectives and their breakdowns as follows:

- Further develop a framework that may be used in vulnerability assessment of critical infrastructure from an IW perspective
    - Further development of IW models and frameworks. This expands on the comparison of IW models in the literature review, and will be primarily deskwork. A new model will be proposed.
    - Assess existing frameworks. This will be primarily based on deskwork, and will be an extension of the vulnerability and risk assessment discussions from the literature review.
    - Development of new framework. This will be primarily deskwork, where the proposed IW model will be integrated into the analysis of the vulnerability and risk assessment frameworks. From this a new vulnerability assessment framework will be proposed.
- Gather data relating to attacks against information infrastructure;
    - Gather data regarding the number of attacks. Document and secondary data analysis will be conducted to assess trends in the number of and types of attacks. Data from the research workshop will also contribute.
    - Gather data regarding computer-based security incidents. Document and secondary data analysis will be conducted to assess global trends of threats and vulnerabilities with regards to computer-security incidents. The interviews and research workshop will also contribute.
    - Gather data regarding cell phone security incidents. Document and secondary data analysis will be conducted to assess global trends of threats and vulnerabilities with regards to mobile-related security incidents. The interviews and research workshop will also contribute.
- Further establish the cellular phone infrastructure as a critical information infrastructure;
    - A survey of informal enterprises using questionnaires will assess the possible economic impact from the informal sector should large-scale outages occur.

Interview results will solicit information on the perceived criticality of mobile phones on various sectors. Document analysis will also contribute.

- Apply the proposed framework to a generic cellular phone infrastructure to assess potential vulnerabilities that may be encountered;
    - The proposed vulnerability assessment framework will be used to triangulate the data collected from the various research methodologies. This will provide a generic vulnerability and risk profile for a mobile infrastructure in an IW environment.

The secondary objectives include:

- Conducting a basic vulnerability assessment on another infrastructure;
    - This will be deskwork, based on document analysis. The purpose is to provide an initial test of the proposed vulnerability assessment framework.
- Provide suggestions for solutions and considerations to improve the protection of information infrastructures, and discuss related aspects that do not fall under the vulnerability assessment;
    - This will be based on document analysis of whitepapers and vendor recommendations. Possible solutions to security issues and concerns may be suggested in the research workshop, which will contribute to this section.

Table 3.1 illustrates the applicability of the research methods to the objectives. The sections in this chapter describe the research methodologies in more detail; including the administrative processes, data gathering protocols and the data analysis methods that are employed in the study. The chapter is structured as follows: Section 3.2 describes the administrative process, particularly the defence and acceptance of the research proposal, and the ethical clearance process. Section 3.3 describes all desk-based research, which includes the trend and incident analysis, creating the proposed frameworks, computer simulations, mathematical calculations, and the application of the proposed models. Section 3.4 describes the interview process, and Section 3.5 describes the workshop. Section 3.6 describes the survey. Section 3.7 summarises and concludes the chapter.

Table 3.1: The Relationship of Research Methodology to Research Objectives

Methods / Objectives	Trend Analysis		Primary Data Collection					
	Document	Secondary Data	Interviews	Workshop	Survey	Simulations	Calculations	Other Deskwork
Further develop frameworks								✓
IW	✓							✓
Vulnerability	✓							✓
Gather Security Information	✓	✓	✓	✓		✓	✓	
Attack trends	✓	✓	✓	✓				
Security Trends	✓	✓	✓	✓				
Mobile Security Trends	✓	✓	✓	✓		✓	✓	
Establish the criticality of the mobile infrastructure	✓	✓	✓		✓			
Apply Framework								✓
2nd Vulnerability assessment	✓							✓
Recommendations	✓		✓	✓				✓

3.2 Administrative Process

This section describes the administrative process that is required by the Faculty of Management Studies at the University of KwaZulu-Natal to conduct the research study. Two major milestones are required prior to conducting the study: defending the research proposal and obtaining ethical clearance. The proposal was successfully defended and formal acceptance was received on the 5 October 2009; a copy of the acceptance letter is provided in Appendix I. Section 3.2.1 presents the ethical clearance process for this study in more detail.

3.2.1 Ethical Clearance

The ethical clearance process is to ensure the candidate understands and adheres to ethical principles while conducting the research. The form to apply for ethical clearance and the relevant documentation is submitted to the Faculty, who then approve the application and submit it to the University Ethics Committee, which provides the final ethical approval.

As part of the ethical clearance respondents for the interview process were identified and gatekeeper's letters were obtained to access them. Copies of informed consent forms, interview schedule and draft surveys need to be provided. Some of the organisations that were providing gatekeeper's letters required ethical clearance prior to providing approval; as a result provisional ethical clearance was obtained on the 12 December 2009. This was then submitted to the organisations to provide gatekeeper's approval. Final ethical clearance was obtained on the 17 May 2009. See Appendix J for copies of the ethical clearance letters.

3.3 Desk-Based Research

This section describes the desk-based research methodologies. Section 3.3.1 discusses the creation of the models and Section 3.3.2 describes the application and testing of the model and framework. Section 3.3.3 describes the methods used to conduct the trend and incident analysis, Section 3.3.4 describes the mathematical methodologies, and Section 3.3.5 describes the simulations. Section 3.3.6 describes the formulation of the recommendations.

3.3.1 Creating the Models

A primary objective of the study was to develop and propose a vulnerability assessment framework from an IW perspective. This involves the creation of two models: an IW model and the vulnerability assessment framework. The models were developed by comparing existing models (discussed in Chapter 2) and identifying common aspects; these aspects are then incorporated into a single model in order to provide a generic model that is scalable.

As IW has high-level considerations such as situational context, and technical aspects such as the actual attack and defence methods and tools, a need for a consolidated IW model and a vulnerability assessment framework from an IW perspective. Both the need for consolidated taxonomies or models for IW and the consideration of broader contexts rather in addition to the technical aspects is corroborated by Armistead (2010). The purpose of proposing the IW model is to provide a model which provides a single, consolidated description of an IW event by integrating the models that describe various aspects of IW. Existing high-level models are also considered (which are presented in Sections 4.2.1 to 4.2.5), and their common aspects incorporated into the consolidated model. Similarly, the proposed vulnerability assessment model was aimed at providing a framework which takes both high-level contextual issues and the technical issues and implementation into considerations. The majority of vulnerability and risk assessment methods presented in Section 2.7

are either too broad, or limited to the technical aspects. In addition, the existing frameworks are asset-centric rather than infrastructure-centric; the proposed model provides a single metric with which to measure the vulnerability and risk of an infrastructure or a single asset as required.

The proposed IW model is a descriptive model. This is in two parts: a high-level taxonomy adapted from the models discussed in the literature review; and an information warfare lifecycle model which is used to describe IW incidents. The vulnerability assessment incorporates techniques and common elements from existing frameworks to provide a top-down approach where the vulnerabilities and associated risks are assessed at a high-level, which flows to in-depth technical assessments. A technique for providing vulnerability and risk metrics for an entire infrastructure is proposed; this may also be used to assess the vulnerability and risk relating to specific IW areas and attack types. The information warfare lifecycle model was also used to in the development of the vulnerability assessment framework by relating IW characteristics to components of vulnerability and risk assessments. Chapter 4 presents the new models.

As the models are descriptive, it is possible to propose the models and then apply them. The test of these models will be the accuracy with which they describe the phenomena to which it is being applied. As such the models were tested by applying them to cases. For the IW Lifecycle model, it was tested by applying it to a number of IW incidents of varying type and complexity to determine the accuracy with which it described those incidents. The vulnerability assessment was applied to a cloud computing scenario to determine the accuracy with which it described the scenario. These tests are presented in Chapter 4.

3.3.2 Applying the Proposed Models

A need was identified for a consolidate model that describes IW incidents and a vulnerability assessment framework that considers both contextual and technical aspects from an IW perspective; this need is corroborated by Armistead (2010). The motivations for the proposed models are presented in more detail Section 3.3.1.

The models were initially applied to cases to determine their accuracy in describing the phenomena they are applied to. For the IW model, a series of IW incidents of varying type and complexity were used for the cases. For the vulnerability assessment framework, a cloud computing scenario was employed. These are presented in Chapter 4.

The proposed IW model is applied to the documents that describe specific incidents. The model breaks down the incident qualitatively into categories from which trends can be extracted. The

model is also used as a guide for developing the vulnerability assessment framework from an IW perspective.

The application of the proposed vulnerability assessment framework forms one of the major objectives of the research. The framework is applied to the case of a generic mobile phone infrastructure. The results from the various research methodologies are brought together in specific categories determined by this framework; this provides the overall vulnerability assessment of the mobile infrastructure. This is presented in Chapter 8.

3.3.3 Trend and Incident Analysis

A primary objective of the research is to gather information regarding IW and security incidents. This information can be gathered from analysis of documents and secondary data. Chapter 5 presents the trend and incident analysis, which contains a lot of literature; however, as the sources are primarily reports from newspapers, online news agencies, vendor notifications, and white papers, they will be considered as secondary data and documents for analysis. As such, the incidents were not included in the literature review except as examples for specific concepts. Section 3.3.3.1 discusses the document analysis methods in more detail, and Section 3.3.3.2 presents the secondary data collection and analysis.

3.3.3.1 Document Analysis

Document analysis is conducted on online news reports, threat notifications, and corporate weblog postings to identify recent IW and security incidents. The document analysis of specific incident reports illustrates the prevalence of attack types, specific vulnerabilities, and threats. By comparing the reported dates of incidents, trends over time for incident characteristics may become apparent. The proposed IW model is used to analyse these incidents (as described by the documents), and categorise the characteristics of the incident. Document analysis may also provide secondary quantitative data in addition to qualitative information. For example, security surveys generally provide quantitative data illustrating incidents numbers and categorisation; however, incident and trend descriptions are usually qualitative.

The documents were gathered from various sources. A method to semi-automate this process that was used was to subscribe to the major news groups, vendors, and security-related websites via email and social networking websites. These subscriptions then provided alerts when news reports and vendor reports were released, and provided the links to access them. Online search engines were then used to find additional reports online. Newspaper and periodical articles were also used;

should there have been a report on television, then the story was accessed on the relevant news agency's website, and online search engines were used to identify and access alternative reports. Only reports in English were considered.

For the incidents, the following information, where available, is extracted from the documents as determined by the proposed IW model:

- Context and background;
- The nature of the aggressor and target;
- The IW functional area;
- The IW tactic (denial, corruption, steal information);
- Technical aspects in terms of offensive and defensive tools and techniques;
- The outcome and impact of the incident.

Where multiple sources are available, these can be used to corroborate facts, or provide additional detail. The emphasis will be on facts; any assumptions or perceptions that are presented by the authors of the documents are indicated as such. As one of the aspects of IW is the altering of perceptions, it is important not to place too much emphasis on them; however it is still important to consider the perceptions presented in reports, as these may shape public perception and consequently reaction. Where possible, the complexity of the incidents was assessed to indicate the viability of such an attack being conducted again in the future.

The temporal occurrence of the incidents is also of interest; this provides trends in the shift between incident types, or shifts in the technologies or methods used to achieve similar objectives. General increases or decreases in incident numbers will also become evident. For this a timeline is used to illustrate the reported time period of the incident, and show clustering of incidents or incident types. Information regarding the role of information and information technologies in conflict is also extracted from documents. This allows the trends in the relevance of IW, and the impact technology evolution is having on IW.

The document analysis was aimed at extracting specific information regarding incidents, assessing the significance and viability of similar incidents occurring, and trends in incident types and the methods or technologies used.

3.3.3.2 Secondary Data

Secondary data was gathered from reports released from research organisations, vendors, and national computer emergency response teams. As with the document analysis above, subscriptions to the relevant newsletters and vendor notifications via email and social networking websites provided a method of monitoring latest developments in information security related-topics, releases of research reports and surveys, and incidents as they developed. The secondary data is re-analysed in order to identify trends or specific vulnerabilities that contributed to security incidents. This monitors the changing threat and vulnerability landscape, and can predict possible future developments.

Secondary data from national computer emergency response teams (CSIRTs) was gathered from their websites. The data is presented over time, providing for general trends in incident numbers. This data is then analysed for trends across the data sets, looking at the prevalence of specific reported incident types in a global context, as opposed to the localised context provided by the individual data sets.

Secondary data was gained from vendor reports and books; these were used to analyse trends in malware infections. The trends for computer-based malware were re-analysed by re-ranking countries according to infection rates. The infections of African nations could then be assessed in a global context and compared to the world average. The secondary data for mobile malware was fragmented; therefore the various datasets were incorporated to provide trends over a longer period of time.

In some instances, the secondary data is used only to illustrate a point; such as the penetration of mobile devices compared to other communications devices. Secondary data from a webpage was presented to illustrate the susceptibility of South African web servers to hacking. The secondary data is also used to collaborate and supplement outcomes from the qualitative document analysis.

3.3.4 Mathematical Calculations

Certain vulnerabilities can be determined by mathematical calculations. This can determine technical restrictions for certain scenarios to determine vulnerability. The calculations are done primarily for electronic warfare, to determine detection and jamming ranges for wireless communications. Network capacity limits can also be calculated. The results of the calculations determine the feasibility and restrictions of certain attacks. The equations used are identified in the literature review. Graph theory analysis of networks and infrastructure may be used to determine

critical nodes or choke points that may severely hinder network services should they be compromised. The calculations were done by writing a program in the Matlab software, and then confirming the results by hand to ensure no errors occurred. Chapter 7 contains the calculations and analysis.

3.3.5 Simulations

As with mathematical calculations, simulations can be used to analyse the impact of specific variables or scenarios. The simulations are aimed at assessing the performance of network under different loading conditions or electronic warfare performance. By investigating these characteristics of the networks, the susceptibility to certain attacks can be ascertained. The simulations provide visual representation of the results, and can be used for scenarios which are too complex to calculate by hand. The simulations are computer-based Monte-Carlo simulations, where numerous iterations of the same set-up are performed with a randomised input. The results of the iterations are averaged together to provide the final result. The specific simulation set-up is determined by the objectives and certain parameters, and will be discussed with the results and analysis of the simulations in Chapter 7.

3.3.6 Conclusions and Recommendations

The conclusions are drawn from the analysis of the gathered data, and from the outcomes of the vulnerability assessment. The recommendations follow the specific findings in the conclusion; information from the workshop and documents analysis may also provide possible recommendations. A secondary objective of the research is to provide solutions to possible vulnerable areas; these will also form part of the final recommendations.

3.4 Interviews

The interviews were to solicit opinions from experts in the field of information security, IW, and critical infrastructure protection. Both international and South African experts were approached. Expert interviews are also a valid methodology for collecting information during a vulnerability or risk assessment process, as described in Section 2.7.1. The objective of the interviews was to ascertain the perceptions of experts as to the preparedness of South Africa regarding the national critical infrastructure policies, IW concerns relating to South Africa, IW concerns regarding mobile telecommunications, and the criticality of mobile communications. The respondents were assured of

anonymity, therefore no information will be provided that can identify an individual person or an associated organisation.

It was proposed that a minimum of ten interviews should be conducted, of which at least two should be international experts. The British Educational Research Association (2006) suggests six to twelve interviews are sufficient for unstructured interviews, and should the interviews be supplementing other data sufficient respondents are required cover the range of topics in the research study. Guest, Bunce, and Johnson (2005) show that the majority (approximately 70%) of code creation in interviews occurs in the first six, then approximately another 18% in the following six. As the interviews were semi-structured and were in conjunction with additional data, the ten interviews would be sufficient to cover the topic areas and provide the required information. The international respondents were to provide an international context to the South African respondents. Twelve interviews were achieved; this is discussed in more detail below.

The experts were identified through a combination of convenience and judgement sampling. The sample was based on convenience as many were professional contacts that the candidate had made previously, and the others had contact details that were readily available to approach them. The judgement sampling was required as the candidate needed to ascertain if the prospective respondents had the relevant experience. The judgement used was based on either the publications of the prospective respondent, or the candidate's knowledge of their professional experience. All of the prospective international respondents identified have authored a book or major report. The prospective South African respondents have published at least a conference paper, or have had professional contact with the candidate.

A modified E-Delphi method was employed; the respondents had no knowledge of other respondents or their responses, and the interviews were conducted electronically. As a number of respondents were from international locations with large time differences, email was used to communicate with them; for consistency purposes, email was also used for the South African respondents (however, they were given the option of alternate contact should they wish). The E-Delphi method usually seeks to obtain consensus from respondents through iteration, where the outcomes from previous iterations are employed to solicit additional information from the respondents (Lindqvist & Nordanger, 2007). The methodology employed in this study deviates from the E-Delphi method in that consensus of responses were not required; however, reasons for responses were requested.

As per the ethical requirements for the research, as described in Section 3.2.1, consent is required from the organisations where necessary, and the individual prospective participants. Where necessary, the organisations of the prospective respondents were contacted in order to get gatekeeper's permission. The letter requesting the permission is presented in Appendix E. Receiving gatekeeper's permissions was facilitated through email. Some organisations required ethical clearance prior to providing permission; therefore provisional clearance was obtained in order to receive permission from the organisations. Due to the interviews being conducted by email, the informed consent letters were sent as attachments, and in the body of the email it was stated that response to the email indicates consent; however it would be preferred if the respondents explicitly stated their consent. The letter of informed consent is presented in Appendix F.

The interview was semi-structured, in that the questions were tailored or prioritised according to the individual respondent's area of specialty. The questions were pre-tested where the candidate's colleagues checked the questions. The interview questions were designed to meet the objectives of gathering data on the information warfare and security landscape, and establish the criticality on the mobile phone communications in this context. Table 3.2 illustrates the interview questions and their relevance to the study objectives.

A total of twenty-two requests were sent, seven to international experts and fifteen to South African experts. From this, a total of fifteen initial confirmations were received, giving an initial response rate of 68%. Five of the confirmations were from international experts and ten were from South African experts. Of these, twelve completed interviews were received; all five international experts responded, and seven South African experts responded. This is a 55% response rate from the initial requests, and an 80% response rate from the initial confirmations.

The responses to questions relating to perceptions were categorised into negative, neutral, and positive responses. Categories of very negative or very positive were added; these are for cases where the respondent added emphasis. Responses regarding concerns required a range of responses, these were categorised according to the offensive and defensive information warfare models presented in Sections 2.3.2.2 and 2.3.2.1, respectively. Responses were summarised quantitatively, in that the number of responses in each category were recorded. The Nvivo software package and Microsoft Excel were used for the coding and summarising process. For questions where a range of answers were expected, such as identifying threats, the responses were divided into pre-determined categories based on the offensive and defensive models of IW, namely integrity, availability,

confidentiality, information theft, denial, and corruption. Individual responses were then used to provide a more detailed analysis regarding the research objectives.

Table 3.2: Interview Questions Related to the Study Objectives

Questions: / Objectives:	Gather information on information security trends	Gather information on mobile-related security trends	Establish criticality of the mobile phone infrastructure
Are you aware of any critical information infrastructure protection (CIIP) efforts in South Africa?	✓		
If yes: Do you believe it is sufficient? What do you think of SA's efforts compared to those internationally? Are there any international policies that may be beneficial to South Africa?	✓		
What is the largest Information Warfare threat globally and in South Africa? (How will this affect CIIP?)	✓		
Do you think cell phones form part of the critical information infrastructure?		✓	✓
What is the biggest security threat or risk regarding cell phones, and what should or can be done about it?		✓	✓
How important do you think cell phones are for: • Large businesses • Small businesses • Military • Government • Security services • Insurgents/criminals/terrorists		✓	✓
How do you think SA's CIIP efforts are viewed internationally? (for South African respondents only)	✓		
How do the SA efforts and policies compare to those in your country? (for international respondents only)	✓		
Are there any policies in your country that may of benefit to SA, or *vice versa*? (for international respondents only)	✓		

3.5 Workshop

The workshop was aimed at soliciting information regarding information security and mobile-related security trends and concerns in South Africa. In particular, the intent was to corroborate data from the interviews and trend analysis, and to gain additional insight into the vulnerability and threat landscape in South Africa, and the impact of modern ICT technologies on these landscapes.

The prospective participants were invited based on judgement sampling; they had to reside or work in the local area where the workshop was to be held, and had to have the relevant experience or knowledge to contribute to the discussion. The prospective participants consisted primarily of professional contacts that have experience in the information security and risk fields.

The workshop was held at the Riverside Hotel, Durban, South Africa, on the 9 June 2011. This date was selected due to the number of public holidays in May 2011, and conferences in July 2011. Initially nineteen prospective participants were invited; two suggested they be replaced by another person. These persons were invited, giving a total of 21 invitations to participate. Five responded that they were unable to attend, seven did not respond, seven accepted the invitation, and the two remaining suggested their replacements. There were a total of nine people present at the workshop; seven participants, the candidate, and the candidate's supervisor. Multiple recordings were made of the discussions for redundancy. Prior to beginning the discussions, the recording mechanisms and procedure was explained to the participants.

The output of the workshop consists of the topics discussed and focussed on (due to conversational flow), and the agreements and conclusions reached by the participants based on their discussions. The importance of the various topics was inferred from the amount of time focussed on that topic. Information on specific trends may be gained from specific statements from the participants, or their general agreement on these trends. The participants also discussed and proposed solutions to issues raised; these are incorporated into the recommendations arising from the study.

3.6 Survey

The objective of the survey was to assess possible economic impacts of due to the effect of major outages of mobile services on the informal business sector; this contributes to establishing the criticality of the mobile infrastructure. The questionnaire assessed the perceptions of the informal traders as to their reliance on mobile communications for business and the financial usage regarding mobile communications.

The nature of the survey questions was pre-tested by colleagues; the questions were projected onto a screen, and the suitability and phrasing of the questions were discussed. During this process possible wording of the questions to make them suitable for translation into languages other than English (namely Zulu and Xhosa) were assessed. The questionnaire is presented in Appendix G, and the letter of informed consent is presented in Appendix H.

The survey was piloted in central Durban and the surrounding suburbs. For the pilot in the informal markets, the Warwick Project Office, which forms part of the city's urban renewal project, provided a guide who selected respondents and acted as interpreter where required. A total of eight pilot responses were obtained from nine respondents; one did not wish to participate in the survey. The results of the pilot are discussed in Chapter 6. The survey of the informal traders was not completed for two reasons:

- The research is a project on its own, and a more in-depth study is required than what would be done as part of this dissertation; and
- The survey was not essential to the overall outcome of the dissertation, and as per the proposal acceptance letter, it was decided to discontinue this avenue to focus on more promising aspects.

3.7 Chapter Summary

The chapter presented the research methods employed in this study. From the literature review, a new IW model and vulnerability assessment framework is proposed. Secondary data and document analysis will be conducted to analyse trends and incidents; the proposed IW model will be used to analyse incidents described by documents. This will gain information on trends of threats, vulnerabilities, and incidents related to the information and mobile infrastructures. Primary data is to be gathered through expert interviews, a workshop, and a survey. These provide perspectives and experience regarding threats, vulnerabilities, and criticality of the information and mobile infrastructures. The full survey was not completed due to the proposal acceptance requiring confinement of the study to the most promising aspects. Simulations and mathematical calculations and analysis will be conducted to assess the feasibility of certain attack methods. The information is triangulated through the implementation of the proposed vulnerability assessment; from this conclusions can be drawn regarding the vulnerability of the mobile infrastructure.

Chapter 4. New Models

4.1 Introduction

This chapter presents the new models for IW and an infrastructure vulnerability and risk assessment. Section 4.2 presents the new IW model; which will be used for incident analysis in this chapter and Chapter 5, and will be used to further relate IW to the vulnerability and risk analysis framework, which is presented in Section 4.3. Chapter 5 to Chapter 7 will contain the analysis of a mobile phone infrastructure as prescribed by the infrastructure vulnerability framework, and the overall assessment will be provided in Chapter 8. Section 4.4 concludes the chapter.

4.2 Information Warfare Model

This section presents the new model for IW. Armistead (2010, p. 109) claims that the "lack of standardised nomenclature or taxonomy" hinders the ability to conduct information operations; this can be considered to apply to IW. The purpose of proposing this model is to provide a single consolidated model and framework that brings together and relates the various models for IW; the models presented in Sections 4.2.1 to 4.2.5 are derived from those discussed in Chapter 2, by comparing the existing models and combining their common aspects. The generation of the IW model falls into one of the main objectives of the dissertation. Section 4.2.1 proposes a definition for IW, and Section 4.2.2 presents the model describing the relationships between information, data, and knowledge. The consolidated domains are defined in Section 4.2.3, and the model mapping the SANDF IW construct to the spheres of IW is presented in Section 4.2.4. The offensive and defensive IW model is presented in Section 4.2.5. Section 4.2.6 presents the IW Lifecycle Model, which brings together various IW models and frameworks to be able to describe an IW event. This model will be used for incident analysis in Chapter 5, and will be used as a basis for developing the infrastructure vulnerability and risk analysis frameworks from the specific IW viewpoint, which is presented in Section 4.3. Examples of the application of the IW Lifecycle Model are presented in Section 4.2.7.

4.2.1 Information Warfare Definition

From the discussion in Section 2.3.1 the following definition is proposed:

Information warfare is those actions taken to attack, protect, or exploit information and its supporting systems and processes in the physical, information, and cognitive domains in order to achieve tactical, operational, and/or strategic objectives.

4.2.2 Extended Model for Information Relationships

Following the discussion in Section 2.2, a model describing the relationships between different relationship types and the influences of external factors was proposed. This is shown in Figure 4.1. Data can be considered as raw descriptors of an object or event. Data is processed into information; the processing may be subjected to bias introduced by experience, perception, and external influences. The information is understood to form knowledge; this process may also be influenced by external factors and *a priori* knowledge in the form of experience and perception. Knowledge applied is wisdom. An adaptation to this is data is the raw bits and bytes, which is subject to external noise, and is processed by a system to form information that is readable by humans. This is understood to form knowledge; wisdom is the application of this knowledge.

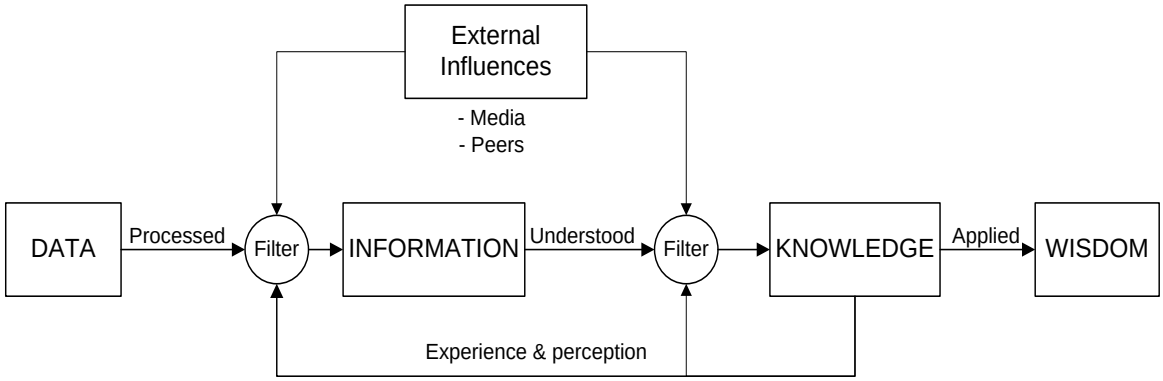


Figure 4.1: The Extended Model for Information Relationships

4.2.3 Information Warfare Domains

Following the discussion in Section 2.3.3, the following domains and sub-domains are proposed:

- Physical (real-world)
    - Hardware
    - Physical person
    - Physical networks
- Information (virtual-world)
    - Processes
    - Software

- Data
- Logical networks

- Cognitive
  - Perception
  - Understanding
  - Will

4.2.4 Information Warfare Constructs and Spheres

Following the discussion in Section 2.3.3, the following model mapping the IW construct of the SANDF to the spheres of IW is proposed. Figure 4.2 shows this model. The enabling domain consists of the IW functional areas that may be used to conduct or impact on the application domain. The application domain creates affects in the various spheres of IW.

Figure 4.2: The Relationship between the IW Functional Areas and IW Spheres

4.2.5 An Offensive and Defensive Information Warfare Model

Following the discussion in Section 2.3.2, the consolidated model describing defensive and offensive IW tactics is presented in Table 4.1.

Table 4.1: The Information Warfare Taxonomy

Offence	Defence	Control Mechanisms
Disrupt Degrade Deny Destroy	**Availability** Utility Timeliness	Restoration Redundancy Access control Authentication
Exploit Steal Compromise	**Confidentiality** Possession Control	Access control Authentication
Corrupt Fabricate Modify Change context Change perceptions	**Integrity** Authenticity Relevancy Accuracy	Non-repudiation Authentication Access control

4.2.6 Information Warfare Lifecycle Model

This section presents the Information Warfare Lifecycle Model; the model was originally proposed in van Niekerk and Maharaj (2011d); and was used to analyse the role of ICTs in the Tunisian and Egyptian unrest in van Niekerk, Pillay and Maharaj (2011). This model was generated by combining the common aspects of multiple models that were presented in Chapter 2:

- Message Flow Model for PSYOPs (Section 2.3.3.7)
- Network Warfare proposed by Veerasamy and Eloff (Section 2.4.4)
- Wik (Section 2.3.5)
- Ventre (Section 2.3.5)

The objective is to generate a consolidated model that can adequately describe IW incidents through a combination of high-level and detailed concepts; yet is scalable to accommodate incidents of differing magnitude. The objective was also for the model to be applicable to the various functional areas of IW which may be distinct from each other, for example electronic warfare and PSYOPs. The reason for generating this model is that the existing models are either high-level, or are specific to a functional area of IW. Therefore a more general model is required, with sufficient detail, which can be related to the vulnerability assessment models.

From the four figures, there are common aspects describing IW:

- There is a context, which includes:
    - An aggressor;
    - Some motivation for the aggressor to attack, or an objective to achieve; and
    - A defender.
- Planning is required, which needs to account for:
    - Operational restrictions for political, legal, ethical, or financial reasons;
    - Technical and human capabilities; and
    - Other considerations, such as social impact.
- The attack occurs:
    - Specific target set(s) are focussed on, using
    - Offensive tactics and tools, according to
    - The IW functional area(s).

- The target defends against the attack, by:
    - Protecting the CIA attributes of information and its systems, through the use of
    - Defensive tactics and technical countermeasures.
- The offensive and defensive operations result in an impact on society in general; who
- React and respond to the incident; which affects the context.

Many detailed models and high-level concepts may overlap; for example the planning of operations will be relevant to the context, attack, and defence. For this reason, a two-layered model was generated, with a detailed layer overlapping a high-level layer. The high-level layer contains the following blocks: context, attack, defence, consequences, reactions, recovery, and influence. The planning block of the detailed layer overlaps the context, attack, and defend and protect blocks of the high-level layer. The attack block contains the target set, functional areas, offensive tactics, and offensive weapons of the detailed layer. The defend and protect block similarly contains the defensive tactics, defensive weapons, and defensive attributes of the detailed layer. The society block is relevant to four high-level blocks: attack, defend and protect, consequences, and recovery. The human block is relevant to the consequences and reaction blocks. The reaction of the humans provides the feedback which ultimately influences the context. The IW Lifecycle Model is shown in Figure 4.3.

Armistead (2010) shows that there is a view that there is still a divide between the technical issues of IW and the broader context that governs these issues. As such, the context, planning, and consideration blocks from Ventre, Wik, and Veerasamy and Eloff are retained through the high-level context and detailed plan information operations/warfare blocks in the proposed IW Lifecycle model. This relates the broader context, planning issues, the technical implementation, and the consequences of IW actions.

4.2.7 Application of the IW Lifecycle Model

The application of the IW model to recent and historical cases of IW incidents is illustrated in this section. The purpose is to provide a basic 'proof of concept' evaluation of the model. Sections 4.2.7.1 to 4.2.7.6 each focus on a specific incident, each of which falls into a different functional area of IW. A brief background of the incident will be provided prior to applying the model.

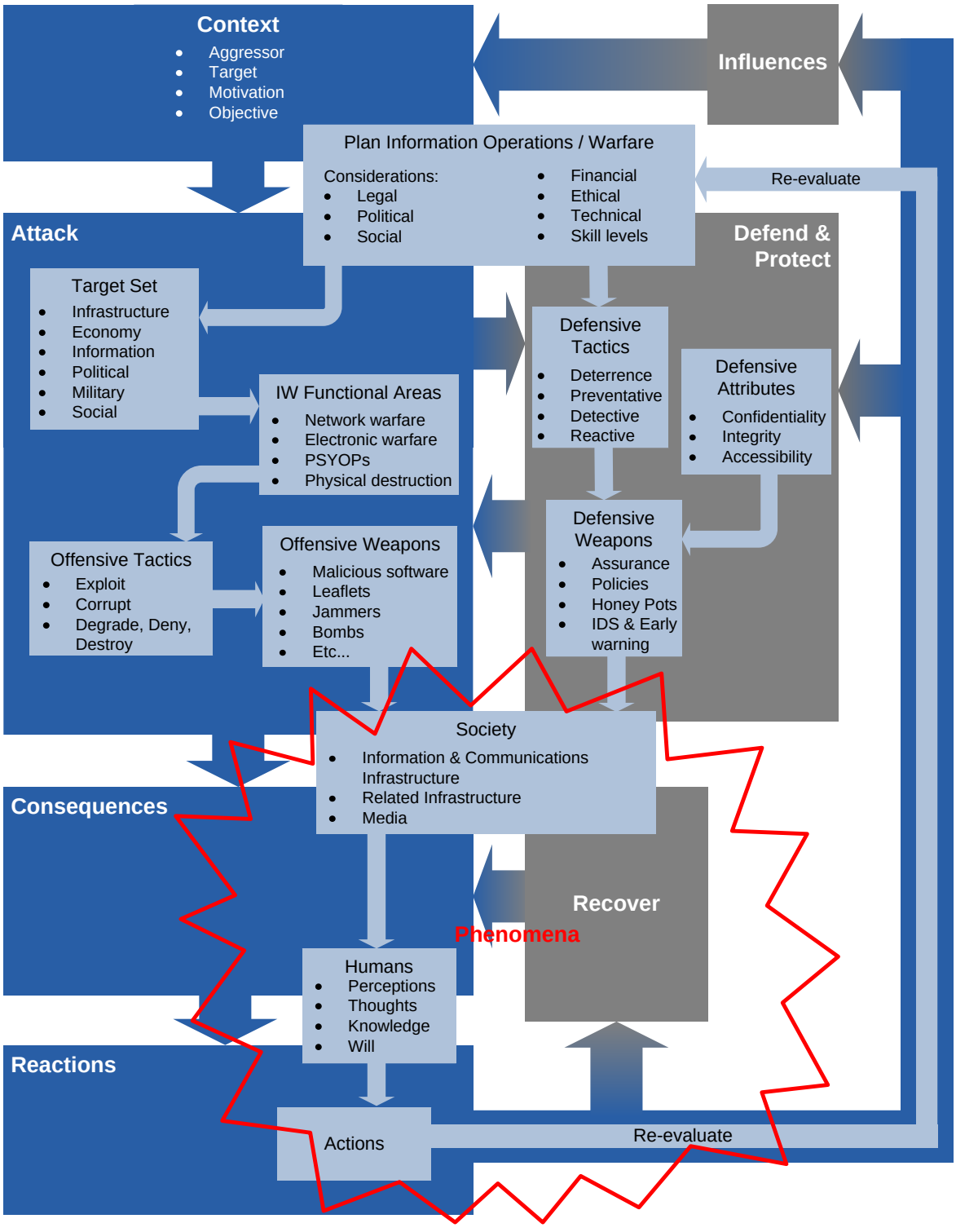


Figure 4.3: The IW Lifecycle Model, van Niekerk and Maharaj (2011); van Niekerk, Pillay, and Maharaj (2011)

4.2.7.1 Estonia: Cyber-based Attack on Infrastructure

Many ethnic Russians were offended when the Estonian government decided to relocate a war memorial which also honoured Russian troops from the Second World War; initially there were street riots during which the Estonian embassy was attacked (Germain, 2008; Rolski, 2007). The DDoS attack via Botnets was first apparent on the 26 and 27 April 2007, and after a few days access to the websites of some newspapers were blocked (Landler & Markoff, 2007). The Russian government denied claims that it was responsible for or aiding the attacks (Germain, 2008; Landler & Markoff, 2007; Rolski, 2007). Initial defensive measures were aided by ISPs who blocked the attack-related traffic. Additional preparations began due to an expected onslaught prior to a public holiday celebrating the Soviet victory in the Second World War; the attack occurred on the 9 and 10 May, where government websites and email systems were severely affected. The major bank was also forced to close its online services resulting in over $1 million in losses (Landler & Markoff, 2007). The worst of the attacks had subsided by the 16 May (Rolski, 2007). This incident resulted in NATO expanding the treaty to include cyber-attacks, and a cyber-defence centre was established in the Estonian capital (StrategyPage.com, 2010c).

The IW Lifecycle analysis of the incident is as follows:

- *Context:*
    - Aggressor(s): Ethnic Russians;
    - Target: Estonian Government;
    - Motivation: Revenge for relocating a war memorial, and to show political dissatisfaction.
- *Attack:*
    - Functional area(s): Network warfare and some psychological warfare employed through network warfare by defacing government websites.
    - Target set: Websites and network communications.
    - Tactic: Primarily DoS; some influence on perception.
    - Weapon: Botnets were used to flood target websites with traffic.
- *Defence*: The initial defence by the Estonians was preventative; aid was requested from international ISPs to block the traffic that was related to the DoS attack.
- *Consequences*: The initial attacks had a minor impact; a few websites of newspapers were inaccessible. As the attacks continued the disruption was more severe, and the main Estonian Bank's online services suffered losses exceeding $1 million.

- *Reaction*: Defensive preparations were increased after the initial attacks. A cyber-protection centre was established after the incident.
- *Influence of context*: The initial context was only minimally influenced; there was some increase in political tensions after Russia was accused being or aiding the perpetrators. A subsequent global impact has been that several nations have included cyber-attacks by expanding existing war treaties.

4.2.7.2 The Channel Dash: Electronic Warfare Operations

Radloff, quoted by Sikwane (2010), described the German electronic warfare operations during World War Two, which are summarised in this section. Three German capital warships and their accompanying destroyers were ordered to return to Germany from France in 1942, necessitating a transit of the English Channel; to protect the warships from detection, German forces simulated interference from atmospheric disturbances on the British coastal radar stations by incrementally increasing noise jamming on the radar stations. The aim was to have the British operators reduce the gain of their radar, further decreasing their ability to detect the warships. The operators fell for the deception, which allowed the warships to transit the English Channel virtually undetected; the warships were out of range by the time the deception was detected.

The IW Lifecycle analysis of the incident is as follows:

- *Context*:
    - Aggressor: German electronic warfare units.
    - Target: English radar stations.
    - Motivation: Disrupt the radar stations to provide cover for warships transiting the English Channel.
    - Restrictions and limitations: As this was a time of war, there was very little in terms of restrictions that could possibly effect planning, other than technical capability.
- *Attack*:
    - Functional area: Electronic warfare.
    - Target set: Military radar sensors.
    - Tactics: Denial in that the functionality of the radar stations was degraded, and deception in that the jamming simulated atmospheric interference, which was aimed at having the radar operators further reduce the capability of the radar stations.
    - Weapons: Jamming equipment.

- *Defence:* The radar operators were deceived and no effective defence conducted.
- *Consequence*: In order to mitigate the effects of the interference, the English radar operators reduced the gain on the radar units; this enabled the German warships to transit the English Channel without being detected.
- *Recovery and Reaction*: The British realised there was deception and returned the radars to their normal operating conditions, however it was too late to intercept the warships.
- *Influence on Context*: The Germans successfully completed their objective.

4.2.7.3 Somalia / Blackhawk Down – PSYOPs

United Nations (UN) forces supplying aid in Somalia were being raided by the local militias; the US deployed a contingent to assist the UN. The US forces targeted a specific warlord, Mohammed Farah Aidid, in an attempt to halt the attacks on the convoys; a series of raids were conducted, during which the infamous Black Hawk Down incident occurred. During the skirmish, five US servicemen were killed and another captured (Adams, 1998). In order to force a US withdrawal from Somalia, the bodies of the US servicemen were dragged in front of CNN cameras. When these images were broadcast, the shock and the public outrage pressured the US government into leaving Somalia after rescuing the captured serviceman (Adams, 1998; Taylor, 2002). This type of psychological attack found both the US public and government completely unprepared; negative media towards the US government, policies, and military command continued after this incident and the subsequent withdrawal (Adams, 1998).

The IW Lifecycle analysis of the incident is as follows:

- *Context:*
    - Aggressor: The Somali warlord, Mohammed Farah Aidid
    - Target: The US public
    - Motivation: To drive the US forces out of Somalia
- *Attack:*
    - Functional area: PSYOPs
    - Target set: Public opinion.
    - Tactic: Affect the will and perception of the US population.
    - Weapon: International mass media. United States servicemen had been involved in a skirmish infamously known as the Black Hawk Down incident. The bodies of those killed in the skirmish were dragged in front of CNN cameras to psychologically shock

the US public. The planning was to affect the morale, will, and society of the US public.

- *Defence*: This attack was a surprise, consequently no defensive measures were taken; very little could be done after the images were released. A reactive defensive measure was conducted by rescuing hostages and withdrawing due to public opinion.
- *Consequences and reaction*: As was planned, the US public were shocked by the images; public opinion pressured the US government to cease operations in Somalia. The negative public reaction and media continued after the US withdrawal.
- *Influence on Context*: The US forces were forced to withdraw due to the strategic use of the international mass media; the political context in the US was altered, and the situation in Somalia was change as the Somali warlord intended.

4.2.7.4 The Wikileaks Incidents – Cyber-based Conflict and Intelligence Warfare

This case study comprises of a number of sub-incidents, making it the most complex of those considered. The initial incidents comprised of four releases of leaked documents; the eventual retaliation to this resulted in a series cyber-attacks and counterattacks. The releases of the documents can be attributed to intelligence warfare in that potentially sensitive information on coalition activities were made public; as were some of the operations of Wikileaks (Gilligan, 2010). The cyber-attacks can be seen as exhibiting an action-reaction cycle which may indicate how an actual cyber-war between nation states would occur.

The Wikileaks releases made the information of US and coalition military and diplomatic activities available online for public consumption throughout 2010; the initial response was condemnation and an investigation into the original leak (Poulsen & Zetter, 2010). The releases appeared to be publicised by media partners of Wikileaks. The release of diplomatic cables resulted in a stronger retaliation, where Wikileaks was targeted directly and setting of counter-attacks; a chronology of the incident is presented here:

- April 2010: A video was released showing journalists being fired on by a helicopter gunship (Bronstein, 2010); the accuracy of some claims regarding the video were questioned (StrategyPage.com, 2010b).
- June 2010: A US intelligence analyst was arrested after the investigation; he appears to be the source of all leaked documents (Poulsen & Zetter, 2010).
- July 2010: Wikileaks releases war logs from Afghanistan (Poulsen, 2010).

- October 2010: Wikileaks releases war logs from Iraq (Stewart, 2010).
- 29 November 2010: Wikileaks releases diplomatic cables and information on US cyber-intelligence; this results in a DDoS attack against the Wikileaks website by a pro-US hacker (Goodwins, 2010).
- Due to US pressure, Paypal, Visa, Mastercard, Amazon, and Swiss bank Post Finance block Wikileaks accounts; and the Wikileaks website is removed from the Internet domain registry (Walker, 2010). The IP address and content is made available on various websites supporting Wikileaks. Queries regarding the finances of Wikileaks are raised, and rape allegations against its founder re-surface (Gilligan, 2010).
- 4 December 2010: The hacker group Anonymous conduct a DDoS attack against the PayPal blog in support of Wikileaks (Walker, 2010).
- 6 December 2010: Anonymous attacks the main websites of Post Finance and PayPal; a pro-US hacker counterattacks Anonymous (*ibid*.).
- 7 December 2010: EveryDNS (who delisted Wikileaks), a US Senate website, Post Finance, the prosecutors of Julian Assange and the rape accuser lawyers are all targeted by Anonymous; who experiences another counter-attack (*ibid*.).
- 8 December 2010: The attack on the lawyers continues; Mastercard, Visa, and PayPal are targeted. Twitter disables the Anonymous profile (*ibid*.).
- 9 December 2010: PayPal continues to be targeted and Amazon is attacked by Anonymous; the counterattacks against Anonymous also continue (*ibid*.).

The first iteration of the IW Lifecycle Model is as follows:

- *Initial Context*: Wikileaks and apparently disillusioned US intelligence analyst may have been motivated to discredit the US, but claimed to be promoting transparency.
- *Planning*: The intelligence analyst had access to the relevant documents; Wikileaks had the technical capability to release the information globally. The possible ethical and legal ramifications did not deter either party.
- *Attack*: Authorised access to a sensitive intelligence network was leveraged; Wikileaks then released these documents. Confidentiality of the information was breached in what appears to be pseudo intelligence warfare and potential PSYOPs (assuming the motivation was to discredit the US).

- *Defence and reaction*: Initially the response was reactive by publicly condemning the releases; the alleged original source of the leak was arrested after an investigation. The reaction and defence due to the release of the diplomatic cables was stronger; multiple financial institutions were pressured into closing Wikileaks accounts, and the website was delisted. This appears to be preventative; in that the delisting reduces the availability of the information to the public, and the blocking of the accounts hinders Wikileaks operations by removing finances. A DDoS attack against the Wikileaks website was also conducted by a pro-US hacker.
- *Consequences and influence*: The international public opinion and support was divided; political tension increased, and vigilante groups became more active.

The second iteration of the IW Lifecycle Model is as follows:

- *Altered context*: Support and international public opinion is divided after Wikileaks has released a number of potentially sensitive documents; the alleged source has been arrested and the releases publicly condemned.
- *Attack*: Diplomatic pressure was applied by the US to remove financial support from Wikileaks; their website is also delisted. A vigilante has targeted Wikileaks with a DDoS attack. This is the reaction from the first iteration.
- *Defence and reaction*: The IP address of the Wikileaks website was made available to allow access; other websites began hosting the content to support Wikileaks. The group Anonymous began targeting those organisations that withdrew support from Wikileaks.
- *Consequences and influence on context*: US diplomatic pressure further polarised international opinion, and a pro-Wikileaks vigilante group began targeting institutions who withdrew support from Wikileaks.

The third iteration of the IW Lifecycle Model is as follows:

- *Altered context*: The international community has been further polarised by US diplomatic pressure against Wikileaks, and additional opposing vigilant groups are conducting DDoS attacks.
- *Attack*: Anonymous conducts DDoS attacks (network warfare) against financial institutions and other websites who supported the US.
- *Defence*: The DDoS attacks by Anonymous appear to have been ignored by the victims in that there was no major reaction. Continued pressure resulted in Twitter removing the Anonymous account.

- *Reaction*: Pro-US hackers counter-attacked Anonymous.
- *Consequences and influence on context*: Frustration with Anonymous due to the inability to access websites probably reduced support for them. DDoS attacks and counter-attacks continued between pro-Wikileaks and pro-US hackers.

4.2.7.5 Revenge Attack against Infrastructure

This section analyses an attack on an Australian sewerage plant by a disgruntled former contractor. This section was not previously published. Over a two-month period in 2000, 800 000 litres of sewerage was released into the public waterways of Maroochy, Australia (Abrams & Weiss, 2008; Wyld, 2004). The perpetrator was Vitek Boden, who was an ex-employee of a company that installed the wireless-controlled sewerage systems that the plant used; he had recently left his job due to differences, and then had his job application turned down by the city council. In an attempt to force the council to hire him, or just for revenge, he used stolen equipment to access the control systems from his car, releasing the sewerage into the waterways (Abrams & Weiss, 2008; Wyld, 2004). This resulted in ecological damage and an unpleasant odour in the surrounding areas. The irregularities at the sewerage plant were investigated, and the controller addressing was altered in an attempt to protect against the attack, however Boden was still able to continue his attack (Abrams & Weiss, 2008). He was caught accidentally after the equipment was found in his car when he was stopped for a traffic violation; as compensation, he was ordered to cover the costs of the cleaning operation in addition to being sentenced to two years imprisonment (Wyld, 2004).

The IW Lifecycle analysis of the incident is as follows:

- *Context*:
    - Aggressor: A disgruntled ex-employee.
    - Motivation: Revenge for a work-related incident regarding his employment, and an attempt to secure employment.
    - Target: The sewerage works in Australia.
- *Attack*:
    - Functional area: Infrastructure warfare.
    - Target set: Infrastructure controllers.
    - Tactic: Corrupt system integrity and malicious control.
    - Weapons: Insider knowledge and stolen equipment.

- *Planning*: Using the stolen equipment, access was gained to the systems; the objective was to release sewerage in an attempt to force being hired to solve the problem. He had the insider knowledge and technical expertise to conduct the attack. The legal and social consequences may have deterred other individuals; however this did not prevent the aggressor.
- *Defence*: The attacks could not be stopped initially; after investigating the problem, the control addressing was adjusted, which temporarily halted the attacks. Boden was later arrested for unrelated activity, which led to the stolen equipment being found.
- *Consequences*: The consequences were primarily physical; the area was polluted and the residents were affected by the unpleasant smell.
- *Recovery*: The perpetrator was ordered to finance the cleanup, and upon his arrest the attacks stopped.
- *Influence of context*: The attack ultimately failed, and the perpetrator was prevented from repeating the attacks.

4.2.7.6 The Tunisian and Egyptian Political Unrest: PSYOPs and Command and Control Warfare in Social Uprisings

This section analyses the social uprisings in Tunisia and Egypt from an IW perspective using the Lifecycle Model. A previous version was published in van Niekerk, Pillay, and Maharaj (2011), and was part of the candidate's contribution to the publication. The national uprising in Tunisia was instigated by unemployed university graduates, and fuelled by discontent on online political dialogue due to two decades of government misrule in late 2010 (Bay, 2011). Diplomatic cables leaked by Wikileaks, some of which outlined the extravagant lifestyle of the Tunisian presidential family, may also have contributed to fuelling the uprising (Kirkpatrick, 2011). The Jasmine revolution began in December, and first gained global prominence in January 2011, just prior to the Tunisian President Ben Ali resigning and fleeing the country (Bay, 2011). Demonstrators documented the protests by video, which were distributed via online social media and mobile phones to promote their cause; these tools were also employed to coordinate the protest actions (Bay, 2011; Kirkpatrick, 2011). The traditional broadcast mass media also contributed to disseminating the protestors' message; Al Jazeera covered the entire period of protests, and Western media began coverage in January 2011 (Kirkpatrick, 2011). The apparent success of the Tunisian demonstrations inspired massive anti-government protests in Egypt, which began less than two weeks after the resignation of the Tunisian government; as with Tunisia, the Egyptian protests were fuelled by increasing prices, poverty, high unemployment, and the extended rule of President

Mubarak's government (Hendawi, 2011). Mobile phones and online social media again appeared to be crucial to the organisation of the demonstrations (Hendawi, 2011). Many of the signs held by the protestors were in English; this indicates an intention of targeting the international community. The fact that a number of national leaders urged then President Mubarak to resign (Lee, 2011; Lekic, 2011; Robinson, 2011) indicates that the protestors successfully influenced the behaviour of the international community.

Both sets of demonstrations were reported to be using social media for both coordination of the protests, and advertise the protestor's plight (Kessler, 2011). Both governments targeted the social media in an effort to curb the protests: Madrigal (2011) reported that the Tunisian authorities attempted to hack into and delete the social media profiles of the primary instigators of the demonstrations. The Egyptian government shut down both mobile and Internet services (Kessler, 2011; Kravets, 2011). Both these efforts were unsuccessful; as the social media allowed the protests to gain momentum; once this critical mass was achieved, the role of the social media appears to have diminished. These uprisings have resulted in subsequent upheaval in North Africa and the Middle East: Yemen, Bahrain, Jordan, Syria, Iran, and Libya all experienced anti-government protests (Black & Chulov, 2011; Sky News, 2011).

The IW Lifecycle analysis of the incident is as follows:

- *Context*:
    - Aggressor: The general population of the nations.
    - Target: The respective governments of the nations.
    - Motivations: Bring attention the dissatisfaction of the population and force the resignation of the governments that were perceived as corrupt and oppressive through internal and international pressure.
- *Planning*: Online social media spread resulted in coordination of the dissatisfied population. Possible harsh government reprisals may have prevented some from participating, however many joined the uprisings.
- *Attack*:
    - Target set: International public opinion, the will of the national governments, and the socio-political constructs of the countries.
    - Functional area: PSYOPs and command and control.
    - Tactics: Coordinate mass demonstrations and influence or corrupt international opinion to pressure the will of the national governments into resigning.

- Weapons: Online social media, mobile devices, the international mass media, and the mass protests themselves.

- *Defence*: The governments attempted to prevent the use of the online social media and mobile platforms to disrupt the organisation of the protests; this again indicates a form of command and control warfare.
- *Consequences and Phenomena*: The protests gained momentum, and the international community was influenced against the respective governments. Protests have subsequently spread throughout the North Africa and Middle East region. Social media and mobile phones have been established as tools for popular uprisings.

4.2.7.7 The Lifecycle Model Summary

The IW Lifecycle Model proposed in Section 4.2.6 was tested by applying it to six incidents; each incident corresponds to an IW functional area, and they are of different magnitude. The background to the incidents was provided from documents; this was then analysed using the model. The proposed model was capable of describing each of the incidents, even though they were associated with different IW functional areas. Large incidents were accommodated with multiple iterations of the cycle. The model therefore meets the objectives of being independent of the IW functional area, and scalable; it was also able to provide detailed information in addition to the high-level cycle.

4.3 Infrastructure Vulnerability and Risk Assessment Framework

This section presents the proposed vulnerability assessment framework. Common and important aspects of the vulnerability and risk assessment frameworks presented in Section 2.7 are incorporated into the consolidated framework; this framework is then linked to IW through the IW model proposed in Section 4.2. The proposal of this framework is a primary objective of the study; the data presented in subsequent chapters will be consolidated and triangulated in Chapter 8 through the use of this framework. The initial framework concept which was presented in the study proposal also guided the data gathering. A previous version of this section was presented in van Niekerk and Maharaj (2011a). Section 4.3.1 presents the proposed framework, and Section 4.3.2 presents an example of its implementation.

4.3.1 Infrastructure Vulnerability Framework

From Section 2.7, it can be seen that many frameworks are high-level, and give little attention to detailed implementation, and are asset or organisation orientated rather than infrastructure

orientated. Most consider general risk, or information risk; only the Minimum Essential Information Infrastructure framework is dedicated to an IW scenario. However, this framework focuses on the technical issues, and not the political, legal, social, or ethical considerations. The intent therefore is to propose a model that is scalable and adaptable, which is layered and guides the user from the high-level to the detailed implementation. It is also intended to be related to cases of IW. The outcome of the framework is to be a single metric or figure for the vulnerability and risk of the infrastructure. Multiple metrics can be used (one each for different perspectives, threats, or other considerations) to compare possible scenarios.

The following risk and vulnerability frameworks and methods will be considered:

- SWOT (Section 2.7.1.8);
- PESTEL (Section 2.7.1.7);
- MEII (Section 2.7.2.1);
- FAIR (Section 2.7.2.4); and,
- TVA Worksheet (Section 2.7.1.9).

The SWOT analysis is a high-level; for an IW situation, the weaknesses can be considered analogous to the vulnerabilities, and strengths can be considered as analogous to the controls, legislation, and policies that are in place, which will mitigate an attack. Threats are the IW threats, and opportunities may be considered as measures that may be improved or introduced to increase the controls or strengths. An addition needs to made, in that the potential impact of an incident needs to be assessed.

For PESTEL, the political, legal, social, and economic considerations may overlap; these can all be grouped into non-technical factors. The technical considerations remain as is, and the ecological considerations can largely be ignored in an IW situation, except where there are possible ecological effects, such as in Section 4.2.7.5. This will fall under the impact assessment, and may be assessed through environmental impact assessments.

For the proposed framework, the highest level of layers will be the modified SWOT analysis as described above, incorporating threats, vulnerabilities, countermeasures, and opportunities. For each of these, the next layer will be the modified PESTEL with two sections: technical; and non-technical, which incorporates the political, economic, social, and legal considerations. This is shown in Table 4.2. A variety of methods may be used for the next layers: two levels of analysis are provided for. Techniques and sources of information may include vendor and national threat

advisories, white papers, political and legal analysis methods, war gaming, and what-if scenario analysis. Information may also be gained from business and national intelligence, Monte-Carlo computer simulations, and expert input through workshops and interviews.

For the technical vulnerabilities, the categorisation of the MEII process may be used to further segment the analysis; this will correspond to Analysis Method 1 in the figure. Methods may be used to assess each category (this will correspond to Analysis Method 2). For example, electronic accessibility may be assessed though penetration testing; singularities and centralisation may be tested by the use of graph theory, and computer simulations may test operating conditions and loading effects. Many technical threats and vulnerabilities may also be determined from CERT or CSIRT advisories and vendor reports; major incidents may be identified through the news media.

For each of the modified SWOT elements, certain variables need to be rated for the IW situation. The non-technical threat (Step 1A in Table 4.2) is related to the context; who a potential aggressor could be, their capabilities, and the likelihood that they will conduct some form of attack. The technical threats (Step 1B) will the likelihood of the technical attack (certain attack methodologies are more common than others – this will be discussed in Chapter 5) and the complexity of conducting the attack. The vulnerability phase (Step 2) consists of identifying the potential vulnerabilities that are to be rated and prioritised in the assessment. Non-technical vulnerabilities (Step 2A) can be associated with both the context and limitations in the planning phase of the IW Lifecycle Model; for instance insufficient legal frameworks, political segregation, or economic dependence may make a nation susceptible to an IW attack. Technical vulnerabilities (Step 2B) can be identified through assessing the categories of the MEII process through the use of various techniques; examples of these are provided in the Analysis Method 2 column of Table 4.2. When a potential vulnerability is identified, the complexity or effort a threat would need to expend in exploiting it should be rated.

The countermeasures and defences (Step 3) may be determined whilst identifying the vulnerabilities; the strength of the controls in place need to be rated; the non-technical factors (Step 3A) will need to be estimated according to available information. The strength of the technical countermeasures (Step 3B) may be determined from datasheets, product specifications, vendor whitepapers and reports, and simulations. For example, a report may rate anti-virus applications according to the success rate of detecting and removing malware; this can then be used to rate the strength of the anti-virus application as a control against malware.

Table 4.2: The Proposed Infrastructure Vulnerability Assessment Framework, van Niekerk and Maharaj (2011a)

SWOT	PESTEL		Analysis Method 1	Analysis Method 2
Step 1. Threats	1A. Non-technical	Social	National & international threat advisories, and reports Business intelligence News Media Trend Analysis	Expert input What-if Analysis Scenario Analysis Employee satisfaction analysis
		Economic		
		Political		
		Legal		
	1B. Technical		CSIRT advisories Business intelligence Vendor advisories	Expert input
Step 2. Vulnerabilities, (Weaknesses)	2A. Non-technical	Social	Business intelligence National & international threat advisories and reports Trend Analysis Political and Legal Analysis	Expert input
		Economic		
		Political		
		Legal		
	2B. Technical		Use MEII or equivalent	Penetration testing Vendor Reports CSIRT Advisories Graph Theory Analysis
Step 3. Countermeasures and Defences (Strengths)	3A. Non-technical	Social	National & international threat advisories, and reports Business intelligence	Expert input
		Economic		
		Political		
		Legal		
	3B. Technical		Vendor whitepapers Product specifications	Expert input Simulations
Step 4. Impact	4A. Non-technical	Social	Wargaming What-if Analysis Scenario Analysis	Expert input
		Economic		
		Political		
		Legal		
	4B. Technical		Simulations	Expert input
	4C. Ecological		What-if Analysis	Environmental Impact Assessment
Step 5. Opportunities	5A. Non-technical	Social	National and business intelligence Political, legal, or economic assessments	Expert input Political and corporate alliances
		Economic		
		Political		
		Legal		
	5B. Technical		Vendor whitepapers Product specifications National and business intelligence	Expert input

The impact of a vulnerability being exploited by a threat (Step 4) can be estimated through use of wargaming, what-if and scenario analyses, simulations, and expert input. Potential ecological consequences (Step 4C) of an attack can be determined with a what-if or scenario analysis coupled with an environmental impact assessment. Possible opportunities or solutions to mitigate vulnerability (Step 5) can be identified through use of intelligence, product specifications, and vendor whitepapers; expert input may also be able to identify possible solutions through experience. Opportunities include participating in political alliances and joint technical committees, or improving and introducing technical controls. Ensuring compliance and accreditation will also aid in mitigating risk and vulnerabilities.

In the paragraphs above five steps in the process were described; during this process certain variables need to be rated; these will be used to determine the vulnerability and risk rating in a process that has been modified from the FAIR analysis. These variables can be summarised as:

- The likelihood of the threat taking action;
- The estimate capability of the threat;
- The required capability to overcome the identified vulnerability;
- The strength of the controls and countermeasures in place to protect the vulnerability; and,
- The impact or loss should the vulnerability be exploited.

These variables will be combined through the use of a modified FAIR process (or equivalent method according to organisational preferences). This is Step 6, and is illustrated in Table 4.3, where the X indicates the two variables are used in a risk matrix to determine the rating of the variable above. The primary modification from the original FAIR process is that the loss or impact no longer has primary and secondary factors. This is due to the fact that the primary impact of an IW attack (which will correspond to the objectives and motivation of the aggressor in the IW Lifecycle Model) will be more significant than any secondary factors; however, if the secondary factors can be estimated this may be incorporated. Another modification is that the variables for rating the threat and vulnerability have been altered. In an IW situation, the likelihood that the threat is making contact indicates an action of some form; the threat rating is therefore a combination of the threat capability and the likelihood of action. The vulnerability rating is a combination of the skill required to exploit the identified vulnerability, and the strength of the control measures in place.

Table 4.3: Proposed Framework Rating Determination, van Niekerk and Maharaj (2011a)

Risk				
Likelihood of a successful attack			X	Loss or Impact
Threat	X	Vulnerability		
Threat action likelihood X Estimated threat capability		Control strength X Required capability to exploit vulnerability		

The likelihood of a successful attack is a combination of the threat and vulnerability ratings; this is then combined with the impact rating to estimate risk for that particular vulnerability and threat pairing. Examples of the risk matrices used in the process are presented in Table 4.4 and Table 4.5; qualitative ratings of very low to very high are used (however these rating can be adjusted according to requirements).

Table 4.4: General Risk Matrix for the IW Fair Process, van Niekerk and Maharaj (2011a)

Variable 2	**Variable 1**				
	V. Low	*Low*	*Med*	*High*	*V. High*
V. Low	V. Low	V. Low	Low	Med	Med
Low	V. Low	Low	Low	Med	High
Med	Low	Low	Med	High	High
High	Low	Med	High	High	V. High
V. High	Med	Med	High	V. High	V. High

Table 4.5: Vulnerability Matrix for the IW Fair Process, van Niekerk and Maharaj (2011a)

Control Strength	**Required Capability to Exploit Vulnerability**				
	V. Low	*Low*	*Med*	*High*	*V. High*
V. Low	V. High	V. High	High	Med	Med
Low	V. High	High	High	Med	Low
Med	High	High	Med	Low	Low
High	High	Med	Low	Low	V. Low
V. High	Med	Med	Low	V. Low	V. Low

To keep track of the threat, vulnerability, and impact associations used in the process above a modified Threats-Vulnerabilities-Assets (TVA) worksheet may be used; an example is illustrated in Table 4.6. The TVA Worksheet is described in Section 2.7.1.9; as it is asset-centric, it needs to be

modified to be vulnerability-centric; threats are associated with the vulnerabilities. The potential impacts of the vulnerability-threat associations are estimated, and for each the risk is determined using the process described above.

Table 4.6: Modified TVA Worksheet

Vulnerability name and rating	Associated threat names and ratings	Estimated impact type and rating	Estimated risk rating
Vulnerability 1 (Rating)	Threat A (Rating)	Impact 1-A-1 (Rating) Impact 1-A-2 (Rating)	Risk 1-A-1 (Rating) Risk 1-A-2 (Rating)
	Threat B (Rating)	Impact 1-B-1 (Rating)	Risk 1-B-1 (Rating)
	Threat C (Rating)	Impact 1-C-1 (Rating)	Risk 1-C-1 (Rating)
Vulnerability 2 (Rating)	Threat B (Rating)	Impact 2-B-1 (Rating)	Risk 2-B-1 (Rating)
	Threat D (Rating)	Impact 2-D-1 (Rating)	Risk 2-D-1 (Rating)

Up to this point, the identified vulnerabilities and the associated risks have been evaluated; the vulnerability and risk ratings of the entire infrastructure need to be determined. Step 7 of the process is determining the ratings for the infrastructure vulnerability and risk using vector mathematics. The magnitude of a vector is calculated as shown in Equation 4.1:

$$\|\mathbf{X}\| = \sqrt[2]{\sum_{i=0}^{I} x_i^2}, \quad \textbf{4.1}$$

where I is the number of elements in the vector. The list of vulnerabilities are taken as a vector, with very low having a value of one, and very high having a value of five. The infrastructure vulnerability is then calculated as the magnitude of the vulnerability vector, as shown in Equation 4.2:

$$Infrastructure\ vulnerablity = \sqrt[2]{\sum_{i=0}^{N} v_i^2}, \quad \textbf{4.2}$$

where N is the number of identified vulnerabilities and v_i is the individual vulnerability rating. Similarly, the infrastructure risk is determined by taking the vector magnitude of all the individual risk ratings, as shown in Equation 4.3:

$$Infrastructure\ risk = \sqrt[2]{\sum_{i=0}^{M} r_i^2}, \quad \textbf{4.3}$$

where M is the number of risk elements and r_i is the individual risk rating. As each vulnerability may have multiple threats associated with it, there may be more than one risk rating per vulnerability; therefore from Equations 4.2 and 4.3, Equation 4.4 should hold true:

$$M \geq N \tag{4.4}$$

Vector magnitude is used to calculate the infrastructure vulnerability and risk as these exhibit similar characteristics: the vector magnitude increases as the number of elements or the magnitude of any one element increases. Likewise, the more individual vulnerabilities, or the more severe any single vulnerability, the greater the overall infrastructure vulnerability will be.

This process provides the ability to compare the overall infrastructure vulnerability or risk as the individual vulnerability or risk ratings change or are introduced or eliminated. The vulnerabilities may be prioritised by calculating the risk magnitude for each identified vulnerability, then ranking them according to their associated risk values. Vulnerabilities with higher risk values need to be addressed with higher priority than those with low risk values. The vulnerability and risk ratings may also be calculated for an individual asset, or for a specific impact type or attack objective, such as DoS, exploitation, corruption, and misuse. The relevant elements are treated as a vector for each area of interest, and the magnitude is calculated. An example of this is illustrated in Table 4.7 and Equations 4.5 to 4.7.

Table 4.7: Vulnerability by Impact Type

Vulnerability	Vulnerability Rating	Impact		
		DoS	*Corruption*	*Exploitation*
V1	3			✓
V2	2		✓	✓
V3	4	✓		
V4	3	✓	✓	✓
V5	5	✓	✓	

$$Vuln_{dos} = \sqrt[2]{(V3)^2 + (V4)^2 + (V5)^2} = \sqrt[2]{16 + 9 + 25} = 7.1 \tag{4.5}$$

$$Vuln_{corrupt} = \sqrt[2]{(V2)^2 + (V4)^2 + (V5)^2} = \sqrt[2]{4 + 9 + 25} = 5.9 \tag{4.6}$$

$$Vuln_{exploit} = \sqrt[2]{(V1)^2 + (V2)^2 + (V4)^2} = \sqrt[2]{9 + 4 + 9} = 4.7 \tag{4.7}$$

From this example, it can be seen that there is a greater vulnerability to a DoS attack compared to one to that will exploit or corrupt the data or information. The overall framework is adaptable in that it is modular, so any one aspect of the high-level structure can be replaced by an analysis or assessment methodology to suit the requirements of the organisation. Section 4.3.2 applies this proposed framework to the case of cloud computing.

4.3.2 Framework Application Example

This section presents an example of the proposed vulnerability assessment framework; in this case it is applied to the case of cloud computing in a corporate IW situation. A secondary objective of the thesis is to provide an additional assessment of an infrastructure; this section performs that role in addition to illustrating the application of the framework. The background to cloud computing is provided in Section 2.8.5. A previous version of this study was published in van Niekerk and Maharaj (2011a). During this assessment, some incidents will be referred to; some will be discussed in more detail in Chapter 5. Section 4.3.2.1 provides a background to the scenario, and Section 4.3.2.2 presents a threat assessment. Section 4.3.2.5 presents the vulnerability and risk assessment, Section 4.3.2.6 presents the opportunities, and Section 4.3.2.7 provides a review of the framework.

4.3.2.1 Scenario Background

Some areas of the scenario will be hypothetical, yet based loosely on actual incidents. It can be assumed that the organisation employing cloud services in residing in Country A. This organisation has provided services to the political opposition of the government of Country B, who has an aggressive network warfare policy, and a number of cyber-based attacks and espionage incidents have been attributed to them. It can be assumed that a hybrid cloud model incorporating a combination of community and private deployments is employed; part of the cloud offers services that contain sensitive government information. A client is required to access the cloud services on all end-user machines, and it is possible to access the services from smart mobile devices.

4.3.2.2 Threat Assessment

This section provides the threat assessment for the scenario. This corresponds to Step 1 in the framework; both non-technical and technical factors will be considered.

Step 1A: Non-technical factors

It is apparent from the Wikileaks incident discussed in Section 4.2.7.4 that organisations which become involved in politically sensitive or controversial incidents may be targeted with cyber-based attacks. Another example of this is the attacks on Google, which are attributed to China

(Information Warfare Monitor, 2009; McMillan, 2010). According to the Trustwave Global Security Report 2011, two of the top three targeted data types are trade secrets and corporate data (Trustwave, 2011). There is also a possibility that there may be political or social attacks through public statements by the government condemning the support of their opposition and malicious rumours, respectively. It can be assumed there is a low prevalence of this, and such a government will have a high capability is such tactics, giving a medium threat. In a context where a company with sensitive information that has supported the political opposition of a government with aggressive cyber-policies, it is apparent there is a high likelihood that it will be attacked.

Step 1B: Technical factors

According to the Cisco Annual Security Report 2010, enterprise networks are regularly infected with malware and consumer systems also experience a high infection rate; large service abuse levels results from this (Cisco, 2011). This report also indicates that since 2008, one of the top three prevalent attack types is a DoS attack (*ibid*.); as discussed in Sections 4.2.7.1 and 4.2.7.4, this was also used to target Estonia and organisations in the Wikileaks incidents. As botnets are created through malware, the DoS attacks are in some way related to malware infection rates; however, the main target of malware is to gain financial account information (Cisco, 2011; Trustwave, 2011). These methods could also be used to gain account details for unauthorised access to cloud services. The Trustwave report also indicated that only a small proportion of attacks against applications were against vulnerable third-party software. Another security problem is that wireless communications are susceptible to interception, even with security measures in place, and the increase in prevalence of smart mobile devices is resulting in new vulnerabilities (Trustwave, 2011). Social engineering is also considered a large threat (Cisco, 2011). According to Hayden (2010), the primary goal in IW is the ability to control an adversary's information through both breaching confidentiality and altering the information integrity; however this is complex. Monitoring the adversary's information is secondary, should full control not be achievable. A DoS attack is a last resort; however, this is the simplest to conduct (Hayden, 2010).

From the threat description the ratings can be determined given a high likelihood of attack from a highly capable aggressor; this is presented in Table 4.8. These ratings will be used in determining the risk.

4.3.2.3 Vulnerability, Countermeasure, and Impact Assessment

The section rates the vulnerabilities and countermeasures. This corresponds to Steps 2 to 4 in the framework.

Table 4.8: Threat Ratings

Attack	Capability	Prevalence/Likelihood	Overall Rating
DoS	High	Low	Medium
Breach confidentiality	Medium	Very High	High
Attack on client vulnerabilities	Medium	Medium	Medium
Malware	High	High	High
Attack on wireless services	Medium	High	High
Exposure due to mobile devices	Medium	High	High
Social engineering	High	High	High
Political attack	High	Low	Medium

Steps 2A, 3A, and 4A: Non-technical factors

For this example there are only a few non-technical factors; these ratings will be from an organisational perspective. The legal liability when considering cloud computing is uncertain as there is no universal standard that governs this. A reasonable control will be a strong service agreement which clearly defines the security responsibilities and liabilities. Due to the legal uncertainty, this can be rated as medium. Any breach could leave the organisation open to legal proceedings; therefore the capability to exploit this vulnerability is low. Using Table 4.5, this gives a vulnerability rating of high. The impact from legal issues can be rated as medium; they use organisation resources and may provide negative publicity.

An organisation does not have the political power of a full nation; therefore the required capability to politically attack the organisation is low. The only protection against this is to have strong political connections; however even this will be unable to prevent any attack, therefore the control can be considered as low. The vulnerability is therefore high; however the impact will not be great, and can be rated as low.

A broad social attack, where malicious rumours are used to damage the organisations image, only requires low capability; however, laws and strong corporate communications will be a strong control to illustrate the false nature of the claims. This gives a social vulnerability to perception

management as medium. The social impact can be considered as low, due to the origin of the rumours. However, should this be coupled with a data breach, both the impact and vulnerability will be high.

Employees who are unaware of potential threats may fall victim to social engineering. Due to the widespread use of social networks, this has become an ideal social engineering tool through which employees can be targeted (Trustwave, 2011). As social networks can be accessed on personal mobile devices that are outside of the organisation's network blocking employee access will have little affect; employee awareness training is cited as the most effective measure (Cisco, 2011; Trustwave, 2011). The required capability to conduct social engineering is low. As it preys on human weaknesses and creates uncertainty, the affects of awareness training will have it limits; therefore the control strength can be rated as medium. This results in a high vulnerability to social engineering. Using the information gained from social engineering, such as logon details, an attacker may breach confidentiality and integrity; this has a very high impact.

Steps 2B, 3B, and 4B: Technical factors

Cloud services may be physically located outside of the physical and network perimeter of the organisation; therefore any data being retrieved from or sent to the cloud will pass through the organisation's network gateway. As the connectivity to the cloud is dependent on the functioning of the gateway, this can be considered as a singularity, or a central point. Should the organisation's gateway be subjected to a DoS attack, the availability of the cloud services will be severely hampered. Little can be done to protect from large quantities of illegitimate traffic overloading the gateway; filtering may help to a small extent. The control strength against a DoS attack is very low. To conduct a DoS attack a botnet needs to be created and maintained, however there are tools available on the Internet to do so. The required capability can therefore be rated as medium; using Table 4.5 the vulnerability rating is seen to be high.

In April 2011 Amazon's cloud services experienced an outage (Brooks, 2011); the potential impact of an outage can be illustrated by this incident, where organisations that relied on these services were badly affected. For the SaaS and PaaS models, where the applications reside on the cloud, an outage may have a high impact as the client organisation will lose the availability of the applications or the ability to run them. For an IaaS model, where the cloud services can be seen as an extension to the client organisation's network, the impact will be low as the internal network will remain functional.

As the client used to access the cloud services is installed on all end-user machines, any design flaw or vulnerability will be repeated for every installation of the client. This is applicable to the concept of homogeneity; in this case it is high, and therefore the vulnerability will increase. Possible solutions to homogeneity proposed in Anderson *et al*. (1999) do not apply here; segmentation of the network will not remove the client vulnerabilities, and heterogeneity is not possible; therefore the control strength can be considered as very low. The client will not be freely available as it is for subscribers to the cloud services; any potential attack would first need to acquire the software in order to discover potential vulnerabilities prior to exploiting them. Therefore the capability required to exploit this is very high. This gives a vulnerability rating of medium. Should a vulnerability be exploited, an attacker may be able to access sensitive information, corrupt the information, or temporarily deny the user access to services. According to Hayden's priorities (described in Section 4.3.2.2), the impact due to a breach of confidentiality or integrity can be rated as very high; temporarily denying a user access can be rated as low.

As the cloud services require network connections, the proper functioning of the internal organisational network will affect availability of the cloud services. Should the internal network be operating very close to its maximum capacity it may be susceptible to internal DoS attacks. This can be created by propagating malware as the infect systems, or a few infected machines transmitting large quantities of data packets; this will degrade legitimate traffic and thus the accessibility to the cloud services. Antivirus applications can be considered to be able to detect and remove a large proportion of known malware; however, they are not effective against previously unseen malware. Therefore they can be rated as having a high control strength. Malware creation kits are freely available on the Internet (Fisher, 2011c), yet the attacker still requires some technical ability; this will therefore be rated as medium. Provided the anti-virus applications are updated regularly, the vulnerability to malware can be rated as low.

The impact of a malware infection will be temporary; the infected machines can be removed from the network and cleaned, but the network services will not be available during recovery. Therefore the impact can be rated as medium for all cloud service models. Some malware, such as keyloggers and backdoors, allow for the retrieval of information from systems and logon details; this will then provide the attackers with the information to gains access to the cloud servers and corrupt the data and breach confidentiality. The vulnerability and threat ratings are the same for malware, however the impact will be more severe, and can be rated as very high.

The introduction of mobility into an organisation's ICT increases vulnerability. The use of wireless networks and mobile communications results in electro-magnetic exposure, which is susceptible to jamming (denial of service) and interception. Whilst there are security measures on both wireless and mobile communications to prevent interception, these measures can still be broken (Nohl & Paget, 2009). The control strength against interception can be considered to be medium. Very little can be done regarding the jamming of wireless communications, except for removing the interference source; the control can therefore be considered as very low. The required capability to jam a connection is low as sufficient interference will do the job; however to break the encryption will be more difficult, and to breach integrity even more so. In addition to this, the attacker would need to be physically within signal range to conduct any of these attacks; this indicates a high level of planning would be required. The required capability will therefore be listed as very high to corrupt integrity, high to breach confidentiality, and low to jam the signal. This results in the respective vulnerabilities being high for jamming, and low for intercepting or corrupting the data in transit. The impact of jamming a mobile wireless connection is low; the user will only lose connectivity briefly. Breaches of integrity and confidentiality will be as before: very high.

Mobile devices may also be lost or stolen which increases physical exposure. The information contained thereon can be used to access cloud services. Whilst there are methods of remotely wiping the devices of all information, the attacker may retrieve the required logon details before the owner realises the device is missing and locks it. The control strength can therefore be considered to be medium. Low capability is required to steal the device. The vulnerability is therefore high. The impact is as before: very high for the breach of confidentiality and integrity.

There is also a degree of physical exposure of an organisation's internal network, and the connection points to the external Internet. An attacker may attempt to gain access in order to breach confidentiality or integrity, or disrupt services. With reasonable physical security and awareness training, gaining access may be difficult; therefore the control strength can be considered as high. The required capability to gain access can be considered to be medium, as there is a risk of getting caught and possibly inside information or assistance would be required to gain full access. This results in a low vulnerability. To cut external physical connections, however, may be simpler, and the required capability is low, with low control strength. This gives a high vulnerability to denial of external connectivity. As before, the impact of breaching confidentiality or integrity is very high, and the impact of denying services is low.

The data residing on the cloud infrastructure (for the IaaS model), and the data in transit between the organisation's network and the cloud infrastructure may also be targeted. Encryption provides a strong control, however it can be broken. It can therefore be rated as high for preventing a breach of confidentiality, and very high for detecting corruption. The required effort to break the encryption can also be rated as high for breaching confidentiality and very high for corrupting the information; this results in a low and very low vulnerability, respectively. The impact for these breaches will be very high.

The functioning of cloud services is dependent on the correct functioning of the organisation's Internet service provider (ISP). Should a DoS attack be successfully mounted against the ISP, the organisation will lose access to the cloud services; no control can be provided by the organisation for this, and the strength can be considered to be very low. However, the ISPs are resilient, and have their own control measures; the required capability to disrupt them would be very high. The vulnerability is therefore medium. As for a DoS attack on the organisation's gateway, the impact will be low for IaaS and high for both SaaS and PaaS models.

4.3.2.4 Modified TVA Worksheet and Individual Risk Ratings

The threats from Section 4.3.2.2 and the vulnerability and impact rating from Section 4.3.2.3 are summarised in Table 4.9. Using the modified FAIR method (Table 4.3) and the risk matrix (Table 4.4), the risk rating is determined.

4.3.2.5 Infrastructure Vulnerability and Risk Ratings

The ratings for the infrastructure vulnerability and risk are determined using Equations 4.2 and 4.3, respectively. The individual ratings are listed in Table 4.9; where very low is equivalent to 1 and very high is equivalent to 5. The infrastructure vulnerability and risk ratings are calculated for the IaaS and SaaS/PaaS models; and ratings for the three impact types (denial, corruption, and breach of confidentiality) are determined. These are presented in Table 4.10. There are a total of fifteen identified vulnerabilities, and twenty-three associated risks (with two variants between the cloud service models). From Table 4.10, it can be seen that the greatest vulnerability is to DoS attacks, then breaches of confidentiality, and least vulnerable to corruption of information. However, the highest risk is for confidentiality breaches, then corruption, and then DoS has the lowest risk. This corresponds to Hayden's (2010) claims that accessing information is more beneficial to an attacker; however, it is more difficult compared to simply denying access to the victim. Breaching confidentiality has a lasting impact, and is both detrimental to the victim and beneficial to the attacker; whereas denial of the victim's services is only detrimental to the victim for the period that

the attacker is able to allocate resources to the attack. There is also a difference in risk between the IaaS and SaaS/PaaS models; this is due to the potential impact that differs between the two service models. The non-technical areas also contributed to the risk; this indicates that considering the context will impact on the risk and vulnerability assessment.

Table 4.9: Cloud Services TVA Worksheet

Vulnerability name and rating	Associated threat names and ratings	Estimated impact type and rating	Estimated risk rating
Political (HIGH)	Political (MEDIUM)	LOW	Political (MEDIUM)
Social (MEDIUM)	Rumour (MEDIUM)	Rumour (LOW)	Rumour (LOW)
	Including breach (HIGH)	Including breach (HIGH)	Including breach (HIGH)
Social engineering (HIGH)	Social engineering (V HIGH)	Integrity (V HIGH)	Integrity (V HIGH)
		Confidentiality (V HIGH)	Confidentiality (V HIGH)
Gateway singularity (HIGH)	DoS (MEDIUM)	SaaS/PaaS (HIGH)	DoS SaaS (HIGH)
		IaaS (LOW)	DoS IaaS (MEDIUM)
Client vulnerability – homogeneity (MEDIUM)	Attack on client vulnerability (MEDIUM)	Integrity (V HIGH)	Integrity (HIGH)
		Confidentiality (V HIGH)	Confidentiality (HIGH)
		Denial (LOW)	Denial (LOW)
Internal network operating capacity (LOW)	Malware (HIGH)	Denial (MEDIUM)	Denial (MEDIUM)
Malware – key loggers and backdoors (LOW)	Malware (HIGH)	Integrity (V HIGH)	Integrity (HIGH)
		Confidentiality (V HIGH)	Confidentiality (HIGH)
Wireless interception (LOW)	Corruption (LOW) Interception (HIGH)	Integrity (V HIGH)	Integrity (MEDIUM)
		Confidentiality (V HIGH)	Confidentiality (HIGH)
Wireless jamming (HIGH)	Jamming (HIGH)	Denial (LOW)	Denial (MEDIUM)
Mobile devices – exposure (HIGH)	Theft (HIGH)	Integrity (V HIGH)	Integrity (V HIGH)
		Confidentiality (V HIGH)	Confidentiality (V HIGH)
Network physical exposure (LOW)	Inside access (MEDIUM)	Integrity (V HIGH)	Integrity (HIGH)
		Confidentiality (V HIGH)	Confidentiality (HIGH)
External connection exposure (HIGH)	Physical attack (MEDIUM)	Denial SaaS/PaaS (HIGH)	SaaS/PaaS (HIGH)
		Denial IaaS (LOW)	IaaS (LOW)
Encryption vulnerabilities – integrity (V LOW)	Encryption attacks (HIGH)	Integrity (V HIGH)	Integrity (MEDIUM)
Encryption vulnerabilities – confidentiality (LOW)	Encryption attacks (HIGH)	Confidentiality (V HIGH)	Confidentiality (HIGH)
Dependence on ISP (MEDIUM)	DoS attack on ISP (MEDIUM)	SaaS/PaaS (HIGH)	DoS SaaS (HIGH)
		IaaS (LOW)	DoS IaaS (LOW)

Table 4.10: Infrastructure Vulnerability and Risk Ratings, adapted from van Niekerk and Maharaj (2011a)			
	IaaS	**SaaS/PaaS**	**Maximum possible rating**
Denial and disruption	$V_I = 8.37$ $R_I = 6.24$	$V_I = 8.37$ $R_I = 8.37$	$V_I = 12.25$ $R_I = 12.25$
Breach of confidentiality	$V_I = 7.55$ $R_I = 11.4$	$V_I = 7.55$ $R_I = 11.4$	$V_I = 13.23$ $R_I = 13.23$
Corruption	$V_I = 7.35$ $R_I = 10.77$	$V_I = 7.35$ $R_I = 10.77$	$V_I = 13.23$ $R_I = 13.23$
Non-Technical	$V_I = 5.0$ $R_I = 5.39$	$V_I = 5.0$ $R_I = 5.39$	$V_I = 7.07$ $R_I = 8.66$
Overall	$V_I = 12.0$ $R_I = 17.72$	$V_I = 12.0$ $R_I = 18.57$	$V_I = 19.36$ $R_I = 23.98$

The ratings presented here are for an IW scenario where there is a high likelihood of attack; for normal organisational operating conditions, the risks will not be as high, and there will also be a reduction in the vulnerability due to the different context.

As confidentiality is the highest risk, the priority should be on addressing the relevant vulnerabilities. Addressing some non-technical issues may also reduce the threat context, which will reduce all risks. The two individual vulnerabilities that have the highest risk are social engineering and exposure due to mobile devices; these need to be addressed in particular.

4.3.2.6 Possible Opportunities

This section presents possible opportunities to reduce the risks and vulnerabilities presented above. This corresponds to Step 5 in the proposed vulnerability framework, presented in Table 4.2.

Step 5A: Non-technical factors

The organisation's political and legal standing may be improved by joining international partnerships and alliances. By becoming involved the organisation may be able to contribute to the necessary international security standards regarding cloud computing. Ensuring compliance to international standards will also aid in reducing risk and vulnerabilities. As social engineering and exposure due to mobility are the two highest risk vulnerabilities, awareness training should be conducted to improve employee resilience against these attacks.

Step 5B: Technical factors

The organisation may introduce improved or additional technical security measures; improving technical access controls to the network and cloud services will reduce the vulnerability and risk of a breach.

4.3.2.7 Framework Review

The proposed vulnerability assessment framework was applied to a hypothetical scenario of an organisation under threat of an IW attack; the assessment was conducted to investigate the vulnerabilities and risks regarding the organisation's deployment of cloud computing services.

The vulnerability framework was able to adequately describe the scenario, and the results were consistent with the literature regarding IW threats. The modular and layered nature of the framework will provide a user to replace certain techniques or methodologies with those that are more suitable for their specific needs.

4.4 Chapter Summary

The chapter presented the proposed adapted IW model, the IW Lifecycle model, and the vulnerability assessment framework. A need was identified for a consolidated and standardised model for IW; the proposed framework intended to contribute towards this. It was also used to generate the proposed vulnerability assessment framework, which is from an IW perspective. This framework will be employed throughout the remainder of the thesis to perform the vulnerability assessment of the mobile infrastructure.

Both the IW model and the vulnerability assessment framework were applied to case studies; the IW model was used to analyse a series of historical and current incidents, and the vulnerability assessment framework was applied to a hypothetical scenario of an organisation employing cloud computing services. The IW model was able to describe the various incidents, even though they were related to different functional areas, and were of differing magnitude. The results of the vulnerability framework were consistent with literature. These results indicated that breach of confidentiality is the highest risk; however, there is a higher vulnerability to DoS attacks. The introduction of non-technical context factors does influence the overall risk and vulnerabilities.

Chapter 5. Trend and Incident Analysis

5.1 Introduction

This chapter will discuss various trends that may be realised after discussing recent cyber-based incidents over the previous 12 years up to 20 October 2011; no information after this date was considered. Secondary data is also used to illustrate the cyber-environment for South Africa in a global context. The information presented was gathered from a variety of documents, including online and print news, books, academic articles, and reports. The chapter is organised into a funnel approach, where the later sections have a narrower focus than the earlier sections.

Section 5.2 illustrates the importance of information as a strategic asset and how it relates to information warfare and security. Section 5.3 discusses the trends of recent conflicts, and the changing role that electronic warfare and network warfare are taking. Section 5.4 analyses the trends of cyber-based incidents, and how the Internet is becoming weaponised. Sections 5.5 and 5.6 follow this line of analysis, yet focus on the security incidents related to mobile phones and Web 2.0 technologies, respectively. Section 5.7 discusses these trends and secondary data in the South African environment, and places this in a global context. There may be some repetition regarding the analysis of specific incidents; however, the analysis will be conducted from different viewpoints. Section 5.8 summarises the chapter. Figure 5.1 illustrates the structure and flow of the chapter.

5.2 Information as a Strategic Asset

Information is a crucial element when in a state of conflict or competition. Unconventional and asymmetric conflict may be conducted by states, and non-state actors such as insurgents and criminals; this section will also discuss the role of corporate competition and network warfare as asymmetric conflicts. Society is becoming more reliant on the virtual world, and the information and related processes and systems are becoming increasingly important to strategic decision making. The effective use of information may prove to be an equaliser in an asymmetric environment, for example e-commerce allows small companies to compete on a global scale, and can reduce the decision cycle time through the production of timely, accurate and relevant information. A previous version of this section was published in van Niekerk & Maharaj (2010a). Section 5.2.1 will provide a history of strategic information; Section 5.2.2 presents concepts

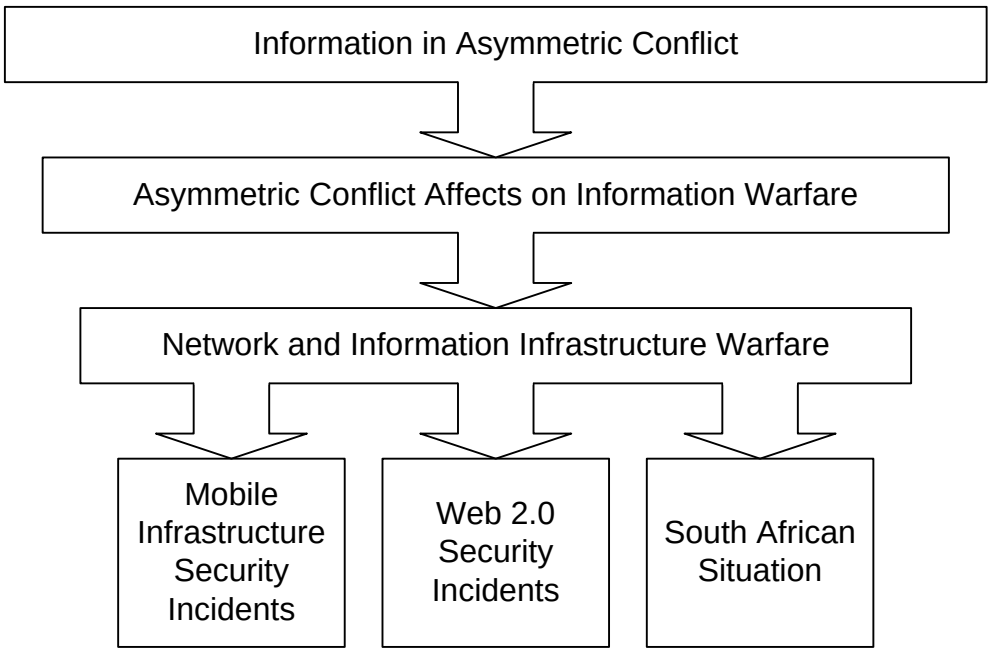


Figure 5.1: Chapter Structure and Flow

regarding conflict and competition in asymmetric environments; Section 5.2.3 illustrates the application of trend analysis to information security and warfare; and Section 5.2.4 summarises the section.

5.2.1 A History of Strategic Information

The concept of strategic information may be found in various forms throughout history. Examples from the myths and legends of the ancient world include the example of the Trojan Horse, where the Greeks used their knowledge of the Trojan customs to deceive and ultimately defeat them. The fall of the old gods in Norse mythology was brought about through the use of information by the trickster god Loki. Both Sun Tzu and Sextus Julius Frontinus in his work *Strategemata* discuss deception in battle (van Creveld, 2000). Alexander the Great made use of intelligence to find weaknesses in the Persian Empire, which allowed him to defeat a numerically superior force, and Genghis Khan improved his communications lines to allow his forces to provide critical mass at any point (Delibasis, 2007). A German general in the First World War, von Seekt, also recognised the importance of knowledge (van Creveld, 2000). Numerous examples of code-breaking, propaganda and deception can be found in the Second World War (Delibasis, 2007), and this continued through to modern times during the Cold War between the West and former Soviet Bloc; in South Africa the Apartheid regime censored the media in an attempt to control information, and this continues in some regimes today.

Stannard (2008) provides examples of the South African Air Force using intelligence and information to avoid superior Soviet-made aircraft in order to avoid casualties in their sorties into Angola; this allowed a technologically inferior force to be more efficient than the superior one. During the Angolan and Mozambique campaigns, the detail of intelligence needed to be great – specific locations and addresses were needed prior to conducting raids. An example also shows that intelligence may prove beneficial beyond the battlefield: the South African forces captured a Soviet-made air-defence system in Angola which had not previously been seen by Western intelligence; this provided the South Africans with the opportunity to "trade" intelligence (Stannard, 2008).

5.2.2 Conflict and Competition in an Asymmetric and Unconventional Environment

Asymmetric conflict is usually when one participant has a vast superiority over the other, most commonly in technological abilities or numbers; this situation usually results in an unconventional conflict, where the inferior participant changes tactics to compensate for the asymmetry. There are also cases of moral or ethical asymmetry, such as the use of child soldiers, suicide bombers, and human shields. With the modern pervasiveness of information and communications technology, the information asymmetry between adversaries and competitors has become more pronounced.

5.2.2.1 State of Asymmetric Conflicts

The majority of modern armed-conflicts are unconventional, and involve non-state actors. Table 5.1 shows the number of armed conflicts for the period 2002 to 2005, from a dataset initiated by Gleditsch, Wallensteen, Eriksson, Sollenberg, & Strand (2002). Table 5.2 shows the number of non-state armed conflicts for the same period. The two tables originate from different data-sets, so there is not a perfect match, however it can be seen that a large number of conflicts are classed as minor, and that the number of non-state armed conflicts is relatively large; from this it can be determined that the vast majority of armed conflicts are low-intensity with non-state actors. Figure 5.2 shows the number of armed conflicts for a longer period (1994-2008); as can be seen from 2003 there has been a gradual increase in the number of armed conflicts, primarily due to the increase in minor armed conflicts. From Table 5.2 it appears that the majority of non-state conflicts occur in Sub-Saharan Africa, making this particularly relevant to the study from a South African perspective.

Table 5.1: Armed Conflicts 2002-2005				
	2002	2003	2004	2005
Minor (25-999 deaths p.a.)	25	24	25	27
Major / War (>1000 deaths p.a.)	7	5	7	5
Total	**32**	**29**	**32**	**32**

Source: UCDP/PRIO Armed Conflict Dataset Ver.4-2009 (Uppsala Conflict Data Program, International Peace Research Centre, 2009); Gleditsch *et al*. (2002)

Table 5.2: Non-State Armed Conflicts				
Region	2002	2003	2004	2005
Sub-Saharan Africa	24	23	17	14
Americas	2	2	4	3
Asia, Central and South	3	5	3	4
Asia, East & SE & Oceania	2	0	1	1
Middle East & North Africa	3	3	3	3
Total	**34**	**33**	**28**	**25**

Source: UCDP/Human Security Centre Dataset (Uppsala Conflict Data Program, Internation Peace Research Institute, 2007).

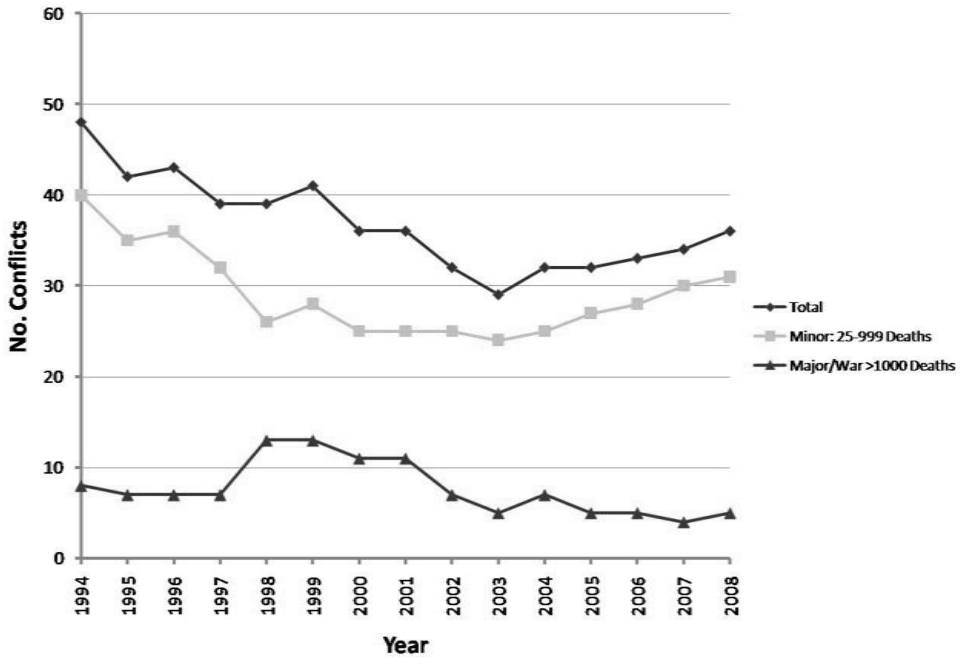


Figure 5.2: Number of Armed Conflicts per Year, source: UCDP/PRIO Armed Conflict Dataset Ver.4-2009 (Uppsala Conflict Data Program, International Peace Research Centre, 2009); Gleditsch *et al.* (2002)

The low-intensity unconventional conflicts may have an impact on business, in that many revolve around the areas rich in strategic raw materials; therefore industries reliant on these materials may face shortages or increased prices, or may be required to introduce additional security measures for their operations in regions of conflict. Security and defence-related industries may actually receive a boost due to conflict in that there is a greater demand for their products and services. Tourism may also be negatively affected in areas which experience heightened levels of violence. It is therefore important to follow the trends in conflict as it may impact on business, or on the political environment resulting in increased tensions and therefore the possibility of related security incidents.

5.2.2.2 Strategic Information Related to Piracy

Piracy at sea is growing, particularly off the coast of Somalia, where pirates see this as a viable financial or economic venture; and they have learnt that the ransom for the crew and cargo is far more rewarding than robbery (Carney, 2009). Many shipping corporations have learnt that tolerating the pirates and paying the ransom is often less costly and troublesome than having to deal with the insurance, the resulting investigations and the negative impact on their reputations (Torchia, 2009). Webb (2009) reports that the Somali pirates are utilising a form of business intelligence, whereby informants in London are providing shipping details to the pirates by satellite phone; this information provides the pirates with a strategic asset that allows them to plan and choose their targets. However, the pirates still make mistakes despite their advantage of being forewarned; the French naval flagship was misidentified in poor light and attacked, which resulted in the capture of five pirates (Asquin, 2009). Decision makers in the shipping companies, and those who rely on these companies, would be wise to keep track of pirate tactics and trends to evaluate the risk of using shorted (but pirate-infested) routes as opposed to longer (but safer) shipping lanes. Due to hostilities amongst many of the nations that are providing naval forces to police the pirate-infested waters, a fully co-ordinated effort is difficult; this has resulted in a neutral communications channel called Mercury (StrategyPage.com, 2009b). This circumvents the political hostilities, and together with increased aerial reconnaissance is hindering the pirate's operations (StrategyPage.com, 2009b).

Broadcasts may also be pirated; as they are wireless, it is easy to receive the signal, which then could be unscrambled using modified decoders, enabling the broadcast to be viewed without having to pay the subscription. An example is DirectTV in the United States; the access cards for their TV systems were pirated (Jones, Kovacich, & Luzwick, 2002). The company monitored online activity,

to understand the workings of the signal pirates, and then using this information released apparent updates that rendered the pirated access cards useless (*ibid*.). It is also possible to interfere with these broadcasts by transmitting another signal over it, which effectively jams the signal; this occurred in Sri Lanka, where the British Broadcasting Corporation suspended their partnership with the Sri Lankan national broadcaster after the transmission had been interfered with (TamilNet.com, 2009). Other media, such as CDs, DVDs, and software are also pirated, resulting in loss to the production companies; it is in their interests to protect the copyright of their products, which has resulted in an ongoing struggle between to improve copyright protection schemes and methods to break them.

5.2.2.3 Strategic Information and Asymmetric Competition in Business

During the industrial age, organisations that were heavily dependent on communications needed to be centralised; however, the rapid advancements in information and communications technology have allowed organisations to become geographically dispersed without compromising their communications. Even though organisations are physically dispersed, the employees may become virtually coalesced through regular contact via the use of communications technologies and social networking applications.

The concept of asymmetric conflict may be seen in the corporate sector. Small, medium, and micro enterprises (SMMEs) are disadvantaged when compared to larger companies; they do not have the financial strength, buying power, employee numbers and possibly brand recognition that the larger corporations are renowned for. By making effective use of information technologies, and particularly the Internet, the SMMEs can compete on a global scale. Their smaller size and lower overheads allows them to be more adaptable, undercut costs of their larger competitors, or offer customised services, all of which would prove to be an advantage. This is analogous to small guerrilla forces in a military context.

Information regarding the culture of a target audience is of strategic value in both propaganda and marketing. Iraqi propaganda broadcasts during the 1991 Gulf War failed in their attempt to disillusion American forces due to their lack of understanding of American culture; the broadcasts claimed that the soldier's wives would be sleeping with Tom Cruise, Tom Selleck, and Bart Simpson (Denning, 1999). Coca Cola introduced Diet Coke into Japan, and the product failed and had to be renamed Low-Calorie Coke due to a negative perception of dieting in Japan (Nakamoto, 1996); this shows how a lack of understanding the target audience can have negative strategic implications.

Corporations may also be provided opportunities by asymmetric conflict: a California-based company developed software based on PayPal's model for identifying cyber-criminals which they used to discover terrorist financing networks and trends in roadside-bomb attacks (Weinberger, 2009).

5.2.2.4 Network Warfare as an Asymmetric Conflict

Cyber-attacks provide the attacker with an asymmetric advantage: Hayden (2010), a retired general, claims that Internet "geography" favours the attacker. Major cyber-attacks include the DDoS attacks against Estonia and Georgia. The largest Estonian bank was forced to close its Internet banking website and is estimated to have lost over $1 million (Rolski, 2007). The cyber-attack on Georgia preceded the Russian military incursion into South Ossetia, and by targeting the government and media organisation the Georgian ability to communicate domestically and internationally was severely hindered (Hart, 2008); this gave the Russians information dominance regarding the view of the conflict.

Cyber-incidents may also be used to gain information; Section 5.4 will discuss these in more detail. Phishing attacks are aimed at tricking online banking customers into revealing sensitive account information that allows criminals to access the money (Pickworth, 2009). Phishing attacks were involved in the SMS banking fraud in 2009, where an excess of R5 million was stolen (De Vries, 2009); a scam that targeted South African Airways in 2007 resulted in a R14 million loss (Rondganger, 2007). Remediation costs from major outbreaks of viruses and worms may also prove to be costly (Veerasamy & Eloff, 2008).

Cyber-attacks are asymmetric in that the attacker may be able to maintain a high degree of anonymity; whilst it is possible to identify individual computers that are involved in a DDoS attack, the persons controlling them may never be identified. The cost to the attacker is also far less than that of the defender. Cyber-based scams also present a lower risk than a physical robbery, and may be more rewarding, as can be seen from the examples the amounts stolen were in the order of millions of Rands.

It is not yet established as to what constitutes network warfare in the form of cyber-war: some contend that for it to be a true cyber-war, then it should be nation-states as the main protagonists (Schneier, 2010; Fiterman, 2010). Others argue that due to the global shift towards unconventional conflict between sub-national groups and organisations, cyber-war cannot be expected to follow the traditional war between nation-states, and will rather exhibit the trend of sub-national groups and

organisations participating as a major protagonist (Fiterman, 2010). Should this be the case, then it is probable that cyber-war would exhibit asymmetries, as are found in the modern unconventional conflicts.

5.2.3 The Application of Trend Analysis to Information Warfare and Security

As mentioned in Section 5.2.2.4, cyber-based security incidents are asymmetric in that the attack is essentially faceless. There is a definite need to protect corporate and personal information and the systems the information resides on, as a breach raises concerns of information integrity, corporate image and legal liabilities. Knowing the trends in security incidents and the legalities that surround them is of strategic importance. This section discusses examples and illustrates the usefulness of applying trends to generate models.

A written information security policy is a strategic asset in that it aids in mitigating corporate liability should an employee use a corporate system for breaching confidential information or launching an attack on another party; should there be no written policy, that employee cannot be held liable for misconduct, which will place liability on senior management (Etsebeth, 2006). Similarly, it is possible for organisations to be held legally liable for a compromised system to be emitting unsolicited or malicious transmission; many organisations set their gateway or firewall policies to filter data ingress, however leave egress policies and allow networks to freely transmit over the Internet (Brenton, 2006). By providing egress protection, the organisation may preserve the availability of its gateways to the Internet from flooding; and may mitigate the legal implications of participating in a DDoS attack, even if it was unintentional. This policy is also wise with wireless application services on mobile phones, as unsolicited and spam SMS messages may also result in legal liability. In South Africa, the Wireless Applications Service Providers Association attempts to regulate the industry and fines offending organisations (Perelson, Ophoff, & Botha, 2006).

To illustrate the creation of knowledge from information, and the use in strategic decision making with regard to risk analysis, a trend showing the potential compensation payout for the number of records compromised if an organisation's systems were breached was generated; this is shown in Figure 5.3. The plot was generated from actual compensation amounts due to legal proceedings in the United States. A trend line was then fitted to the data points using the trendline option in Microsoft Excel, and the equation of the trend line was displayed in the figure. As can be seen, the trend in compensation amounts follows a power law, and increases rapidly initially compared to the increase in number of records compromised, and then levels off for larger numbers of records that

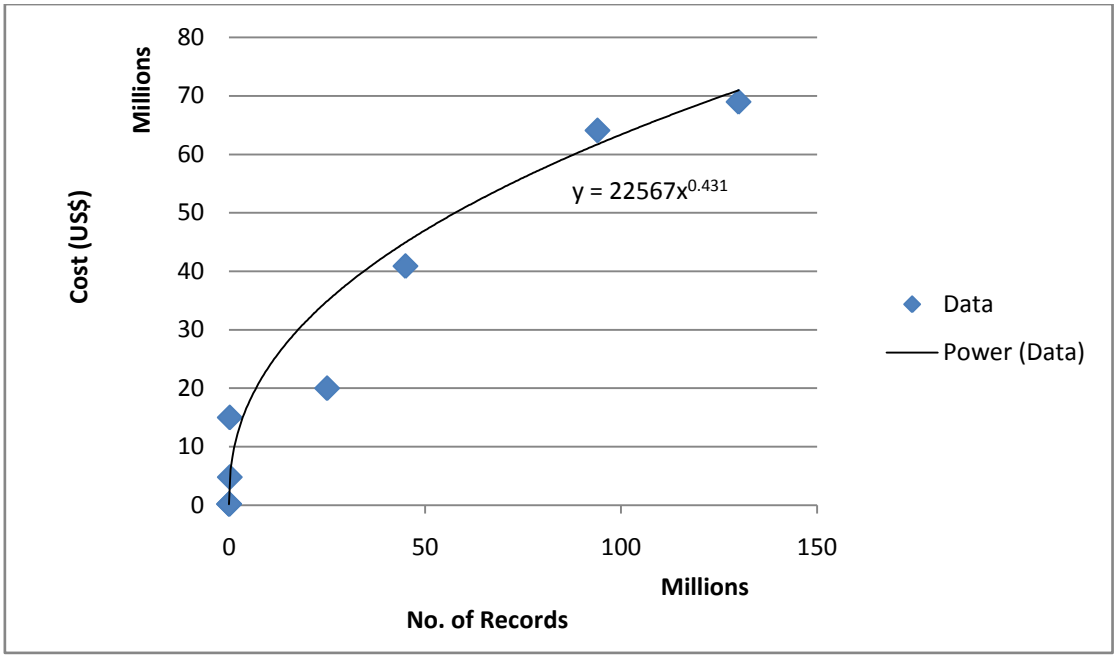


Figure 5.3: Graph of Compensation Payout for Data Breaches, source (Open Security Foundation, 2011)

were compromised. This is a rough estimate; with more data points the plot will be more accurate, and can be used to calculate the potential loss due to a data breach.

The Ponemon Institute (2008; 2009a; 2010a; 2010b; 2010c; 2011a; 2011b) releases annual studies of the costs of data breaches. Table 5.3 summarises these costs per record breached. The main trend that is that the cost to the organisation per record breached is increasing each year.

Table 5.3: Cost Per Record Breached, source: Ponemon Institute (2008; 2009a; 2010a; 2010b; 2010c; 2011a; 2011b; 2011c)

	2005	2006	2007	2008	2009	2010
US	$138.00	$182.00	$197.00	$202.00	$204.00	$214.00
UK			£47.00	£60.00	£64.00	£71.00
Germany				112.00 €	132.00 €	
Australia					$123.00	$128.00

Similarly, the fine for distributing spam emails in the United States can be approximated with the following equation (Hartman, 2005):

$$F = 500 \times L_{email} \times T_{distributed}, \quad \textbf{5.1}$$

where F is the fine is Dollars, L_{email} is the size of the emailing list, and $T_{distributed}$ is the number of times the emails were sent per annum.

Such models may be used in a risk analysis process to calculate the financial impact due to systems being compromised and used to distribute spam, or the data being breached. Likewise, analysing trends in attack statistics and methods may aid the identification of future threats and the likely vulnerabilities that they will exploit. These trends will also be useful in attempting to protect critical information infrastructure from attack.

5.2.4 Summary

Information, data, and knowledge may aid in strategic decision making. This section provided a history of strategic information, and the benefits in an asymmetric environment. Examples were provided to illustrate the corporate sector and network warfare have strong asymmetric elements, and the role strategic information may play in these situations. Examples of using trends to predict financial impact from information security breaches were provided.

5.3 Trends in Conflicts and the Impact on Information Warfare

In order to assess what the future roles of IW could entail, it is necessary to analyse trends in recent conflicts. Of particular interest is the technology level employed in conflicts, and how this would affect the enabling domain of the IW construct. This section will analyse the employed technologies in a number of sample conflicts and incidents from 1993 to 2010. An earlier version of this section was published in van Niekerk & Maharaj (2009c). The chronological order of the conflicts and incidents is shown in Figure 5.4; however, they will be discussed in groupings according to themes in Section 5.3.1. Section 5.3.2 will summarise the trends in these conflicts, and Section 5.3.3 will discuss the potential future roles of IW.

5.3.1 Background to the Sample Conflicts

The conflict in Somalia is generally known for the Black Hawk Down incident in 1993, however the events preceding and immediately following that incident is what defined that conflict. The United Nations troops providing aid in Somalia were continuously having their convoys ambushed and raided by the warlords; the primary weapons used for this purpose were remotely detonated mines. United States forces entered Somalia to support the United Nations, and aimed to capture the most powerful warlord, Mohammed Farrah Aidid, and his aides. The Central Intelligence Agency supplied sophisticated electronic surveillance technology; however, this was defeated by the Somalis, who were using basic-handheld radios and drums to communicate (Adams, 1998). The action that ended involvement of the United States in Somalia was the defiling of the bodies of US

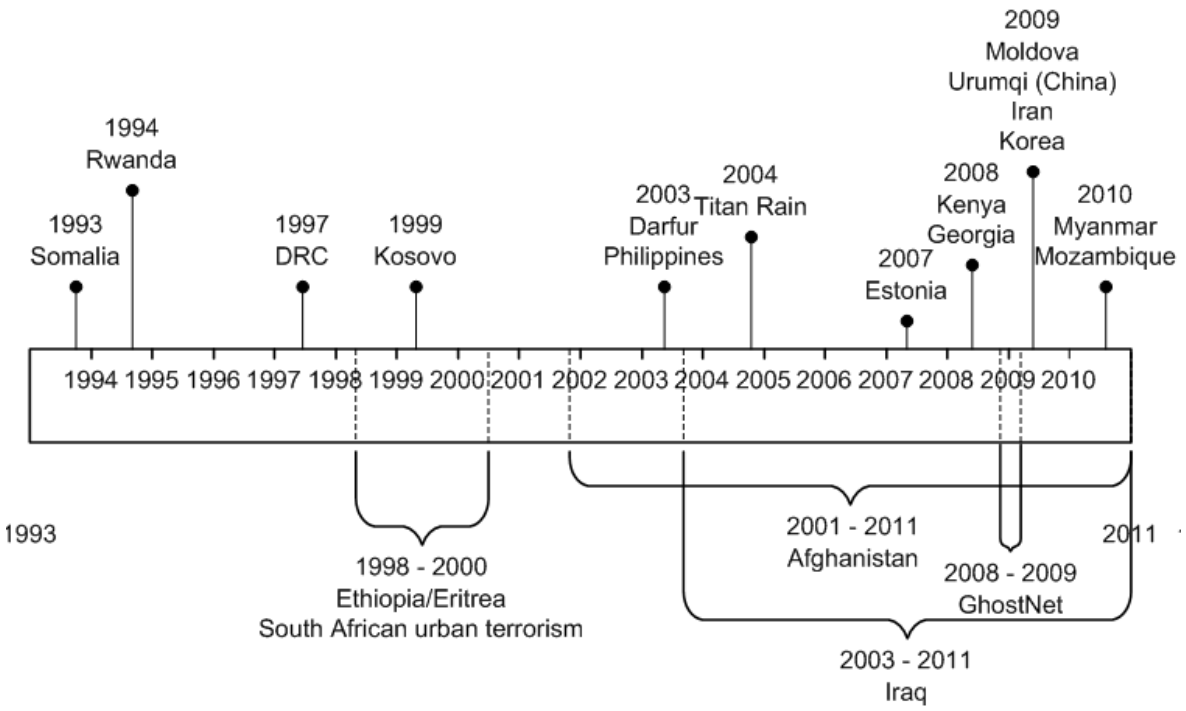


Figure 5.4: Timeline of Conflicts and Incidents, van Niekerk and Maharaj (2009c)

servicemen in front of CNN cameras; this resulted in the US public successfully pressuring the government to withdraw (Taylor, 2002). This incident was described in more detail in Section 4.2.7.3. Subsequently, handheld radios and mobile phones were captured along with Somali pirates; therefore it is obvious that these devices are still being used to coordinated attacks (Shachtman, 2009b).

The Rwandan genocide of 1994 used a mix of low-technology and high-technology; radio broadcasts were used to incite the violence, yet machetes were the main weapon to conduct the slaughter (Hutchinson, Huhtinen, & Rantapelkonen, 2007). Ethnic tensions in the Congo region and Darfur in 2003 employed similar low-technology solutions. The border war between Ethiopia and Eritrea, where two of the world's poorest nations managed to field advanced weapon systems, including fighter aircraft with electronic warfare systems, came as a surprise (Du Toit, 2003). These examples illustrate the use of improvisation with everyday items to conduct violent conflict, however technology can be bought and introduced almost overnight; this creates a degree of uncertainty in the battlefield.

Ignatieff (2001) has dubbed the NATO intervention in Kosovo as a "virtual war"; the actual fighting consisted of aerial bombardment, there were a number of cyber-based attacks from both sides, and a propaganda war through the media. The initial attacks concentrated on suppressing the Yugoslav

air-defence network, before migrating to military ground forces and dual-use targets. These latter targets could be used by both civilian and the military; such as bridges, broadcasting stations and power substations (Ignatieff, 2001). The conflict in Afghanistan and Iraq in 2003 was initiated in a similar fashion; with the suppression of adversary capabilities using bombardment and electronic warfare, which was followed by a ground offensive (conducted by the rebels in the Afghan case). These conflicts also saw the introduction of embedded journalists who reported virtually real-time from the battlefield. After the overthrow of the regimes, the conflict turned into an insurgency, where ambushes were orchestrated through the use of suicide bombers and improvised explosive devices (IEDs); which have been the most effective weapon deployed against coalition forces (Eshel, 2007). Many of the IEDs are remotely detonated using everyday devices, such as toy radio controls and mobile phones (Eshel, 2007); and are comparatively low-technology compared to the systems of the coalition forces. Similar devices were used in the urban terrorism in Cape Town during the late 1990's; again mobile phones were occasionally used as trigger devices (Sabasteanski, 2005).

Political confrontation has migrated to the communication networks; in April 2007 Estonia was subjected to cyber-based attacks that were a demonstration of dissatisfaction over the relocation of a war memorial. Estonia was left without some critical services as the websites of the government, financial institutions and media were attacked for a period of three weeks (Veerasamy N. , 2009b; Germain, 2008); this was described in more detail in Section 4.2.7.1. In 2009 three waves of similar attacks targeted the websites of financial institutions, government and the media in the United States and South Korea (Sudworth, 2009). As discussed in Section 5.2.2.4, Georgia was also targeted with similar attacks; this case is unique in that the cyber-attack immediately preceded by the Russian incursion into South Ossetia. The Russian government denied involvement in the cyber-attacks, and it appears as they were orchestrated by hackers sympathetic to the Russian cause (Waterman, 2008). Myanmar also experienced a large scale DoS attack in 2010 due to internal political conflict (Labovitz, 2010). Modern equipment was fielded by both sides in the fighting itself (McDermott, 2009). Intelligence gathering of a confrontational nature has also migrated to cyber-space; in 2004 during the Titan Rain incident, military computers were penetrated in what appeared to be an intelligence gathering operation (Thornburgh, 2005a;2005b), and the GhostNet cyber-espionage network targeted political adversaries (Information Warfare Monitor, 2009). The Israeli conflict with Palestinian groups also migrated online through the "Electronic Intifada" (Yin, 2009). This conflict is largely asymmetric, and Israel is reported to be using unmanned aerial

vehicles for surveillance and electronic warfare activities (Kunkel, 2008a). There are also reports of Israeli IW units hacking into mobile phone and media systems to disseminate PSYOPs messages (StrategyPage.com, 2009a); for the purposes of this dissertation, the concept in penetrating the communications infrastructure to insert illegitimate messages is important.

Mobile phone SMS services and social networking applications have been used to orchestrate anti-government protests, and to provide information after government-initiated media blackouts; the Philippines government resigned in 2003 (Rigby, 2008). Three occurred in 2009: the Iran post-election protests (Faris & Heacock, 2009), Moldova's "Twitter Revolution" (Hodge, 2009a), and unrest in Urumqi, China (World Movement for Democracy, c. 2009). Subsequently there was political unrest in Tunisia and Egypt in early 2011, where social media and mobile devices played a role (Bay, 2011; Kessler, 2011). Mobile phone SMS services were also used to distribute hate messages in Kenya during the 2008 election period (Okeowo, 2008); and were used to aid the orchestration of the 2010 food riots in Mozambique (Jacobs & Duarte, 2010).

The incidents described in this section illustrate the increasing asymmetric nature of conflict, and the roles that civilian communications technologies are playing in these conflicts. The trends will be discussed in more detail in Section 5.3.2, and the impacts of these trends on IW will be discussed in Section 5.3.3.

5.3.2 Conflict Trends

In the conflicts presented in Section 5.3.1, some did exhibit direct engagements between forces with modern equipment; however; the majority exhibited asymmetric warfare, with the use of civilian infrastructure and technology as the primary tools for the inferior party. The introduction of network warfare as a tool in conflict is also apparent.

A conflict may therefore have a technological complexity that can be divided into two broad categories: low-technology and high-technology. However, a conflict may transition between the two, or exhibit a mixture of the characteristics. These characteristics are shown in Figure 5.5. As example of a conflict is transitioning between the two complexities is the Iraq conflict; the initial coalition invasion exhibit force-on-force conflict. Subsequently, during the peacekeeping phase, the conflict has become an insurgency-type conflict, where improvised devices (such as IEDs) are driving the technological development of the superior forces, who struggle to counter such devices. The funding for research into jamming IEDs approximated US$ 6 billion in the 2006 fiscal year; procurement costs for these devices have exceed US$ 380 million since 2003 (Eshel, 2007). This

illustrates the impact an improvised device can have on the more advanced militaries. It should therefore be noted that improvised or low-technology solutions may be extremely effective at countering modern high-technologies.

- Unconventional, guerrilla tactics, possibility of high asymmetry.
- Use of readily available civilian equipment and systems.
- Improvisation using available equipment e.g. IEDs.
- Possibility of cyber-war and hacking (if infrastructure supports it)
- Use of civilian media.

- Conventional force-on-force, possibility of low asymmetry.
- Deployment of modern war-fighting technologies and introduction of new technology.
- Convergence of Information and Communication Technologies (ICT).
- High probability of related cyber-war & hacking.
- Use of civilian media.

Figure 5.5: Technological Aspects of Conflict, adapted from van Niekerk and Maharaj (2009c)

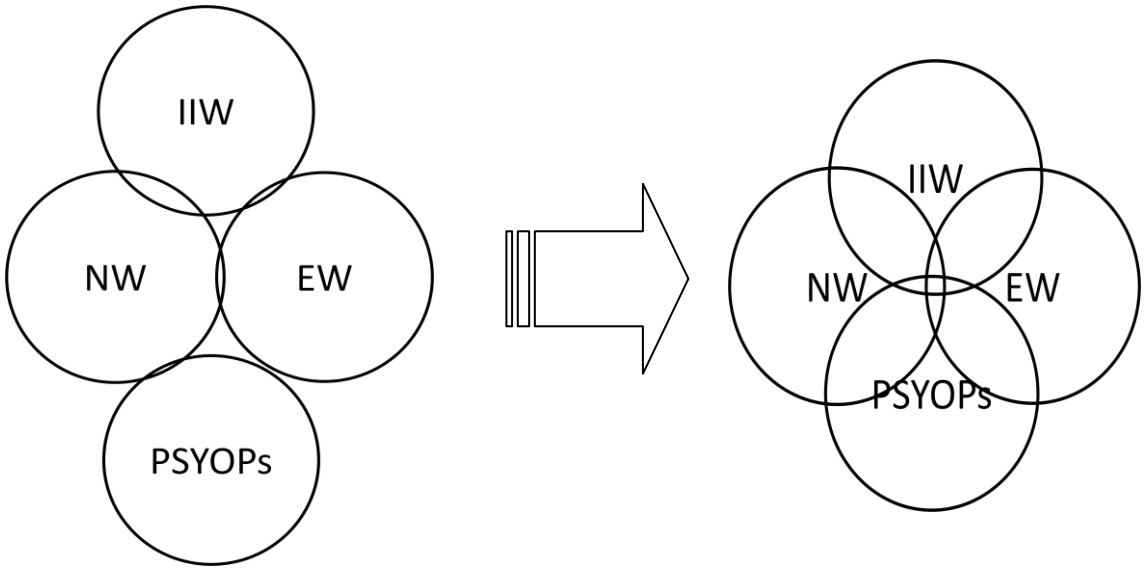
The conflicts exhibiting network warfare follow a high-technology route, where the convergence of ICTs can be readily seen. The conflict becomes largely virtual, where the actual attacks and counter-attacks are conducted across the Internet. The potential use of such an attack was seen in the Georgian conflict, where a DoS attack disrupted the Georgian communications during the initial stages of the Russian incursion. The mass anti-government demonstrations illustrate the fact that the ICT technologies become an enabler to the masses, who use these technologies to mobilise themselves and propagate their ideology.

The arising conflicts occur for two reasons: ideology, or disputes over territory. Ideological conflicts are more likely to be information-based; as the conflict intensifies physical forces may become involved. Information-based conflicts cannot take and hold territory, therefore any territorial disputes will constitute primarily of physical forces. However, their tactics and success may be governed by information-superiority, allowing them to out-manoeuvre the adversary.

5.3.3 The Impact on Information Warfare, and its Future Roles in Conflict

The conflict trends described above will have an impact on IW. The convergence of ICTs and the migration of mass-communications to computer-based systems, such as social networks and smart mobile devices, also results in the convergence of IW functional areas.

A result of ICT convergence is that mobile devices are becoming smarter: they have processors, mass storage, cameras, traditional telecommunications, data communications, and social networking applications. This combination of wireless communications technologies and the capability for both data and voice communications results in a convergence of electronic warfare, network warfare, and information infrastructure warfare. Similarly, the social media and mass communications over the Internet result in a convergence of psychological operations, network warfare, and information infrastructure warfare. The use of the broadcast media for the spreading of hate speech illustrates a convergence of psychological operations with electronic warfare, as the broadcasts could be jammed. This is illustrated in Figure 5.6.



Key:

EW – Electronic arfare
IIW – Information infrastructure warfare
NW – Network warfare
PSYOPS – Psychological operations

Figure 5.6: The Convergence of the IW Functional Areas

Just as the use of civilian technologies in conflict is impacting on the military, military-style technology is becoming available in non-military situations. Jamming (electronic warfare) is being used to combat the use of smuggled mobile phones in prisons (Hodge, 2009b); the threat of IEDs and illegal use of mobile communications may require the use of electronic warfare civilian safety

operations. Another example is the use of a man-portable air defence system to attack a DHL aircraft at Baghdad International Airport in 2003 (McKenna, 2007); this indicates a decreasing distinction between military and civilian technologies. This raises a potential ethical dilemma: when can civilian infrastructures be targeted, and for what reason? Typically the targeting of civilian infrastructures is viewed negatively (Ignatieff, 2001); however inaction when radio stations to continuously advocate genocide, as in Rwanda, may be viewed as more immoral. The use of IW tactics, where the broadcasts may be jammed or prevented without physical destruction may make the action more acceptable from a moral standpoint.

As cyber-space is global, and there is an ever-increasing demand on the electro-magnetic spectrum due to wireless communications, it is inevitable that there will be an overlap in military and civilian uses of the information sphere. Therefore it is highly likely that military operations in cyber-space will have some impact on the civilian usage of the information sphere.

The roles of IW may therefore evolve from the concept of information superiority in a traditional military conflict to one that is capable of addressing a wider range of threats; this may include the targeting of civilian infrastructures out of necessity during policing actions in low-intensity conflicts, peacekeeping operations, or mass uprisings by populations against national governments. The use of these tactics, particularly network warfare tactics, may be employed by opposing factions who become vigilantes in tense political situations for ideological or patriotic reasons. Likewise, the use of military IW technologies may be used to support civil safety and security in situations where non-state aggressors have superiority over security forces in the information sphere. Section 5.4 focuses on this aspect of IW; Sections 5.5 and 5.6 focus on the specific cases of the mobile phones and Web 2.0 technologies, respectively.

5.4 The Weaponisation of the Internet

This section presents a trend analysis of IW and security incidents related to computer networks. As before, it will consist of incident case studies; these will be more in-depth than those presented in Section 5.3. The case studies will be presented in Section 5.4.1, and secondary data analysis will be presented in Section 5.4.2. This section aims at illustrating trends with regards to incidents using IW tactics; this will provide information regarding the context and threats for the vulnerability framework. A previous version was published in van Niekerk and Maharaj (2010c).

5.4.1 Incident Case Studies

The incidents considered here range from 1998 to 2010, and include large-scale DoS attacks, major system penetrations, and major virus outbreaks. A timeline of the incidents is shown in Figure 5.7. Some were analysed in Section 4.2.7 and a summary will be provided; the remainder will be analysed using the IW Lifecycle Model.

From Figure 5.7, general trends can be seen. Large-scale DoS attacks appear to occur from 2007 onwards; whilst other examples exist, these are the only ones that were of national scale. There appears to be a decline of major viruses and worms that cause network disruptions; malware has shifted its focus to financial gain for criminals. System penetrations appear to be evenly spread over the considered time-frame.

5.4.1.1 Solar Sunrise

In February 1998, US Department of Defence systems were penetrated by a series of attacks; the subsequent multi-agency investigation was code-named Solar Sunrise (Cordesman, 2000; GlobalSecurity.org, 2011). The attackers hid their tracks, and it appeared that they were originating from multiple points across the globe (GlobalSecurity.org, 2011). The attacks were traced to two teenagers in California, led by another in Israel (Cordesman, 2000). This incident occurred during a period when the US was preparing for possible military action due to problems with the UN weapons inspections in Iraq; there was an initial concern that the attacks may attempt to disrupt deployments (GlobalSecurity.org, 2011).

The importance of this incident is that it is one of the first recorded cyber-based attacks, and illustrated that teenagers had the ability to compromise government and military systems; this confirmed the vulnerabilities and the lack of warning capabilities of a cyber-attack that an exercise codenamed "Eligible Receiver" found (GlobalSecurity.org, 2011).

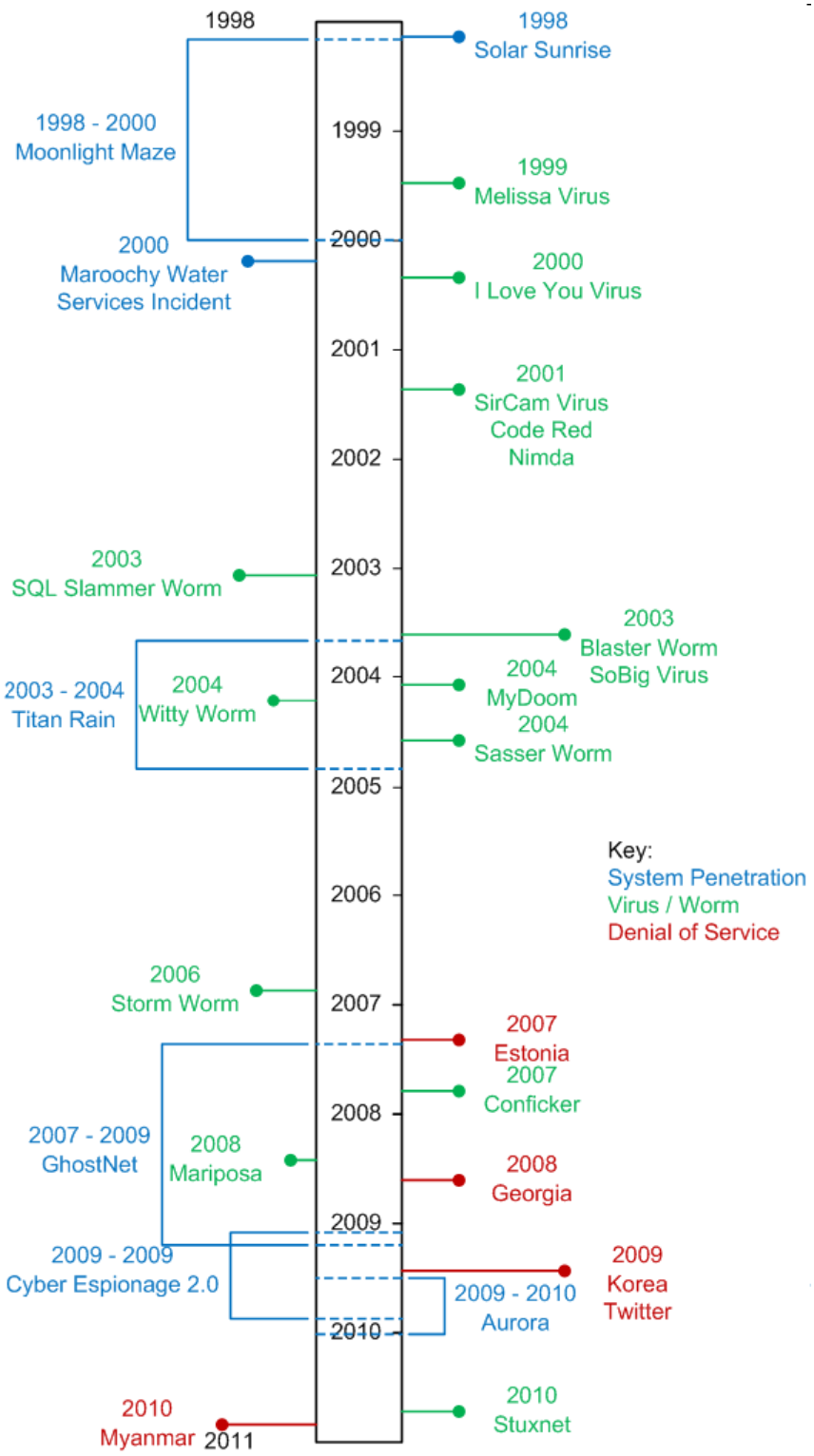


Figure 5.7: Timeline of Major Cyber-Incidents

5.4.1.2 Moonlight Maze

This is a series of attacks that began in March 1998 and lasted approximately three years; the first official report was in October 1999, and the incidents were codenamed "Moonlight Maze" (Adams, 2001; Cable News Network, 2001; Cordesman, 2000). At the time this was the largest sustained attack on the US through the Internet, and appears to have originated from Russia; the targets included military, Department of Energy nuclear research laboratories, and the National Space Agency (Cable News Network, 2001; Cordesman, 2000). The timing and source of the attacks led experts to believe that they were state-sponsored (Cordesman, 2000). Large quantities of information were copied, and backdoors left for future access; as a result, the US Department of Defence ordered new encryption, and upgraded intrusion detection systems and firewalls (Adams, 2001; Cordesman, 2000).

The motivation appeared to be industrial espionage to gain technological information; hackers were used in network warfare to penetrate systems and extract the information. The US Department of Defence upgraded its network defences to mitigate the possibility of future successful attacks. The importance of this incident is it again illustrated the vulnerabilities to this type of attack, and is the first recorded incident of such a magnitude that appears to be state-sponsored espionage.

5.4.1.3 Maroochy Water Services

This incident was analysed in Section 4.2.7.5. To summarise, a disgruntled former employee used stolen equipment to penetrate sewerage works in Australia, and released raw sewerage into the public waterways. This incident has been used as the main example for an attack on infrastructure and the vulnerability of infrastructures to attack. The Stuxnet incident has further illustrated the possibility of cyber-based attacks on infrastructure, and will be discussed in Section 5.4.1.13.

5.4.1.4 Titan Rain

In 2003 to 2004 there were a series of system penetration into the US government, research facilities, and the military; these penetrations were given the codename "Titan Rain" (Thornburgh, 2005a). The targeted systems would be methodically commandeered by the attackers, who would then copy as much information (in terms of computer files) as they could onto temporary storage in South-East Asia; these files would then be transferred from the temporary storage to servers in the Chinese mainland (*ibid.*). Beginning during the night of 1 November 2004, an intense period of intrusions occurred where four military systems were attacked within a twelve hour period (Espiner, 2005). Among the stolen files was software for flight planning, and military helicopter specifications; nothing was secret, yet the information is controlled by strict export restrictions

(Espiner, 2005; Thornburgh, 2005b). From the reports, many are certain that the attacks were conducted, or sanctioned, by the Chinese government; however this very difficult to prove (Thornburgh, 2005b). It appears that in an attempt to defend the systems, the Titan Rain servers were counter-hacked; however, the person who was counter-hacking the servers, investigating the attacks, and passing the information onto the relevant authorities, lost his job as hacking was illegal in the US, and it could not be determined if his actions were sanctioned by the authorities. During later investigations, the Chinese government did not co-operate with the US investigators (*ibid.*).

Using the IW Lifecycle model, the motivation for the attacks appears to be intelligence gathering and industrial espionage. The functional areas are therefore using network warfare to conduct intelligence gathering. The attack used expert hackers to penetrate systems, and copy files. A defence was mounted, however this was hindered by the US's own laws, and the Chinese government refusing to co-operate. What is important in this case is the effective use of hacking to gather intelligence and penetrate military networks. This could be used in a conflict situation where strategic and tactical information is required.

5.4.1.5 Estonia

This incident was described and analysed in Section 4.2.7.1; therefore a summary is provided here. A botnet-based DDoS attack was launched against Estonia in 2007, apparently by ethnic Russians who were offended by the relocation of a war-memorial. The attacks occurred over a period of three weeks, and government, financial, and media websites were targeted. The importance of this case is it is the first illustration that a nation's networks and function could be severely hindered by a large-scale attack on computer networks over the Internet.

5.4.1.6 Georgia

Georgia was also the focus of a DDoS attack in 2008; the attack occurred just before Russian military forces entered the Georgian-South Ossetia conflict in support of the South Ossetians; the Russian government denied allegations that they were responsible for or supporting the attacks, and claimed that they were also a victim of DDoS attacks (Hart, 2008). The results of the attacks included internal and external communication difficulties for Georgia; in addition Georgian websites were also defaced (Coleman, 2008b). The traffic generated by the DDoS attack was estimated at approximately 814 Mbps (Labovitz, 2010). The attacks occurred at an opportune moment for the Russian military, as due to the lack of communication by the Georgians, Russian opinion dominated the media regarding the conflict.

Using the IW Lifecycle model, assuming the DDoS attacks were sanctioned by the Russian government, the motivation would be to hinder Georgian communications in support of a military incursion, conduct psychological operations against the Georgians (through web defacements), and dominate the international perspective on the conflict by denying the information flow from Georgia. Botnets were used as a tool to conduct network-warfare, which supported psychological operations and command and control warfare. This incident illustrates the potential of using a DDoS attack (network warfare) via the Internet to support physical military actions.

5.4.1.7 The GhostNet Cyber-Espionage Attacks

The Information Warfare Monitor (2009) investigated a cyber-espionage network, which they named GhostNet. Computers were compromised by using social engineering and email attachments with malicious code to exploit vulnerabilities; these computers could then be mined for information. The retrieved information could then be used to further propagate the infection as legitimate documents (such as meeting minutes) would be circulated with malicious code (Information Warfare Monitor, 2009). The first recorded infections dated from May 2007, with spikes in December 2007 and August 2008, and lasted until March 2009; approximately 30% of the estimated 1300 infected computers across 103 countries were considered high-value targets. The ultimate target appears to be the Office of the Dalai Lama and organisations or political representation that has interaction with the office; the origin of the attacks appears to be in China (Information Warfare Monitor, 2009). Symantec Security Response released an online video illustrating the tools and the capability of espionage network; the attackers could take full control of an infected computer and monitor any activity on it (Symantec Security Response, 2009). The investigation began by request due to suspicions of system penetration; during the investigation the infections were removed (Information Warfare Monitor, 2009).

Using the IW Lifecycle model, the motivation for the attacks is political espionage, in the context of political tensions between the office of the Dalai Lama and China. Malicious documents and social engineering were used to conduct network warfare, and ultimately gather intelligence. The investigation also removed the infection, thereby defending against it. This incident further illustrates the use of the Internet in mass remote espionage.

5.4.1.8 DDoS Attacks on South Korea and the United States

In July 2009 a series of DDoS attacks that appeared to originate from compromised systems located across sixteen countries were used to target websites in South Korea and the United States over a period of days (Chan-Kyong, 2009; South African Press Association, 2009b). Compared to the

attacks against Estonia and Georgia, this did not appear to have a large impact; however it illustrates the potential of an individual, group, or nation to anonymously attack systems in multiple nations.

5.4.1.9 DDoS Attacks on Twitter

In 2009 a number of social networking websites were subjected to a DoS attack; Twitter was the worst affected and was inaccessible for a number of hours (Menn & Gelles, 2009). This attack appears to be related to the Russia-Georgia conflict in that the attack appears to have been aimed at silencing a pro-Georgian blogger by Russian hackers (Miguel, 2009). A few days later, a second DDoS attack targeted Twitter; on this occasion it appears to be related to the DDoS attacks on the websites in South Korea and the United States (Adhikari, 2009).

The motivation for both the attacks appears to be silencing bloggers from making politically sensitive comments; the context is from previous political or ideological conflict. It can be assumed that botnets were again the tool used to conduct network warfare. Subsequent to the attacks, Twitter has improved its resilience to DDoS attacks. These attacks indicate that social websites may also be targeted due to one or more subscribers making politically sensitive comments. This confirms that the broader context is important when considering IW attacks.

5.4.1.10 The Shadow Network: Cyber-Espionage 2.0

This appears to be a second iteration of cyber-espionage originating in China; these attacks utilised free social media websites and email, such as Google, Yahoo! Mail and Twitter, as part of the command-and-control structure of the espionage network in order to "maintain persistence" (Information Warfare Monitor and Shadowserver Foundation, 2010). The Office of the Dalai Lama again appears to have been targeted as 1500 letters sent by the office between January and November 2009 were recovered; in addition a number of documents from the Indian government, some marked secret, and visa applications to the Indian representation in Afghanistan were recovered (*ibid*.).

As with GhostNet, the motivation appears to be political espionage, in a context of political tension. This signifies the use of freely available online public communication and social applications as part of the espionage network. This further illustrates the use of the Internet to conduct mass espionage.

5.4.1.11 Operation Aurora: Cyber-Espionage on Google

During the period when Google was threatening to cease operations in China due to censorship concerns, it was noticed that breaches had compromised Google's systems in what appeared to be state-sponsored corporate espionage emanating from China (McMillan, 2010). The attack type is known as an advanced persistent threat, and is in some ways similar to the GhostNet and Shadow Network espionage attempts; the McAfee team investigation the breaches of Google and other corporations named this attack "Operation Aurora" (Kurtz, 2010). As with the GhostNet espionage network, the attackers could gain complete control of the infected computers (South African Press Association, 2010). At the same time as the details were unfolding, a DoS attack was directed at lawyers involved in a software piracy case against China (*ibid*.).

The motivation appears to be corporate and political espionage in a context of a tense political, economic, and corporate atmosphere. Network warfare attacks using the advanced persistent threat were employed to gain intelligence. As in previous cases, the investigation sought to recover and prevent these attacks. This further illustrates the use of the Internet as a vector for espionage; and the growing number of such attacks emanating from China is resulting in growing concern.

5.4.1.12 Myanmar/Burma

A DDoS attack against Myanmar (previously Burma) appears to have begun on the 25 October 2010, and peaked on the 1 November; the generated traffic was estimated to be in the region of 10 to 15 Gbps (Labovitz, 2010; Ragan, 2010). As the nation's external connectivity consists of 45Mbps terrestrial and satellite links, the nation's connectivity was easily overwhelmed. The motivation for this attack appears to be political, as this occurred just prior to the country's general elections, and the government has been known sever the Internet connectivity. Anti-government websites hosted outside of the nation were targeted by DDoS attacks earlier in 2010 (Labovitz, 2010).

The motivation for the attacks appeared political; due to the scale of the attack it can be assumed that a large botnet was used to effectively deny international connectivity. The scale of the traffic flood should be noted; many nations would be hard-pressed not to have severe network degradation due to an attack of this intensity.

5.4.1.13 Malware

From Figure 5.7, there is a noticeable decrease in major malware outbreaks; the only noticeable incident was the Stuxnet worm, and this is due to its advanced design rather than sheer quantity of

infections. Table 5.4 lists the most expensive malware in terms of estimated financial impact, which is usually due to lost productivity and clean up (Kretkowski, 2007; Marquit, 2010).

Table 5.4: Costliest Malware, sources: Kretkowski (2007) and Marquit (2010)

Name	Year	Impact (US$)
Morris	1988	10 million
Blaster	2003	320 million
Sasser	2004	500 million
Nimda	2001	635 million
SQL Slammer	2003	750 million
SirCam	2001	1 billion
Melissa	1999	1.2 billion
Code Red	2001	2 billion
Conficker	2007	9.1 billion
ILOVEYOU	2000	15 billion
SoBig	2003	37.1 billion
MyDoom	2004	38.5 billion

In addition to its financial impact, the speed at which the SQL Slammer worm spread was phenomenal; in half an hour it had infected many countries across all continents, and is shown by the interactive timeline (PBS.org, 2003b). The Witty worm of 2004 was the first known to be specifically designed to attack network security software. This attack was vendor specific to the product family of IBM Internet Security Systems; this limited its overall damage, even though it carried a destructive payload which gradually overwrites the hard-drive of infected PCs (Kretkowski, 2007). The Storm worm of 2006 was used to infect computers and turn them into bots, used to send spam; many versions tricked potential victims into downloading the malware with the use of fake links to online news reports or videos (Strickland, 2008).

In 2009 there was a resurgence of the Conficker worm; reports indicate that British and French military systems were infected, causing widespread outages (Kirk, 2009; Willsher, 2009). There were reports that British warships were affected (Kirk, 2009) and that French fighter aircraft were prevented from taking off due to the infections (Willsher, 2009). This incident illustrates the possible use of malware to disrupt military systems and hinder war-fighting capability.

The Mariposa botnet has also been considered as the worst malware of all time; it was estimated to have infected approximately 12 million PCs and stole credit card and online banking details

(Associated Press, 2010). It appeared in late 2008, and spread through over 190 countries; those arrested by Spanish police in connection with some of the larger botnets bought this on the black market (Associated Press, 2010).

Other versions of credential stealing malware are the Zeus series and SpyEye Trojans; these were originally rivals, but there were plans to merge the two into a single, powerful kit. There were also reports that existing clients of Zeus would receive a discount when purchasing SpyEye (Krebs, 2010). Stevens and Jackson (2010) provide an in-depth report of the Zeus Trojan, which illustrates how advanced the Trojan was; the most expensive version was selling for approximately US$ 3000 to US$ 4000. The Zeus malware also migrated to mobile platforms to target mobile banking (Kitten, 2010). The Rustock botnet was estimated to control over one million bots, making this the largest single botnet in 2010; the cost of hiring ten thousand bots was US$ 15 in 2010 (Symantec Corporation, 2011a). This indicates an underground economy based on the production and hiring of malware used for cyber-crime, spam, and DDoS attacks. Occasionally the kits for the malware are made freely available online: the Zeus code eventually appeared for free, followed a few weeks later by the "Black Hole" exploit kit (Fisher, 2011c).

The Stuxnet worm of 2010 was extremely advanced: it exploited four zero-day vulnerabilities, had multiple propagation methods, and utilised stolen digital certificates; it also is the first malware to specifically target industrial control systems (Falliere, O Murchu, & Chien, 2010; Keizer, 2010; Matrosov, Rodionov, Harley, & Malcho, 2010). Despite this, some experts believe there were mistakes, and that the worm could have been far more effective (Fisher & Roberts, 2011). The infection statistics of the worm were unusual: over 50% of the infections occurred in Iran (Falliere, O Murchu, & Chien, 2010; Keizer, 2010; Matrosov, Rodionov, Harley, & Malcho, 2010); and the targeted Siemens programmable logic controllers were used in an Iranian nuclear facility which was affected by the worm (Keizer, 2010; Moyer, 2010). This leads many to believe that the facility was the ultimate target of the worm, and that due to its sophistication, it was created by a state-sponsored group (Fisher & Roberts, 2011; Keizer, 2010; Moyer, 2010). The ability to spread through USB drives allows the virus to cross over air-gaps into sensitive industrial networks, and the interference of the control systems may result in physical damage to the equipment. This incident is important as the capability to attack infrastructure through pseudo-targeted malware (in that it is product-specific) has been clearly demonstrated. There are also reports that the code for the worm is available to criminal elements (Kiley, 2010).

From Figure 5.7 and Table 5.4, it can be seen that the period from 1999-2004 exhibited the bulk of the damaging malware; subsequently, the malware appears to be focussed more on creating botnets for use in cyber-crime; there appears to be an online black market economy based on these botnets. The impact of Conficker on military systems in 2009 and the Stuxnet incident in 2010 illustrate that the use of malware in a military network warfare scenario is no longer theoretical; the capability to target and affect both infrastructure and military information systems has been clearly demonstrated.

5.4.1.14 Other Incidents

This section presents examples of additional incidents; some of these incidents (or reports thereof) were released late in the study, and are therefore not analysed in-depth, but are included for completeness.

In 1994 hackers accessed a US Air Force Research centre, known as Rome Labs, through the use of sniffer programs; from there they accessed other government networks (Cordesman, 2000). Initially the investigators were content with monitoring the hacking activities to determine the source; one was found to be living in the UK, and the relevant authorities were contacted. Eventually the hackers used the Rome Labs systems to penetrate a Korean nuclear facility and copy information; this caused a panic as it was not immediately apparent if the facility was in North or South Korea. A few days later a teenager in the UK was arrested and admitted to participating in the attacks. The US Air Force lost over US$ 200,000 in the attack, not including costs for the investigation, monitoring, and recovery (Cordesman, 2000).

In 2001, suspicious intrusions were noticed in the systems of Mountain View, California; similar intrusions were found throughout the US and appeared to originate from South East Asia and the Middle East (PBS.org, 2003a). This appears to be related to evidence of monitoring of the US infrastructure uncovered when Al Qaeda computers were seized and examined after the 9/11 attacks (PBS.org, 2003a).

Internal political tensions may also exhibit the use of cyber-based attacks: a series of hacking attacks and DDoS attacks occurred during both the 2005 elections in Kyrgyzstan (Open Net Initiative, 2005) and the 2006 elections in Belarus (Open Net Initiative, 2006). These attacks resulted in the websites of the media, non-government organisations, and political parties becoming inaccessible. International political tensions also result in spates of web-defacements; an example occurred during the NATO air strikes on Serbia (Hutchinson & Warren, 2001). In 2009 and 2011, a

series of anti-government protests occurred; these protests made use of mobile technology and online social networks to co-ordinate activity and distribute information. The 2011 demonstration in Tunisia and Egypt was analysed in Section 4.2.7.6. A website known as Wikileaks was releasing compromised military and diplomatic information, which eventually resulted in a series of vigilante DoS attacks; this was analysed in Section 4.2.7.4.

In August 2011 a report was released detailing intrusions into many international organisations over a five-year period; a total of 72 victims were listed in the report. The systems of the organisations were compromised using the advanced persistent threat, similar to the Google Aurora attacks; this series has been named "Operation Shady RAT" (Alperovitch, 2011). Although the report did not name the origin of the attacks, China is suspected of conducting the espionage (Nakashima, 2011). In addition to this, 2011 also exhibited a number of other significant system penetrations and attacks, some of which may be related to Operation Shady RAT:

- The International Monetary Fund was reportedly hacked by a nation state (Kitten, 2011; Paul, 2011);
- Systems of three departments in the Canadian government were penetrated by an attack that appeared to originate in China. This included financial and defence research department (Weston, 2011);
- The French Ministry of Finance confirmed computers were compromised, and apparently connected to China (Roberts, 2011a);
- Malware was planted on the NASDAQ web portal (Leyden, 2011);
- The London Stock Exchange reportedly suffered attacks (Goodin, 2011a);
- Sony was the victim of multiple penetrations, most notably the PlayStation Network (Kitten, 2011; Paul, 2011);
- Google uncovered a campaign to compromise email accounts of Chinese political activists and officials in the US and Asia, media, and military personnel (Kitten, 2011; Paul, 2011);
- Epsilon, an email marketer, had its subscribers details exposed after its servers were penetrated (Kitten, 2011; Paul, 2011);
- Details of CitiGroup cardholders (in the US) were exposed after a penetration through the web portal (Kitten, 2011; Paul, 2011);
- Iran reported a second malware-based cyber-attack in April 2011 (Dareini, 2011);
- A report indicates a rising number of attacks against critical infrastructure organisations, particularly for ransom (Mills, 2011);

- An infection in a Massachusetts Department of Labour and Workforce Development by the Qakbot worm was observed copying 200 MB of information each day during the infection (Roberts, 2011b);
- RSA's SecurID authentication product was compromised by a advanced cyber-attack (Kitten, 2011; Paul, 2011);
- Lockheed Martin (a defence contractor) experienced attempted penetrations related to the SecurID hack, but it was reported that no data was compromised (Kitten, 2011; Paul, 2011);
- L-3 Communications (also a defence contractor) experienced attempted penetrations related to the SecurID hack (Poulsen, 2011);
- Northrop Grumman (another defence contractor) suspected a cyber-attack related to the SecurID hack (Kaplan, 2011);
- The Oak Ridge National Laboratory in the US reported an advanced persistent threat attack similar to the one used against Google and RSA (Munger, 2011);
- The Zimbabwe Stock Exchange website was hacked twice, apparently to be used to host malicious content (Kabweza, 2011);
- The Hong Kong Stock Exchange suffered disruptions due to hack attempts (Subhedar & Leung, 2011);
- Hacker groups LulzSec (responsible for the Sony attacks) and AntiSec also target other websites, such as the US Senate, Central Intelligence Agency, and Apple (Sherr, 2011);
- A Japanese military contractor, Mitsubishi, was a victim of "hack attack" in September 2011, where information was stolen from infected systems (Savitz, 2011);
- A certificate authority DigiNotar was breached and the private key used for digital certificates was compromised. Counterfeit certificates were then distributed, indicating that this attack may breach other victims other than the initial attack (Chabrow, 2011);
- In October 2011 there were reports that key-logger malware had infected the US Air Force systems that are used to control and pilot unmanned aerial vehicles (Roberts, 2011d; Shachtman, 2011);
- In October 2011 malware was discovered that appears to be strongly related in the Stuxnet worm (Symantec Security Response, 2011).

These incidents illustrate the early vulnerabilities to penetration and potential espionage; similar attacks are still occurring. There is also more indication that cyber-attacks appear to be strongly

linked to political tensions and competition. The infection of the US Air Force systems further illustrates the applicability of malware to military systems and IW operations.

5.4.1.15 Discussion of Incident Trends

From the incidents presented in Sections 5.4.1.1 to 5.4.1.14, trends can be seen. The initial worms in the early 2000s resulted in degradation of network services and financial impact due to hindered productivity and recovery; this form of malware has given way to botnets, which can be used to steal details for cyber-crime, send spam messages, or conduct DDoS attacks. The major targeted DoS attacks that affected national connectivity have only recently occurred since the advent of the botnets. The low-key DoS attacks against websites are common (Labovitz, 2010); it is the size of the botnets that provides the capability to severely disrupt networks on a national level. Similar technology also appears to have been used in widespread cyber-based espionage.

Whilst many attacks appear to originate from one specific nation, that government may not be involved; it could theoretically be another nation with advanced network warfare capabilities using compromised servers in China. The Stuxnet worm illustrated that malware can be used to target and affect infrastructure; Conficker affected military systems. China and other nations consider network warfare as a first-strike weapon to be used to cripple military deployments or response in the event of a conflict (Mulvenon, 1998). Whilst most of the malicious activity can be attributed to crime, there is growing recognition that the Internet is becoming "weaponised" (van Niekerk & Maharaj, 2010c) or 'militarised' (Habib, 2011). The Internet is likely to be increasingly used for espionage and attack purposes. Reports by Crowdleaks (the successor to Wikileaks) indicate that the US military may have been seeking to develop a rootkit (laurelai, 2011).

Of the incidents, the majority compromised the confidentiality of information; then second came the DoS attacks. This is consistent with Hayden (2010), who claims that the objective should be to control or monitor a competitor's information; if this is not possible then deny them the information. The DoS attacks also appear to be linked to cases where groups want to openly display political dissatisfaction. Espionage networks require stealth, and therefore are less overt. The incidents also confirm the need to consider the broader context when dealing with IW. The rate of system penetrations continues to indicate there are vulnerabilities in many websites and infrastructures; a sufficiently concerted attack should be able to succeed in its objectives to some degree.

5.4.2 Secondary Data Analysis – CSIRT Data

This section presents the analysis of secondary data from various national CSIRTs; the raw data used in the analysis is freely available on the websites or the annual reports of the respective CSIRT. Many other CSIRTs exist, however their data is not made available to the public. Figure 5.8 shows the total number of recorded incidents each year for the CSIRTs; the actual quantities are not as important as the trends. Certain categories, such as spam, were not considered. All the plots in Figure 5.8 show an exponential increase; some then peak and show a decline in the number of incidents. For Brazil and Malaysia the number of incidents at the time of typing in 2011 has already exceeded the 2010 number (CERT Brazil, 2011; Malaysian CERT, 2011).

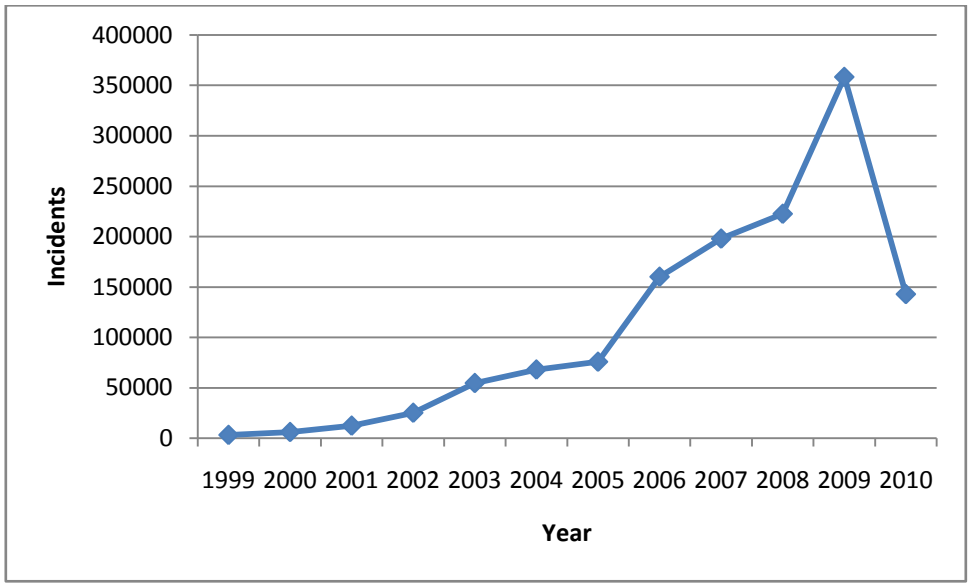


Figure 5.8 (a): Brazil, source: (CERT Brazil, 2011)

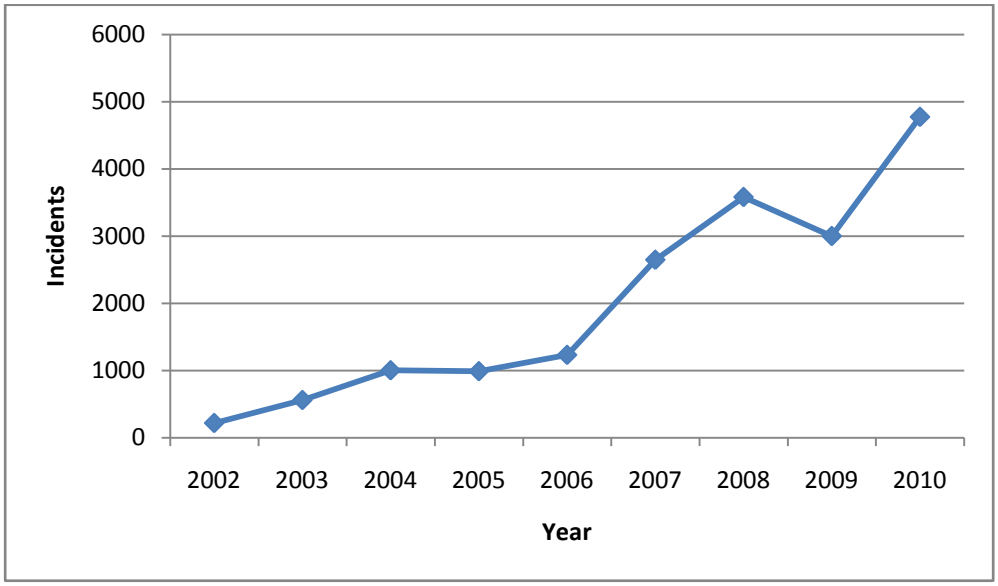


Figure 5.8 (b): Finland, source: (CERT-Finland, 2011)

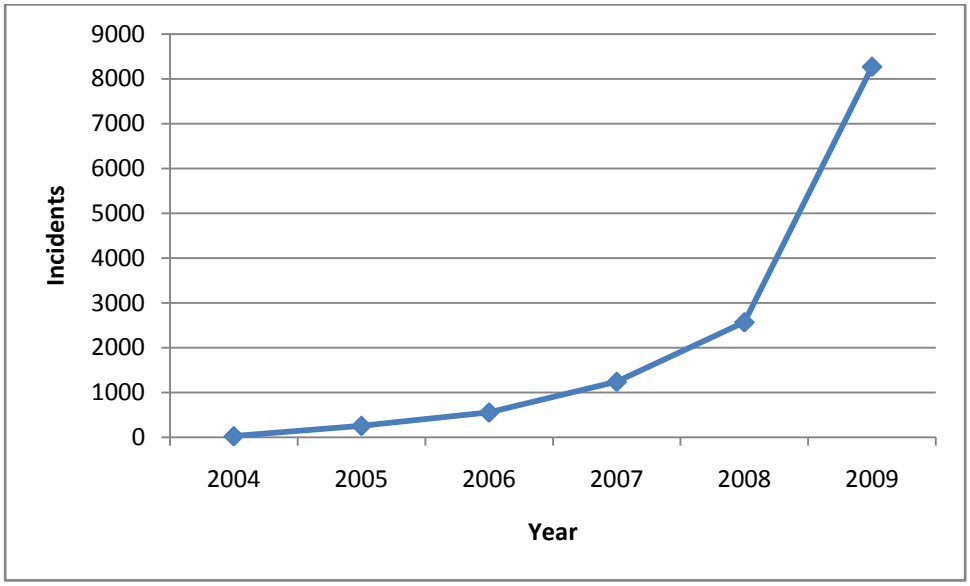


Figure 5.8 (c): India, source: (Indian CERT, 2011)

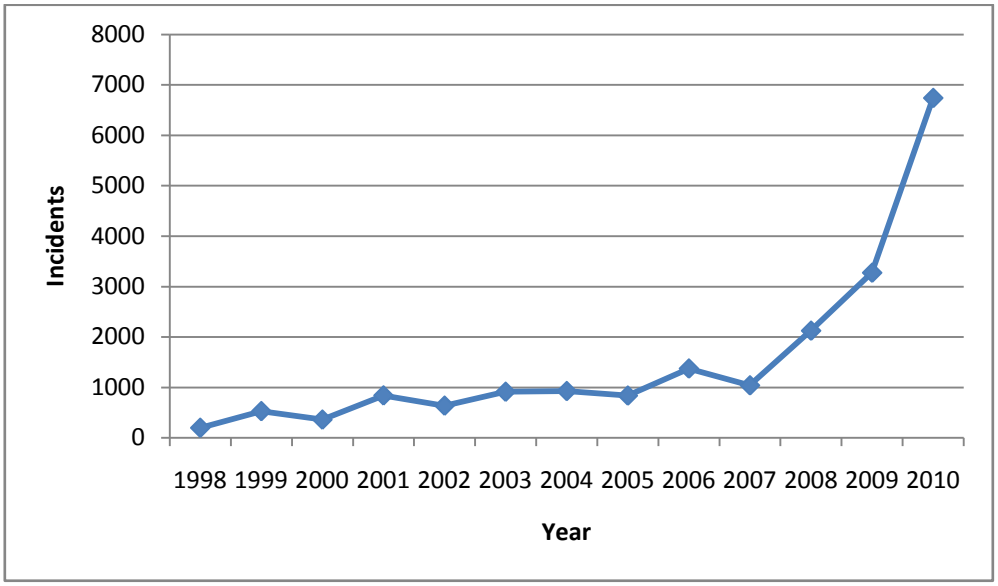


Figure 5.8 (d): Malaysia, source: (Malaysian CERT, 2011)

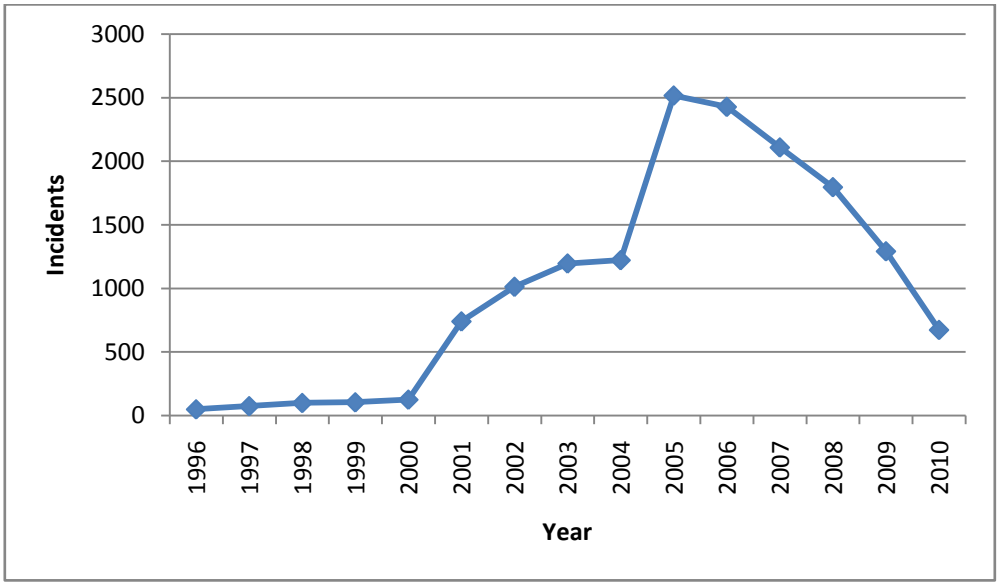


Figure 5.8 (e): Poland, source: (CERT Poland, 2011)

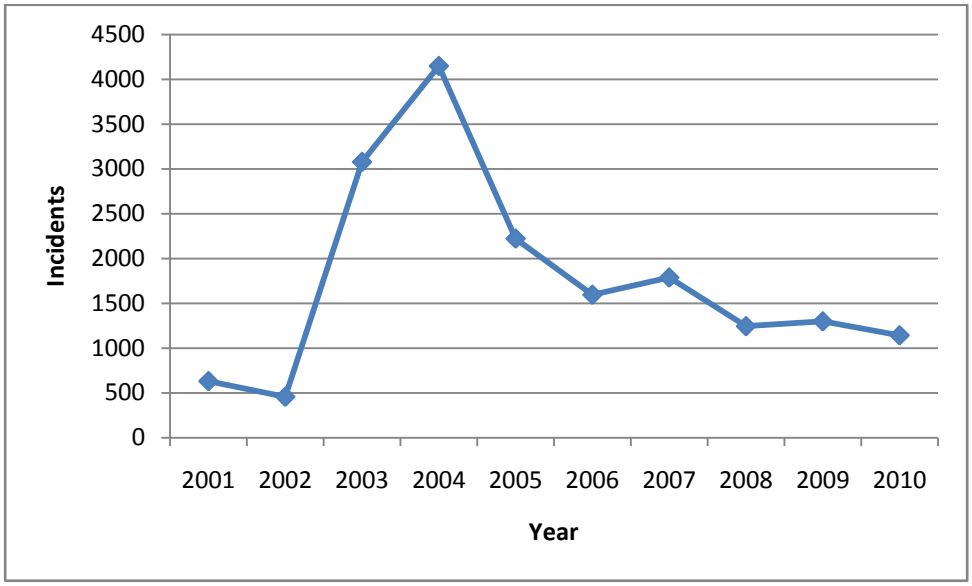


Figure 5.8 (f): Hong Kong, source: (Honk Kong CERT, 2011)

Figure 5.8: Total Number of Recorded Incidents per Annum for Various National CSIRTs

Table 5.5 shows the most prevalent reported incident types for each CSIRT, where 1 is the most prevalent, and 5 is the least prevalent of those considered. The Netherlands was introduced, but was not considered in Figure 5.8 as absolute amounts were not provided; incidents were listed by percentage of the total. Hong Kong data was not used in Table 5.5 as it is only categorised into security incidents and virus incidents. To determine the overall prevalence, values are assigned to the categories according to their ranking, and added (top ranked is assigned a value of five, lowest ranking a value of 1). From this, the five most prevalent reported incidents are (in order): malware, fraud, intrusions and intrusion attempts, scanning, and website attacks. It should be noted that DoS attacks was the sixth most prevalent reported incident type for the CSIRTs of Finland, Malaysia, Poland, and joint sixth for the Netherlands. For Brazil intrusions were ranked sixth and DoS was seventh.

This indicates that malware is still a common problem, and there are a large number of attacks that are aimed at penetrating systems or are scanning, which could be planning an attack. As discussed in Section 5.4.1, recent trends in malware allow them to be used for system intrusion and DoS attacks; therefore the prevalence of malware may be linked to the other reported incidents. As malware is so prevalent, it can be said that the Web is being weaponised; mostly for cyber-crime, however these tools can be used for cyber-warfare and espionage.

Table 5.5: Top Five Ranked Incidents by Prevalence in 2010, sources: CERT Brazil (2011); CERT Finland (2011); Indian CERT (2011); Malaysian CERT (2011); CERT Netherlands (2011); CERT Poland (2011); van Niekerk and Maharaj (2010c)

	Brazil	Finland	India (2009)	Malaysia	Netherlands (2009)	Poland
1	Scanning	Malware	Website compromise, Malware & Viruses	Intrusion and Intrusion Attempts	Malware	Fraud
2	Fraud	Social Engineering	Phishing	Fraud	Vulnerabilities	Offensive Content
3	Worm	Vulnerabilities	Scanning	Malicious Code	Other	Malicious Software
4	Web Server Attacks	System break-in	Others	Harassment	Phishing	Information Collection
5	Other	INFOSEC problem	Denial-of-Service	Vulnerabilities	Hacking	Intrusion Attempt

5.5 Mobile Device and Mobile Infrastructure Incidents

This section discusses incidents regarding mobile phones and the mobile infrastructure. This will be split into two main areas: incidents regarding attacks or misuse of mobile devices or infrastructure, and trends in malware specific to mobile devices. The objective of this section is to identify vulnerabilities and threats from trends in incident reports; this aligns with the study objectives of gathering information in these areas, and then using it in the vulnerability framework. The possible roles of mobile devices and infrastructure in IW will be presented.

5.5.1 Incident Trend Analysis

This section presents the incidents regarding attacks on mobile devices or infrastructure, or misuse of legitimate functionality. Some of the incidents are potential vulnerabilities that have been raised through academic research. A previous version of this section was presented in van Niekerk and Maharaj (2010b).

5.5.1.1 Attack by a Disgruntled Employee

In 1999 the Vodafone messaging network was hacked into by an individual who was disgruntled with his employees; the attacker used the access to send illegitimate SMSs to more than 30,000 international subscribers (Jones, Kovacich, & Luzwick, 2002; Weaver, 1999). The messages claimed that the recipients had won a car, and the attacker's employer should be contacted to claim the prize; the flood of calls blocker the organisations switchboard and severely disrupted business,

resulting in an estimated financial impact of £10,000 (Jones, Kovacich, & Luzwick, 2002; Weaver, 1999). Using the IW Lifecycle model, the motive of the attack was revenge; it appears that a network-based attack was conducted to gain illegitimate access to the mobile infrastructure, which was put to malicious use. As with the Maroochy Water Services incident (Section 5.4.1.3), this incident illustrates that someone with knowledge of the systems can gain illegitimate access; it can therefore be deduced that there are threats to the mobile infrastructure, and that a vulnerability was exploited.

5.5.1.2 The Athens Affair: Espionage on Greek Mobile Phones

In January 2005 it was detected that attackers had gained access to and manipulated network components of Vodafone Greece, allowing them to eavesdrop on more than 100 high-level dignitaries, including the Greek Prime Minister (Prevelakis & Spinellis, 2007). It appears that the attack first occurred just prior to the Athens Olympic Games in August 2004; due to the sophisticated nature of the attack, it was unclear if the system was penetrated from the outside, or there was insider assistance. It is also unclear if the eavesdroppers made recordings of the compromised calls (*ibid*.). The attack was detected when malicious software was discovered on four mobile switching centres (MSCs); the code subverted the legitimate wiretapping capabilities of the MSCs, which created a copy of the phone call that was sent to other mobile phones. An SMS was also transmitted to the attackers providing location information of the original caller (*ibid*.).

As the MSCs are the core of a mobile network, there are advantages to compromising them: the signal through them is not encrypted, whereas the GSM and 3G wireless signals are encrypted; and the MSCs handle the majority of the voice traffic. However, the process to compromise the MSCs was complex: the rogue software had to be installed; remote access was required to add or change the target mobile phone numbers; it needed to remain hidden, therefore it had to circumvent system activity logging and prevent system administrators from discovering the activity. This process is described in details by Prevelakis and Spinellis (2007).

An in-depth knowledge of the process is not required for this study; the fact that such eavesdropping was conducted illustrates that there are vulnerabilities in the mobile infrastructure that can be exploited to monitor mobile communications, and possibly compromise very sensitive information. The motivation of this attack appears to be espionage; with some network warfare aspects being used to control the rogue software. The possibility of insider assistance illustrates the potential threat of malicious insiders in a telecommunications company. It should be noted that legitimate wiretapping functionality was exploited; this is similar to what will be required for

mobile phone networks to implement in South Africa due to the Regulation of Interception of Communications Act (RICA, 2002). Such legitimate functionality may therefore provide attackers the opportunity to intercept mobile communications.

5.5.1.3 The SMS Banking Scandal

In July 2009 it was discovered that a criminal group was intercepting online banking one-time passwords in South Africa; this allowed them to gain access to the accounts, and it is estimated that they stole over ZAR 7 million (van Rooyen, 2009). Potential targets were identified through a phishing scam, and a Vodacom engineer was coerced into assisting the gang; he created duplicate SIM cards which allowed the interception of the SMS containing the one-time password (Dingle, 2009; van Rooyen, 2009). The motivation for this attack was personal gain; some form of psychological operation (social engineering) was employed to coerce the engineer into assisting the gang. As the ultimate target was online banking accounts; this incident illustrates the use of the mobile infrastructure to compromise financial services that make use of mobile communications for security features. The relevance of the insider threat in the mobile telecommunications is further illustrated.

5.5.1.4 The GSM Project

This project used distributed computing to generate a look-up table that would allow an eavesdropper to break the A5/1 stream cipher that is employed to encrypt voice communications in the GSM wireless link (Nohl & Paget, 2009; Ragan, 2009). Whilst the technology required was demonstrated by Nohl and Paget (2009), the GSM Alliance estimates the required look-up table will be 2 TB in size, in addition to the equipment required to intercept the wireless signal (Ragan, 2009). In addition to this, the attack will need to be within range to be able to intercept the target signal; this method will probably not be able to conduct mass interceptions such as The Athens Affair. The motivation of the project was not malicious; it intended to illustrate vulnerabilities is the employed encryption to coerce mobile providers to improve the encryption of their networks (Nohl & Paget, 2009). Due to the complexities of this attack it will be beyond most individuals; governments and intelligence agencies will have access to more sophisticated eavesdropping capabilities so this method would not be required. The methods employed in The Athens Affair and SMS Banking Scandal will probably be more efficient than the method proposed in this section.

5.5.1.5 Exploitation of SMS Service for Denial of Service Attacks

Enck *et al*. (2005) illustrate the potential for conducting a DoS attack on mobile services in a localised area through flooding the network with SMS messages; this will deny both SMS and voice

services. As the SMS service uses a control channel to transmit the message, a flood of messages may prevent the control channel from being allocated to voice calls; there is also the possibility that the switching stations in the network may become saturated. It is proposed that web-based SMS functionality (through External Short Messaging Entities (ESME)) may be compromised and used to flood the mobile network. It was calculated that 240 messages per second would be required to disrupt Washington, D.C., 165 messages per second to disrupt Manhattan. Allowing for improved capacity, these figures increase to 720 messages a second and 330 messages a second, respectively. It was calculated that approximately 325 500 messages per second would be required to disrupt the entire of the US mobile services. Given that the attack is conducted via the Internet, the required traffic capacity was calculated to be at worst 8437.5 kbps for Washington, D.C., 3867.3 kbps for Manhattan, and 3.8 Gbps for the US. It was also noted that using multi-recipient messages will reduce the required traffic (Enck, Traynor, McDaniel, & La Porta, 2005). Given the magnitude of the DDoS attack on Myanmar (presented in Section 5.4.1.12), this traffic is achievable. The calculations conducted by Enck *et al*. are conducted for a South African situation in Section 7.3.

This research illustrates the potential susceptibility of mobile networks to a network-warfare style attack. As the capacity of mobile infrastructure components increases, the required messages and traffic will also need to increase to have the same affect. An interesting scenario may be where the network is flooded with malicious SMSs designed to crash smartphones; these SMSs are described in Mulliner and Miller (2009). This would both disrupt the network and result in many phones needing to be reset; this will be a DoS attack against both the network and the devices.

5.5.1.6 Additional Incidents and Reports

This section presents additional incidents; some of these occurred during 2011 and are not discussed in any depth, but are included for completeness.

After the December 2007 elections in Kenya, the SMS services of the mobile networks were used as a delivery mechanism for hate speech, further inciting ethnic violence in the country (Okeowo, 2008). Reports from the Middle East suggested that Israel has gained access to telephone and mobile phone networks through hacking. In 2008 reports claimed that Israel had used Syrian telecommunications to distribute messages offering rewards for information on missing troops; and attacks on the Lebanese telecommunications used the voicemail and SMS services to disseminate anti-Hezbollah messages (StrategyPage.com, 2008; StrategyPage.com, 2009a). In 2009 messages were sent to residents of Gaza warning them to remain indoors during Israeli military operations (StrategyPage.com, 2009a). In addition, television and radio stations were also hacked into. These

incidents illustrate the possibility of legitimate functionality of mobile services being put to alternative use; in these cases psychological operations. In the case of the Israeli attacks, it appears that network warfare methods were used to access and compromise the telecommunications systems; this further illustrates that vulnerabilities do exist which may result in the mobile infrastructure being compromised from a remote network-based attack. There have also been reports that Israeli unmanned aerial vehicles are jamming mobile phones and other broadcasts in Gaza (Shachtman, 2008). In September 2011 reports emerged that mobile phone networks in South Korea had been affected when it was alleged that the North Korean forces electronically attacked a US military aircraft (AFP, 2011). This indicates the potential use of electronic warfare against mobile communications; particularly in a conflict situation. Electronic warfare tactics have also been used to detected illegal mobile phones smuggled into prisons (Hodge, 2009b), and is being proposed to jam the mobile communications in US jails (Singel, 2009). Such commercial devices could also be used by attackers to disrupt legitimate mobile communications in cities.

A phone hacking scandal resurfaced in the UK during 2011; journalists are accused of gaining access to individuals' voicemail for information in news coverage (INet Bridge and AFP, 2011). This further illustrates the vulnerability of telecommunication systems to illegitimate access. One of the war logs from Afghanistan that was released by Wikileaks (Section 4.2.7.4) indicated there was concern by coalition forces that the insurgents had insider assistance in the Afghan mobile networks, who would eavesdrop on coalition mobile calls (Tisdall, 2010). The report indicated that the calls from all ranks of the military and diplomatic representation was carried by the Afghan networks; from this it can be deduced that some militaries do routinely use mobile phones on deployment. Therefore, the security concerns of mobile devices apply to the military, and IW. Proposals for Android applications in military battlefield equipment (Ackerman, 2010) and a proposed mobile infrastructure for mobile computing in the US Army (US Army Signal Center of Excellence, 2011) further indicates the growing prevalence of mobile devices and infrastructure to the military, and therefore its relevance to IW.

Mobile phones and social networks have also been used in mass anti-government demonstrations. These occurred in the Philippines in 2003 (Rigby, 2008); Iran, China, and Moldova in 2009 (World Movement for Democracy, c. 2009); and Tunisia, Egypt, and the North African and Middle East region in 2011 (Sky News, 2011). The demonstrations in the Philippines, Tunisia, and Egypt resulted in the respective governments resigning. This presents difficulties in defending against, as

legitimate services are used to instigate actions that are considered illegal by the respective governments. These incidents will be discussed in more detail in Section 5.6.

In 2011 vulnerabilities in GSM modules were demonstrated, where an attacker could identify and locate the modules (by GPS co-ordinates) over the mobile network; similar vulnerabilities also were found in industrial control systems (Fisher, 2011e). Research in Motion (RIM) discovered a severe vulnerability in their BlackBerry servers, where a malicious image sent to a device could potentially provide an attacker control of the servers; a patch was released for this vulnerability (Goodin, 2011b). As the enterprise servers provided control of all BlackBerry devices connected to it, an IW attack against the server could have been severe for the victim organisation. There are also reported concerns over mobile-based DDoS attacks that could target the mobile operators; infected applications flood the mobile towers with requests to overload them (Spirovski, 2010).

It was discovered that there was a breach of the Apple iPad's 3G services in June 2010; the SIM card authentication and email addresses of more than 100,000 high-ranking individuals in the United States were compromised (Tate, 2010). A report in 2011 suggests that the growing public concern over privacy and information security is related to the evolution of mobile technology; people want to know that they are secure when using mobile devices to conduct online transactions (Roman, 2011). Davidson and Yoran (2007) provide an example where a multi-billion Dollar corporate deal was lost due to employees discussing the details using unsecured mobile phones; this indicates either the discussion was intercepted, or some corporations are extremely concerned over the security of mobile devices.

Phishing scams migrated to mobile devices in the United States in 2005 (Enck, Traynor, McDaniel, & La Porta, 2005; Swartz, 2005); these phishing scams appeared on South African mobile networks by 2009 (Francis, 2009). In South Africa, there have also been incidents where users have been billed for unwanted SMS subscription services (Knowler, 2010); this and the phishing scams indicate mobile phones are being subjected to similar techniques that targeted emails. The convergence of mobile devices and social networking applications may further increase the prevalence of these attacks.

The concept of the remote kill switch may prove to be a useful security mechanism, but could also potentially be used maliciously to illegitimately disable devices or clear them of data. Intel has implemented this to allow an SMS to be used to disable lost or stolen notebooks (Roberts, 2010); Google has twice used a similar concept to remotely remove malware of infected Android devices

twice (Keizer, 2011). Should such systems be compromised and used maliciously, an attacker could switch off notebooks at will, or remove legitimate functionality of Android devices. Malware may also be able to exploit any vulnerabilities in this system to deny the use of the devices.

As mobile devices and the towers have antenna, they may be susceptible to attack by directed electromagnetic energy or electromagnetic pulses (EMPs). Miller (2005) indicates that there was low proliferation of weapons using directed energy or EMPs in 2005, and a high technological competency was required to develop such weapons. High-altitude detonation of nuclear weapons also generates a large EMP; this therefore will be restricted to nations with both nuclear weapons technology and the missile capability to detonate the payload at high altitudes (*ibid*.). A report assessing the impacts of EMPs on critical infrastructures in the US indicates that the mobile infrastructure is more susceptible to a widespread EMP than the fixed-line communications infrastructure due to mobile infrastructure components being less robust, and having less backup power (the electrical power grid may also be disrupted due to a large EMP) (EMP Commission, 2008). Miller (2005) states that even if the devices and infrastructure survive, there will be a surge of attempted voice calls, which may overload the infrastructure. Other low-power directed energy weapons may have localised effects; therefore multiple attacks would be required for noticeable effects. The mobile infrastructure would have some measures taken to mitigate the effects of lightning strikes and interference (EMP Commission, 2008); these may be sufficient to protect infrastructure components from homemade devices.

5.5.1.7 Summary and Discussion of Trends

The incidents presented illustrate that there are vulnerabilities in the mobile infrastructure that can be exploited via network warfare. Examples of the relevance of insider threats to the mobile infrastructure were also presented. Once the infrastructure has been compromised, the attackers may accomplish a variety of objectives; including espionage, psychological operations, and compromising the security of financial services relying on mobile communications. Legitimate functionality may also be used in actions that may compromise national security such as the mass anti-government demonstrations. There is also a concern over the threat of EMP or directed energy weapons.

The majority of the cases presented targeted confidentiality; the examples of using the legitimate functionality can be considered as impacting integrity; and there was an example of a possible DoS attack.

5.5.2 Mobile Malware

This section presents trends in mobile malware from the initial appearance of such malware; secondary data and specific reports are considered. Many of the trends presented here are deduced from descriptions and malware listings by Gostev (2006a; 2006b), Morales (2009a; 2009b), and Gostev and Maslennikov (2009). A previous version of this section was presented in van Niekerk and Maharaj (2011b).

5.5.2.1 Trends in Mobile Malware Prevalence

This section presents the trends in the prevalence of mobile malware; the figures for newly detected mobile malware variants and families over time are used to illustrate this prevalence. The numbers of newly detected families per year are illustrated in Figure 5.9. The reports by Gostev and Gostev and Maslennikov are not consistent with the listing presented by Morales; Parial (2005) and Gostev consider the Cabir virus of 2004 as the first mobile virus; however Morales lists three previous versions for the Palm devices, which is supported by the Trustwave report (2011). Morales lists malware up to July 2008; however Gostev and Maslennikov show a number of new malware detected from September 2008; this accounts for the large discrepancy between the two plots in 2008. The plot of the total number of families assumes the higher figure between the two as correct; this provides an estimate of the overall number of detected mobile malware families. This plot exhibits an extremely rapid growth rate.

The increase in the number of malware variants is presented in Figure 5.10. The number of new variants may be significantly underestimated in the figure due to the quantities of mobile malware discovered in the latter part of 2008. The same rapid growth rate is seen. Due to the increasing prevalence of mobile devices in society, and their increasing technical capabilities, this trend is expected to continue.

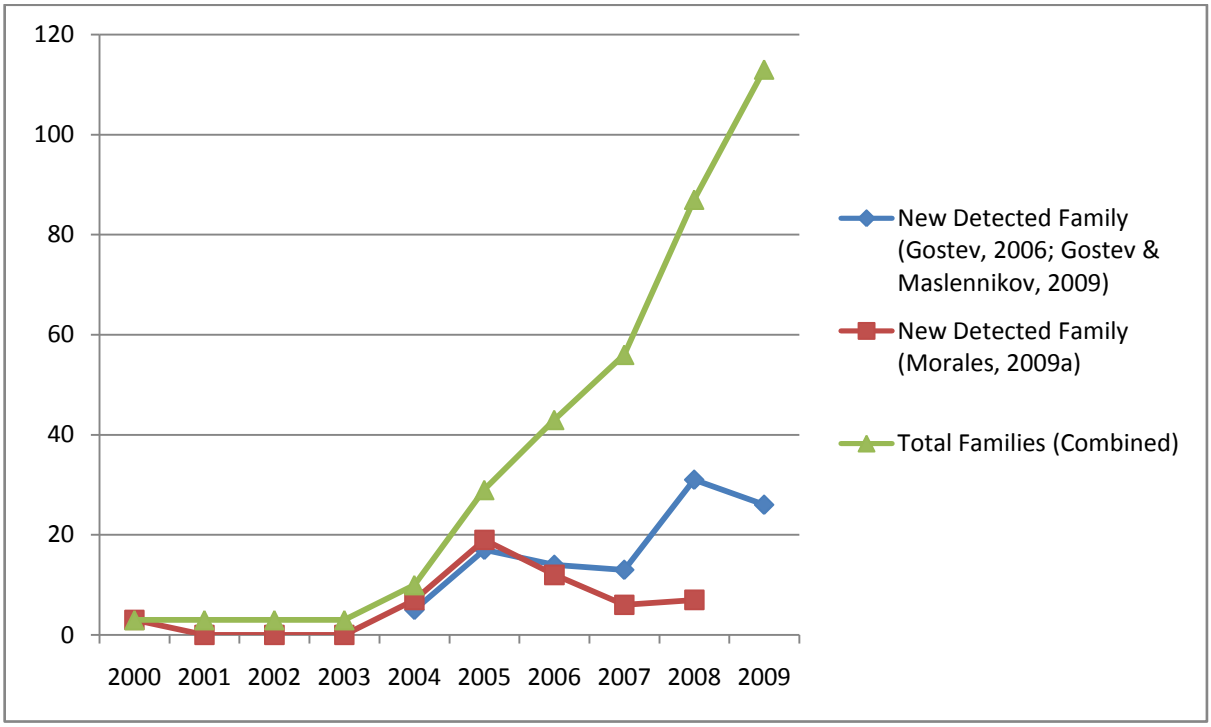


Figure 5.9: Malware Family Numbers, sources: Gostev (2006a), Morales (2009a); and Gostev and Maslennikov (2009); van Niekerk and Maharaj (2011b)

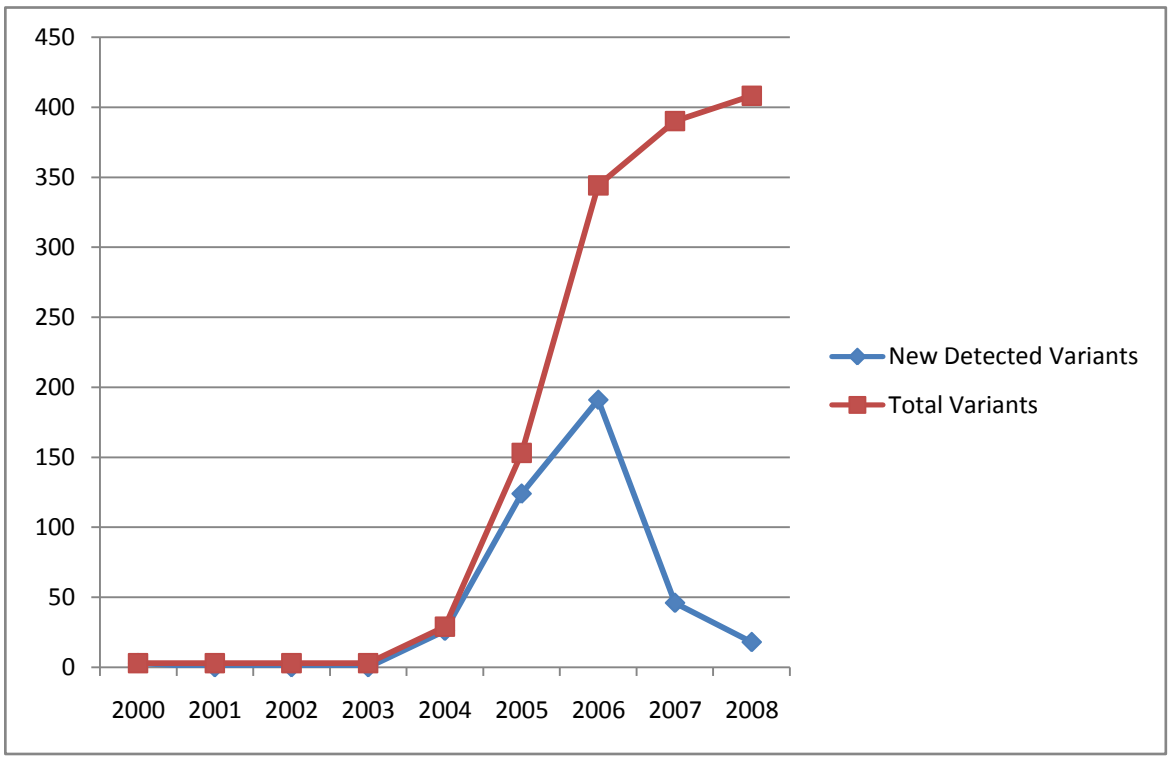


Figure 5.10: Malware Variant Numbers, 2000 – July 2008, source: Morales (2009a); van Niekerk and Maharaj (2011b)

Gostev and Maslennikov (2009) indicate that the number of malware trebled between 2006 and 2009, which maintains the growth rate between 2004 and 2006 that was reported by Gostev (2006a). The Trustwave Global Security Report 2011 (Trustwave, 2011) indicates a 15% increase in mobile ransomware from 2010, and an 8% increase in general mobile malware. The increase in mobile malware illustrates that this is a growing threat, and may soon become as prevalent as traditional PC-based malware.

5.5.2.2 Trends in Targeted Mobile Platforms

The percentage of mobile malware targeting specific platforms from 2004 to August 2009 is shown in Figure 5.11 for malware families and Figure 5.12 for malware variants. The majority of activity surrounds the Symbian platform, with the Java (J2ME) platform also exhibiting a large proportion of activity compared to the other platforms. This is due to the prevalence or popularity of the platforms; the malware coders target the most prevalent operating system or platform to maximise the impact of the malware. The Nokia devices with the Symbian OS were the most common therefore they initially were targeted the most; the majority of Symbian malware is reported to be from the period 2004 to 2006 (Hyppönen, 2010).

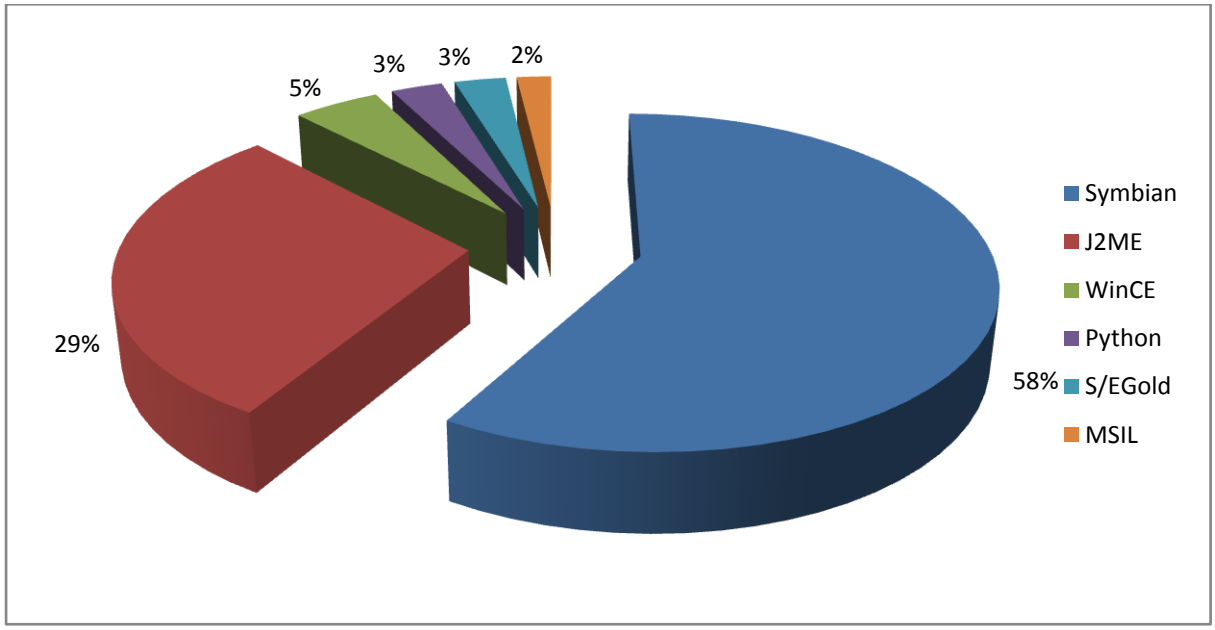


Figure 5.11: Families by Platform, source: Gostev and Maslennikov (2009); van Niekerk and Maharaj (2011b)

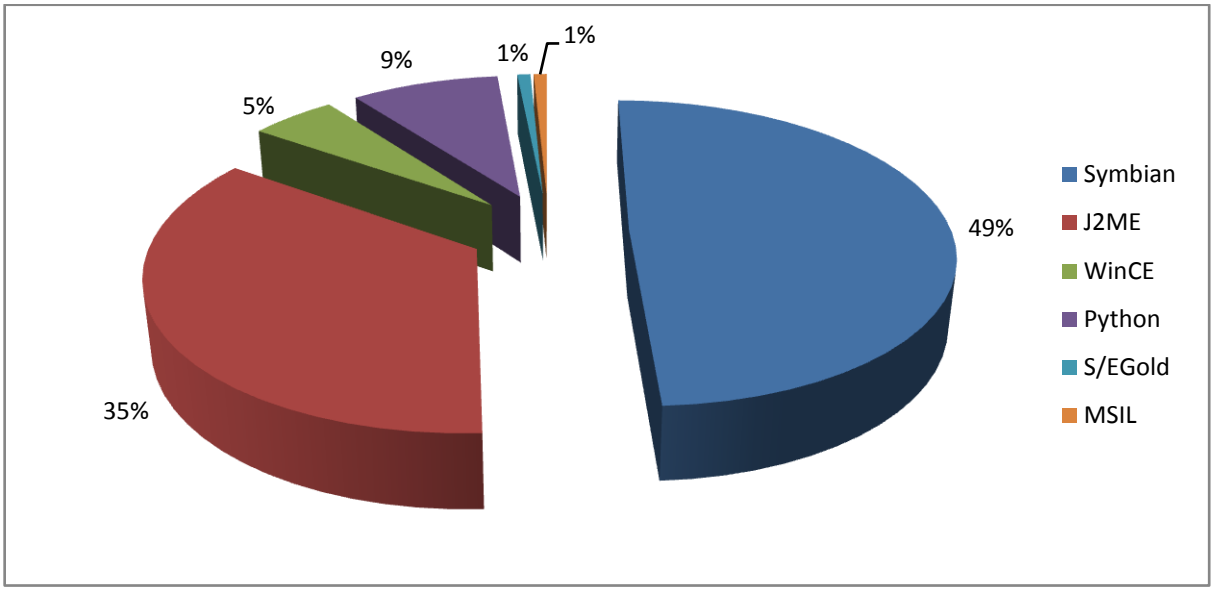


Figure 5.12: Variants by Platform, source: Gostev and Maslennikov (2009); van Niekerk and Maharaj (2011b)

Since the initial studies by Gostev and Maslennikov (2009) and Morales (2009a), additional devices and platforms have been targeted. In particular the Apple iPhone and iPad and the Google Android devices are being targeted; Seriot (2010) lists four malware types for the iPhone, however the discovered malware is limited to jailbroken devices (Hyppönen & Sullivan, 2010).

5.5.2.3 Trends in Malware Type

The percentage of each type of malware reported by Morales (2009a) for the period 2000 to July 2008 is presented in Figure 5.13. From this, it is apparent that Trojans are the most prevalent, followed by viruses and spyware. This indicates that the majority of malware appears legitimate initially, and is therefore probably inserted into legitimate applications, such as a trial or demo version that is freely available. The viruses indicate that some infections occur due to the transmission of infected files. It is difficult to present a graphical representation of malware types per family as variants of the family may be of different type; for example, CommWarrior has Trojan, worm, and virus variants (Morales, 2009a).

The numbers of detected malware types are listed per year in Table 5.6. From this it can be seen that the Trojans and viruses were prevalent up to 2006; during 2007 and 2008 the worm and spyware types were introduced and became prevalent. Account logon details may be compromised by spyware; therefore the introduction of this type indicates that mobile malware may be used for cyber-crime, as traditional PC-based malware is used. The iPhone has also been targeted by worms (Seriot, 2010).

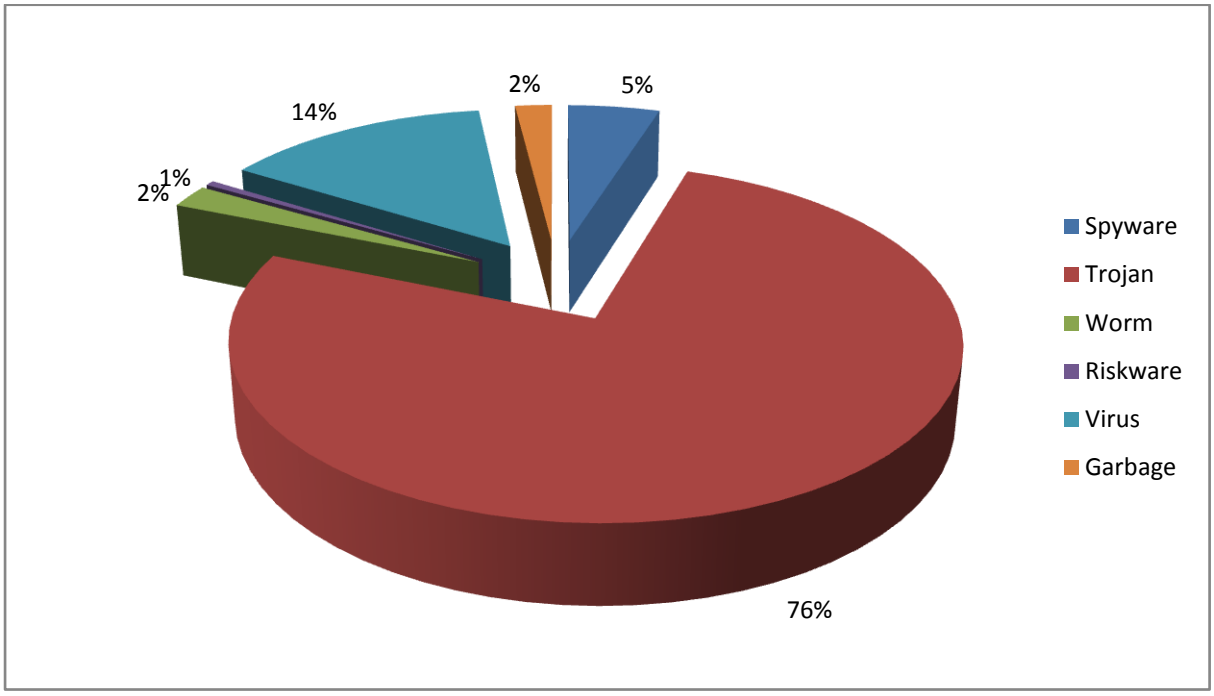


Figure 5.13: Variants by Type, source: Morales (2009a); van Niekerk and Maharaj (2011b)

Table 5.6: Annual Numbers for Types of Malware Variants, source: Morales (2009a); van Niekerk and Maharaj (2011b)

Malware Type	2000	2004	2005	2006	2007	2008	Total
Virus	1	15	19	17	6	0	58
Trojan	2	11	105	160	23	10	311
Worm	0	0	0	0	2	7	9
Spyware	0	0	0	5	15	0	20
Garbage	0	0	0	8	0	0	8
Riskware	0	0	0	1	0	1	2
Total	3	26	124	191	46	18	408

5.5.2.4 Trends in Malware Payloads

The numbers of malware variants and families detected from 2004 to August 2006 are given for their payloads in Table 5.7. From these figures, the top three payloads can be seen to be sending of illegitimate SMSes, interfering or deleting files, and copying information. This trend is also noticed by Morales (2009a); however, he also raises the issue that the infected device's battery may be drained due to the heightened use of the SMS and Bluetooth connectivity due to the malware propagation. The sending of illegitimate SMSes is prevalent due to the fact that it results in

financial gain by criminal elements (Hyppönen & Sullivan, 2010). The SMSes are charged for premium rate or international delivery; however the message is never transmitted fully resulting in a difference between the amounts charged to the victim and the transmission cost. The criminal elements retain this difference. Payloads have also been detected where the device dials these numbers, resulting in large phone bills. It is believed that these attacks will become even more prevalent (Hyppönen, 2010). Of the malware that send SMSes as a payload, only two families are classed as SMS flooders which could potentially be used to conduct DoS attacks; and one family with four variants uses SMS as a propagation vector. A notable family of malware that interferes with system files is the Skulls virus, propagates by Bluetooth and replaces system applications with a skull icon, leaving only the telephone functionality operational (F-Secure Corporation, 2005). The subsequent introduction of mobile spyware may result in increasing amounts of malware that attempt to steal user data; three of the reported iPhone malware variants stole data from the device (Seriot, 2010). One iPhone malware variant behaved like a botnet (Porras, Saidi, & Yegneswaran, 2009); botnets are widely used in PC-based malware as a tool for cyber-crime.

Table 5.7: Malware Payloads, sources: Gostev (2006); Gostev and Maslennikov (2009); van Niekerk and Maharaj (2011b)

Action	Families (%)	Variants (%)
Infects files	4 (3.8)	11 (2.1)
Sends SMS	42 (39.6)	237 (46.1)
Replaces files, icons, fonts, system apps	15 (14.2)	172 (33.5)
Installs additional malware/corrupted apps	8 (7.5)	44 (8.6)
Interferes with anti-virus	5 (4.7)	36 (7)
Disables or blocks functions, storage	5 (4.7)	9 (1.8)
Steals data, monitors calls & SMSes	9 (8.5)	87 (16.9)
Deletes files, fonts, folders, contacts, messages etc	8 (7.5)	8 (1.6)
Interferes with phone booting/restarting	3 (2.8)	7 (1.4)
Nuisance (changes settings etc, fake system messages, fake anti-virus etc)	7 (6.6)	15 (2.9)
Makes calls to paid services	2 (1.9)	3 (0.6)
Other/unknown	11 (10.4)	13 (2.5)

5.5.2.5 Trends in Malware Infection and Propagation Technologies

The technologies employed by malware to infect device and propagate is listed in Table 5.8; this is for malware detected from 2004 to August 2006. From the table, it is apparent that the majority of

vulnerabilities exploited by malware are in the operating system; Bluetooth and file application programming interfaces (APIs) are also prevalent infection and propagation technologies. The Cabir virus was the first to utilise Bluetooth technology to spread (Parial, 2005). The use of the file API confirms the statement in Section 5.5.2.3 that the prevalence of viruses indicates infected files were a major propagation technique.

Table 5.8: Infection and Propagation Technologies, source: Gostev (2006); van Niekerk and Maharaj (2011b)

	Families (%)	**Variants (%)**
Bluetooth	5 (16.1)	33 (19.4)
File API	8 (25.8)	24 (14.1)
Network API	2 (6.5)	3 (1.8)
SMS	2 (6.5)	3 (1.8)
OS Vulnerability	18 (58.1)	124 (72.9)
MMS	2 (6.5)	12 (7.1)
Java	1 (3.2)	2 (1.2)
Email	1 (3.2)	3 (1.8)
Other/Unknown	2 (6.5)	3 (1.8)

The majority of malware infections are ultimately due to the users allowing the malware to install itself on the device, followed by Bluetooth, MMS and multimedia cards (MMC) (Dunham, 2009). However, Dunham also reports a discrepancy in that users indicate larger rates of infections by MMS and Bluetooth rather than user installation; he proposes that the users report the propagation vectors as the infection mechanism as they are unwilling to accept responsibility for allowing the malware to install. From Dunham's report and the statistics illustrated in Table 5.8, it can be assumed that whilst the malware exploited OS vulnerabilities and file APIs, they also used social engineering to prey on the ignorance or gullibility of users to install them and infect the devices. In particular, the CommWarrior malware could propagate via either Bluetooth or MMS, but in the case of MMS some user interaction was required (F-Secure Corporation, c. 2007), which indicates social engineering. Users may also share infected files, especially Trojans, which aids in the propagation; however, as mobile worms are now being detected, a shift may occur where the malware has the capability of spreading autonomously.

5.5.2.6 Emerging Trends and Additional Malware-Related Incidents

Due to the prevalence of mobile devices in modern society, the rapid growth in mobile malware numbers is not surprising. As with traditional PC-based malware, the popular devices are targeted; therefore the Symbian OS of Nokia was initially the focus of malware coders, however with the shift in popularity to the iPhone and Google Android devices, the malware focus has also shifted to these devices. Trojans appear to have been the most prevalent type of mobile malware; however, there has been the introduction of mobile spyware and worms. The malware payload appears to favour those that result in financial profit for criminal elements, yet there are still a large number that may leave a device inoperable due to corrupting files. File APIs, Bluetooth, and operating system vulnerabilities are reported as the most prevalent infection and propagation methods, however in many instances the users allow the malware to install on the device.

The fact that the Ikee.B worm that targets the iPhone behaved as a botnet (Porras, Saidi, & Yegneswaran, 2009) indicates mobile malware attacks may begin to resemble and function more like PC-based malware. The Zeus malware, which was originally PC-based and targeted online banking, migrated to mobile devices and also targeted mobile banking (Kitten, 2010). Mobile phones may also be used to distribute PC-based malware; in March 2010 it was discovered that the Mariposa malware was installed on a PC when Vodafone UK's HTC Magic smartphones with the Android OS was connected to the computer; this malware then stole the user's account passwords (Charette, 2010). Concerns over pre-installed malware have led to the importing of Chinese-made mobile devices and infrastructure components being banned in India (StrategyPage.com, 2010d).

In 2010 CNN hosted and broadcasted a war-game simulating the handling of a major malware attack by senior US government. The scenario, called "Cyber Shockwave", was that malware was using the mobile networks to propagate, and disrupting services; this migrated to computer networks (Cable News Network, 2010). The scenario was interesting as it used the mobile network was the point of entry for a malware-based IW attack, and also considered mobile malware migrating to computer networks. As occurred in the war-game, it will be very difficult to attribute such an attack with any certainty to a single organisation or nation. There is concern that an aggressive worm will spread through mobile networks and disrupt services on a global scale (Hyppönen, 2010), similar to the PC-based Slammer and Sasser worms discussed in Section 5.4. Whilst such a pandemic of mobile malware has not been realised, some of the notable mobile malware, such as Cabir and CommWarrior, have been seen in multiple nations, including South Africa (Gostev, 2006b). The propagation of MMS worms was simulated by Fleizach *et al*. (2007);

this illustrates that in twelve hours approximately 15% to 35% of susceptible devices will be infected, depending on the address book topology. The authors also indicate that such a worm may result in outages or degradation of MMS services due to the MMS switches becoming overloaded. Traynor *et al*. (2009) also illustrate the impact of mobile botnets on the core infrastructure, and conclude that less than 24 000 infected devices would reduce the capacity of components in the core network by 75%, or 141 000 devices for high capability higher capability mobile networks.

The advent of application stores for mobile devices has contributed to the distribution of malware; most notably is the Trojans that are inserted into legitimate free applications and games on the Android store (Mitchell, 2010). Google allows applications to be made available on the store without checking them; should there be complaints or malicious content is discovered, then that application is removed. Apple however, circumvents this by testing all applications prior to making them available on the iTunes store (Hyppönen & Sullivan, 2010). The Android platforms are more vulnerable, and this can be seen by the number of new malware types targeting the platform in 2011 reported by Fisher (2011a; 2011b; 2011d), Roberts (2011c), and Westervelt (2011b). Another concern raised with the Android market is a feature that allows users to remotely install applications onto their devices; should this be compromised there is potential that it is used to remotely install malicious content on devices (Maslennikov, 2011). An application store for Nokia devices is also available, as well as multiple websites providing a platform for developers to sell their products; such online stores and websites may be increasingly targeted in future to distribute malware.

PC-based malware has been distributed via social networking websites (this will be discussed in Section 5.6); what has not been seen yet is malware that exploits the mobile social networking applications. Due to the popularity of both mobile devices and social networking, these integrated mobile social networking applications may become a target for malware developers. Future evolution of technology may result in common operating systems for PCs, tablets, and mobile devices; this may provide malware developers with the ability to produce malware that is device or platform independent, which could easily migrate between the different computing and communication devices due to common vulnerabilities.

The growing prevalence of mobile malware indicates that the mobile devices and infrastructure may be used to conduct network warfare, using multiple communication technologies to propagate and infect devices. The mobile networks could be an entry point for a major network warfare attack on a nation, as suggested by the "Cyber Shockwave" scenario; this will truly disrupt the communications

and networking functions within a nation. The psychological impact of such an attack could also be large.

5.5.3 The Role of Mobile Devices and Infrastructure in IW

Figure 5.14 illustrates the roles of mobile devices and infrastructure in IW.

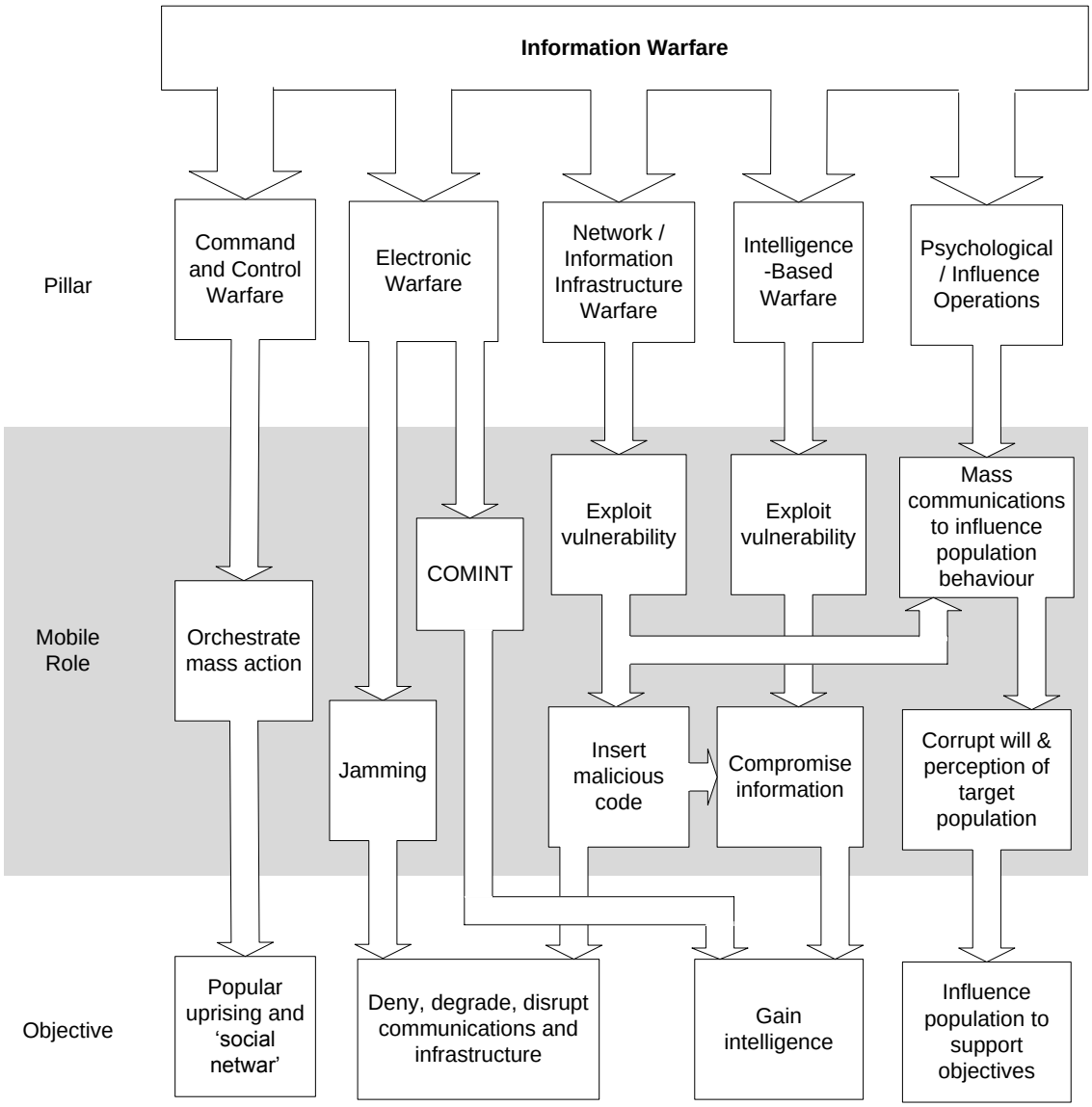


Figure 5.14: The Role of Mobile Devices and Infrastructure in Information Warfare

Mobile devices have been used as an improvised command and control platform to instigate mass action, which has resulted in popular uprisings. Electronic warfare may target the wireless transmissions to either jam them to deny communications, or intercept the information and thus

gain intelligence. Malicious code can be distributed in network warfare attacks that overload the channel capacity or infrastructure components, and thus deny or degrade services. Network warfare and infrastructure warfare are combined as in this scenario the network and infrastructure can be considered the same entity. Malicious code may also be used to create backdoors, allowing attackers to compromise information and gain intelligence. This backdoor access may also allow for attackers to illegitimately transmit psychological operations messages to influence populations; this may also be achieved through legitimate access. The predicted security problems with mobile devices and infrastructure, combined with their prevalence in Africa, may contribute to the susceptibility of African nations to cyber-attack (Goodman & Harris, 2010).

5.6 Web 2.0 Incidents

This section discusses incidents regarding Web 2.0 technologies. The objective of this section is to identify vulnerabilities and threats from trends in incident reports; this aligns with the study objectives of gathering information in these areas, and then using it in the vulnerability framework. The possible roles of Web 2.0 technologies in IW will be presented. This section is a combination of two previous publications: Pillay, van Niekerk, and Maharaj (2010), and van Niekerk, Ramluckan, and Maharaj (2011); the candidate's contribution to these papers is presented here.

5.6.1 Incidents

In Pillay, van Niekerk, and Maharaj (2010), the use of Web 2.0 technologies and social networking for public advocacy by civil society organisations is illustrated. These technologies have been used to promote awareness, pressure organisations into changing policy, and co-ordinating information and raising funds in disaster relief operations; the use by government organisations for communication was also illustrated. This indicates that this technology may be used to manage perception and psychological operations; this can therefore be seen as a form of social information warfare. This is applicable to the military environment in what is being termed "influence operations" by the US military; this is an extension to psychological operations in that it also includes public affairs and other related information operations (Larson, *et al*., 2009). Web 2.0 technologies, and in particular social media, are a many-to-many communications medium, these tools can be used in public relations, crisis communications, and similar activities.

After the earthquake in Haiti, and aircraft carrying aid was unable to land; this was posted on Twitter, which resulted in a flood of posts directed at the US Air Force account to let the plane land;

it had done so within an hour (Kennedy, 2010). Web 2.0 technologies are being actively used to conduct influence operations by the Israeli Defence Force (Hodge, 2008; Pfeffer & Izikovich, 2009): activities include posts from embassies and posting videos of precision air-strikes. The Israeli Defence Force is actively recruiting specialist in social media to aid in plugging information leaks and conducting influence operations (Pfeffer, 2010; Pfeffer & Izikovich, 2009). In 2010 an Israeli raid on an aid ship killed a number of people; images and videos were used by both sides to influence perception, however the opposition appeared to have been more successful than the Israelis (Shachtman, 2010). In 2011 reports surfaced that the US military has been developing and possibly using software named "Persona", which is aimed at generating and managing fake social media profiles (Stein, 2011). These fake profiles could be used to influence consensus on controversial issues or possibly target individuals be impersonating out-of touch school acquaintances (Kerrigan, 2011; Stein, 2011). These incidents illustrate active use of Web 2.0 and social media by the military for IW.

More extreme incidents are the mass anti-government demonstrations that have been orchestrated via SMS and social media; in 2003 the Philippines president eventually resigned due to protests of up 700 000 people at a time which was largely instigated through SMS (Rigby, 2008). In 2009 Moldova saw the "Twitter Revolution"; mobile devices and social media were instrumental in uprisings in Urumqi, China; and in June 2009 there were mass protest in Iran due to the perception of flawed national elections (World Movement for Democracy, c. 2009). What is interesting about the Iranian protest that the Web 2.0 and mobile technologies were also used to transmit information out of the country as the authorities were censoring the traditional media and Internet access. Information was therefore shared through websites such as Twitter and Facebook; The US State Department found this source of information so crucial that Twitter was requested to delay a network upgrade that would have prevented access to the site (United Nations Foundation, 2009). In 2010 Mozambique experienced food riots, where SMS was again used to instigate the riots (Jacobs & Duarte, 2010); this was effective despite the relatively low mobile penetration of 29% in the country (Business Monitor International, 2010). In January 2011 the Tunisian and Egyptian governments resigned after mass anti-government demonstrations orchestrated by social media; these are described in detail in Section 4.2.7.6. Similar unrest has spread through the Middle East and North African regions (Sky News, 2011). In Uganda, Swaziland, and Cameroon the governments have blocked access to social networking websites following protests seeking political reform (Malakata, 2011). There was also a proposal to block access to social media in Russia due to

national security concerns; this followed a DoS attack on the blog of the Russian President in 2011 (Isachenkov, 2011).

During the 2009 Iran protests, the authorities also blocked access to many social media websites (World Movement for Democracy, c. 2009); Chinese authorities blocked access to SMS services after the riots in Urumqi; these services were only restored six months later (Daily News, 2010). The Tunisian authorities attempted to hack into and delete social media profiles of the main instigators of the demonstrations (Madrigal, 2011). The Egyptian government responded to the unrest by shutting off access to the Internet and mobile services (Kravets, 2011). However, a work around was provided by Google where a fixed-line telephone number was provided for users to leave a voicemail message; this message would then be posted on Twitter (News24.com, 2011). The concept of preventing access to the Internet and social media was not successful in Egypt as the protests had gained momentum at the time and was therefore not as reliant on social media as in the initial stages; once the concept had spread the communications medium was no longer required. The incidents and government reactions to unrest illustrate a growing concern over the power of social media to orchestrate and spread the unrest, even in regions where the Internet or mobile penetration is not high. The use of such technologies to co-ordinate mass demonstrations and the attempts by the authorities to disrupt this can be considered as a form of command and control warfare.

Web 2.0 technologies present a threat in the form of a conduit for information leaks; the Wikileaks incident described in Section 4.2.7.4 is a prime example of this. The Israelis military was forced to abandon a raid after a soldier carelessly posted the location and time of the operation; this still occurred even though an awareness message was distributed to warn against such leaks (Hodge, 2010). Information about the head of a UK intelligence service was posted on Facebook by his wife; this potentially revealed their residential address, identities of their friends, and other activities (Shachtman, 2009a). The security issue regarding this is debated; most of the information was known, however the possibility of such information being use to attack or compromise him through his family raised concerns (Grobler, 2010; Shachtman, 2009a). It is difficult to determine the eventual impact of information releases; a seemingly insignificant piece of information may be linked to others, allowing more complete intelligence to be built. The Trustwave Global Security Report lists personal information exposure as comprising 30% of attacks via social media, and corporate information exposure as comprising 20% (Trustwave, 2011). The existence of the US

Military's Magenta rootkit and Persona software was also released by the successor to Wikileaks (laurelai, 2011; Stein, 2011).

This threat of leaks corresponds to the possibility of intelligence gathering through social media; data mining contributes 20% of the attacks on social networks (Trustwave, 2011). The US Air Force monitored public reaction and backlash to an unannounced flight by Air Force One and its accompanying fighters over New York; it initially raised fears of another 9/11 type attack by the public as it appeared that a commercial airliner was being chased by the fighters (Lardner, 2009). Intelligence gathering operations may also target individuals: in early 2011 a warning was released by the US Department of Defence regarding a false-flag operation. A fake profile using a photo of a recently retired colonel was attempting to add members of the US information operations community as friends on LinkedIn (Harding, 2011). Subsequently a second warning has been posted on LinkedIn regarding suspicious profiles and activity (Katelhut, 2011; Meeks, 2011). These social engineering and false-flag operations could have serious consequences should a high-level individual be compromised. An experiment used a fake social media profile under the name of Robin Sage; the profile claimed to be employed by the US Department of the Navy as a cyber-security analyst, and have an advanced degree from the Massachusetts Institute of Technology. The profile picture depicted a female in her twenties. Approximately 300 connections were made in a month; many of these were high-level individuals, many of whom did not realise that the profile was a fake (Cisco, 2011). This further illustrates the threat of social engineering on Web 2.0 sites. Lawton (2007) indicates that users may be tricked into clicking on malicious links due to sexual content; users could also be enticed into controversial or embarrassing behaviour, which is then used to blackmail them (van Niekerk, Ramluckan, & Maharaj, 2011). The role of Web 2.0 technologies in "hacking executives" is further illustrated by Dhanjani, Rios, and Hardin (2009).

Malware has also used social media as a vector to propagate: KoobFace tricked Facebook users into clicking on a link that downloaded a Trojan which hijacked web browsers (Villeneuve, 2010). Facebook was also used to propagate malicious emails by the Pushdo botnet (Westervelt, 2009), and legitimate websites for job listings were targeted by the Bredolab Trojan (Westervelt, 2011a). The Trustwave report indicates that 25% of attacks on social media are related to malware (Trustwave, 2011) and a Symantec report lists social media as contributing 12% of the considered malicious websites; this is the second most prevalent type of malicious website (Symantec Corporation, 2011a). Due to the nature of Web 2.0, these websites have more vulnerabilities than

traditional Web 1.0 websites, as they require scripting for users to upload and access content (Lawton, 2007).

Due to security concerns, the US military attempted to ban troop access to social media (Shachtman, 2009c), however some access was granted (StrategyPage.com, 2010a), and eventually it was decided not to ban access (Ackerman, 2011). Many organisations also attempt to block employee access; these attempts are ineffective as the employees will still gain access through personal devices. Monitoring posts (as the Israeli military attempted) only discovers when there has been a leak, but does not prevent them; however this may allow a rapid response to mitigate damage. Awareness education is mentioned as the most effective measure to mitigate against social media security incidents (Trustwave, 2011); however, as in the leak by the Israeli soldier, this is not always effective due to user apathy. The US Army has included social media in its document on threat awareness and reporting (Department of the Army, 2010). A defence-in-depth process, where all three methodologies are employed to some degree may prove the most effective. In van Niekerk, Ramluckan, and Maharaj (2011) the concept of a "honey pot" for social media is proposed; this is intended to be the use of fake profiles that are intended to attract attackers and then reverse-social engineer them in order to gain insight into their attack methods and objectives. Information gathered from this may then be used in awareness training and improve monitoring to detect attacks.

The widespread availability of mobile devices with cameras and social media access may result in the movements of military forces being recorded and posted publicly by civilians; the time taken to capture and post the image is quick, therefore the information will be available on the Web before anything can be done to prevent it. This may prevent the concept of a surprise attack; however, a large scale DDoS attack (such as the one that occurred during the Russian involvement in South Ossetia and Georgia) may prevent this.

5.6.2 Incident and Trend Summary

A number of incidents indicate breaches of confidentiality, or attempts thereof. Due to careless posting, social media may be an effective tool for gathering open source intelligence. The integrity of links and profiles may be called into question due to the number of fake profiles and malicious links. Social media has been seen to be used for perception management as well as targeted attacks; it can also be used to propagate malware and orchestrate mass demonstrations. Therefore it is a versatile tool that can be used for network warfare, intelligence gathering, psychological operations,

or an improvised command and control platform. There is evidence of military use of social media and Web 2.0 technologies.

These technologies obviously create a security risk through the possibility of leaks, malicious links and, and questionable content. The increasing prevalence of the technologies will also result in increasing threats and vulnerabilities. Denying access may be ineffective at an organisational level, and it has been seen that this tactic did not halt the mass demonstrations in Egypt and Tunisia. Monitoring posts will likewise not prevent leaks, however may act as a method of dissuading careless posting and acting as an early warning system. Whilst awareness has been cited as being the best countermeasure; an incident illustrates that this is not always effective. A defence-in-depth strategy using all three methodologies may be more effective, and the concept of a social media honey pot was proposed.

5.6.3 The Role of Web 2.0 in IW

The vulnerabilities of Web 2.0 and the ability to socially engineer users may allow targeted attacks on infrastructure through these websites, in addition to mass perception management. In van Niekerk, Ramluckan, and Maharaj (2011) a model is proposed to describe Web 2.0 as an instrument of power in a psychological operations message flow model in addition to a framework to describe targeted attacks on individuals. A model describing the role of Web 2.0 in IW was also proposed by the candidate; an updated version is presented in Figure 5.15.

In the figure, the relevant pillars of IW are shown, and the corresponding role that Web 2.0 technologies play, and the objective of these functions. For this scenario, electronic warfare is not applicable, and is not shown. Network warfare and infrastructure warfare are combined as the roles of Web 2.0 in these aspects are the same. Web 2.0 can act as an improvised command and control platform to orchestrate mass demonstrations which ultimately results in popular uprisings. Vulnerabilities may be exploited to gain illegitimate access or insert malicious code that will allow the extracting of intelligence or disruption of infrastructure services. The technology can be used to socially engineer individuals to assist with extracting information and disrupting the infrastructure. Mass communications can be used to influence populations in psychological operations.

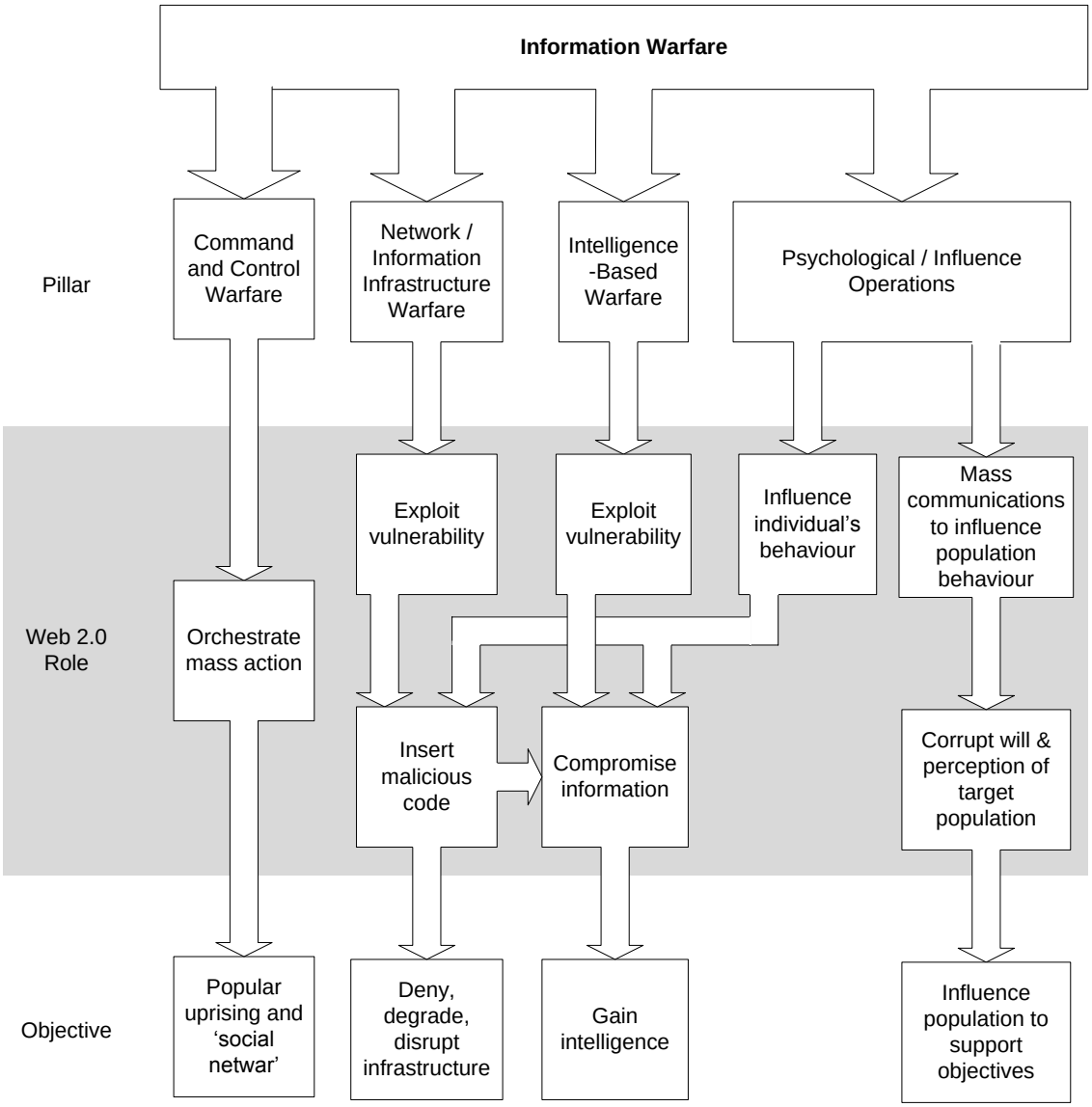


Figure 5.15: The Role of Web 2.0 in Information Warfare, van Niekerk, Ramluckan, and Maharaj (2011)

5.7 South African Trends

This section describes trends and that are specific South Africa, however it is necessary to consider South Africa in its regional and global context, therefore information for Africa and in particular the SADC region is relevant. This will be used to assess the context that South Africa is in, and the relevant threats and vulnerabilities. This section corresponds to the study objective of gathering information on security incidents and trends. This is a combination of sections from three previous research outputs: van Niekerk (2010b), van Niekerk and Maharaj (2010c), and van Niekerk and Maharaj (c. 2012).

5.7.1.1 Statistics of the African Cyber-Landscape and Related Concerns and Incidents

As described in Section 2.8.4.3, there is a ratio of approximately 10.8 mobile subscriptions for every landline subscription for both voice and data in South Africa. There is an estimated 8.82 Internet users per 100 inhabitants (International Telecommunications Union, 2011) in South Africa. This figure may increase due to additional undersea cables being introduced; this will increase the availability and affordability of broadband services in the country, and consequently its prevalence. Figure 5.16 shows the increasing and projected capacity of the undersea cables for Sub-Saharan Africa and South Africa. By the end of 2011 South Africa is expected to have four active cables providing a maximum capacity of 11 460 Gbps; this is expected to have increased to six cables with a maximum capacity of 29 380 Gbps by the end of 2013. Comparatively, Sub-Saharan Africa is expected to have eight cables with a maximum capacity of 15 140 Gbps by the end of 2011; increasing to eleven cables with a capacity of 37 660 Gbps by 2013. This data is provided and updated regularly by Song (2011). Given the capacity of 2 920 Gbps in 2008, this is a five-fold increase in five years for South Africa, and thirteen-fold increase for Sub-Saharan Africa.

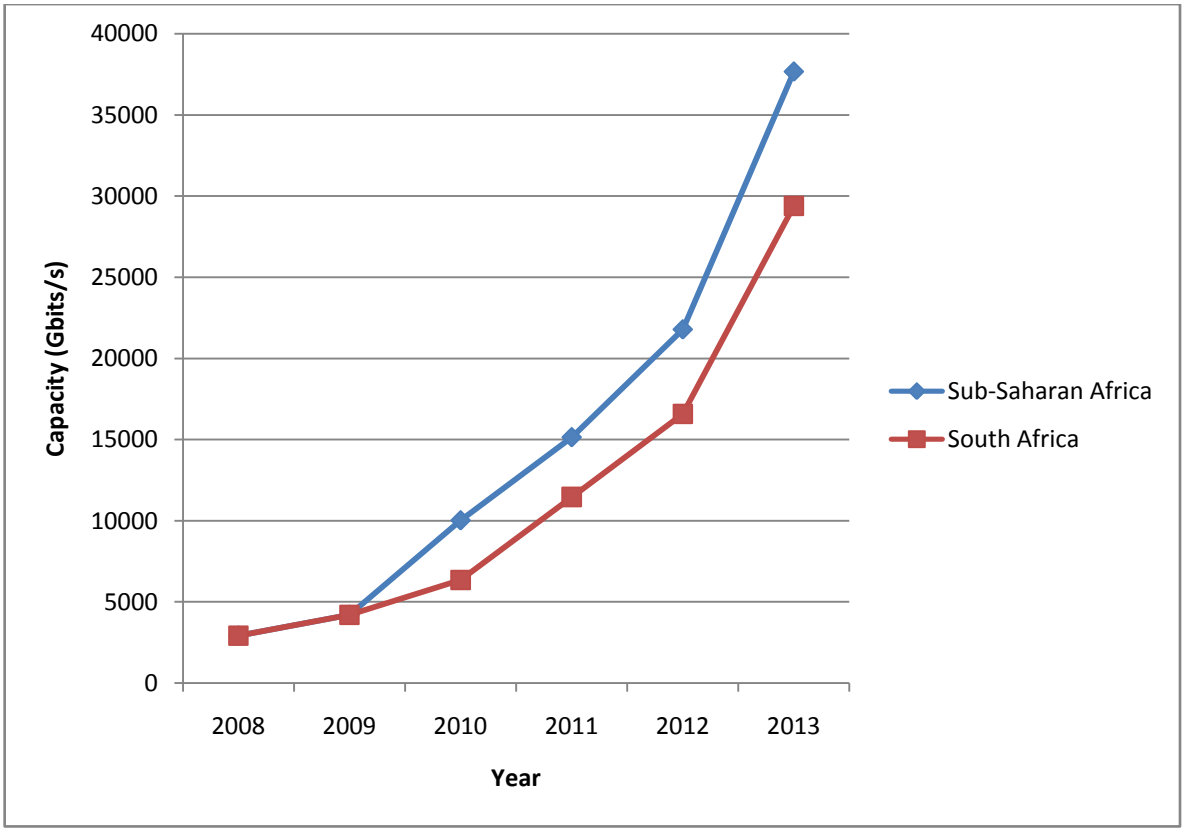


Figure 5.16: Increase and Projection of Undersea Cable Capacity, sources: Song (2011) and van Niekerk (2010b)

Of particular concern is the lack of information security awareness in South Africa despite the growing prevalence of broadband services in the country; this has been raised independently by a number of researchers (Fryer, Merrit, & Trias, 2010; Jansen van Vuuren, Phahlamohlaka, & Brazzoli, 2010; van Niekerk, 2010b). The premise is that as new undersea cables become active, the increased availability of broadband will reduce prices, resulting in those portions of the population who previously have not been able to afford it gaining access. Whilst this additional connectivity will aid development in the region, the influx of users will result in the number of vulnerable users who are unaware of the security issues surrounding computers and the Internet. The increase in vulnerable users may result in a rapid increase in malware infections and cyber-crime (Fryer, Merrit, & Trias, 2010; Jansen van Vuuren, Phahlamohlaka, & Brazzoli, 2010; van Niekerk, 2010b); this vulnerability may also be exploited for IW purposes. It is also predicted that bots will infect 80% of the computers in Africa (Carr, 2010); some believe this is nearly realised (Jansen van Vuuren, Phahlamohlaka, & Brazzoli, 2010). Such a high infection rate may result in the African Internet becoming a massive botnet that can be used in large-scale cyber-attacks; this will have severe impacts on network performance in Africa. Whilst these researchers have focused on broadband services in general, Goodman and Harris (2010) focus on the security problems that the rapid proliferation of mobile phones may cause. The premise is similar: the high prevalence of mobile devices combined with the predicted future security problems and vulnerabilities for the mobile infrastructure and devices will result in growing susceptibility of African nations to cyber-attacks and cyber-crime. The lack of general information security awareness is also noted as a contributing factor (Goodman & Harris, 2010). It was reported that the monetary loss due to cyber-crime in South Africa is estimated at R10.9 billion for 2010 (Symantec Corporation, 2011b).

The SADC region is already experiencing high malware infection rates; Figure 5.17 shows the infection rates of this region according to the Microsoft Security Intelligence Report (Microsoft Corporation, 2009; 2010a; 2010b; 2011a). The infections are measured in CCM, which is the number of computers cleaned by the Microsoft Malicious Software Removal Tool for every 1000 computers checked (Microsoft Corporation, 2011a). From this it can be seen that some of South Africa's neighbouring countries, namely Zimbabwe, Lesotho, and Swaziland, have very high infection rates. South Africa was below the worldwide average in the first half of 2009, but since then is higher than the average.

Table 5.9 shows the ranking of the SADC nations in terms of infection rate; this is out of 212 nations for 2009 and the first half of 2010, then 125 nations for the second half of 2010. From his it

can be seen that South Africa is in the top quarter of nations in terms of infection rates; some neighbouring nations are even higher. The general trend is that the SADC nations listed here are increasing in their ranking; this indicates that infections are becoming more prevalent in these countries compared to the rest of the world.

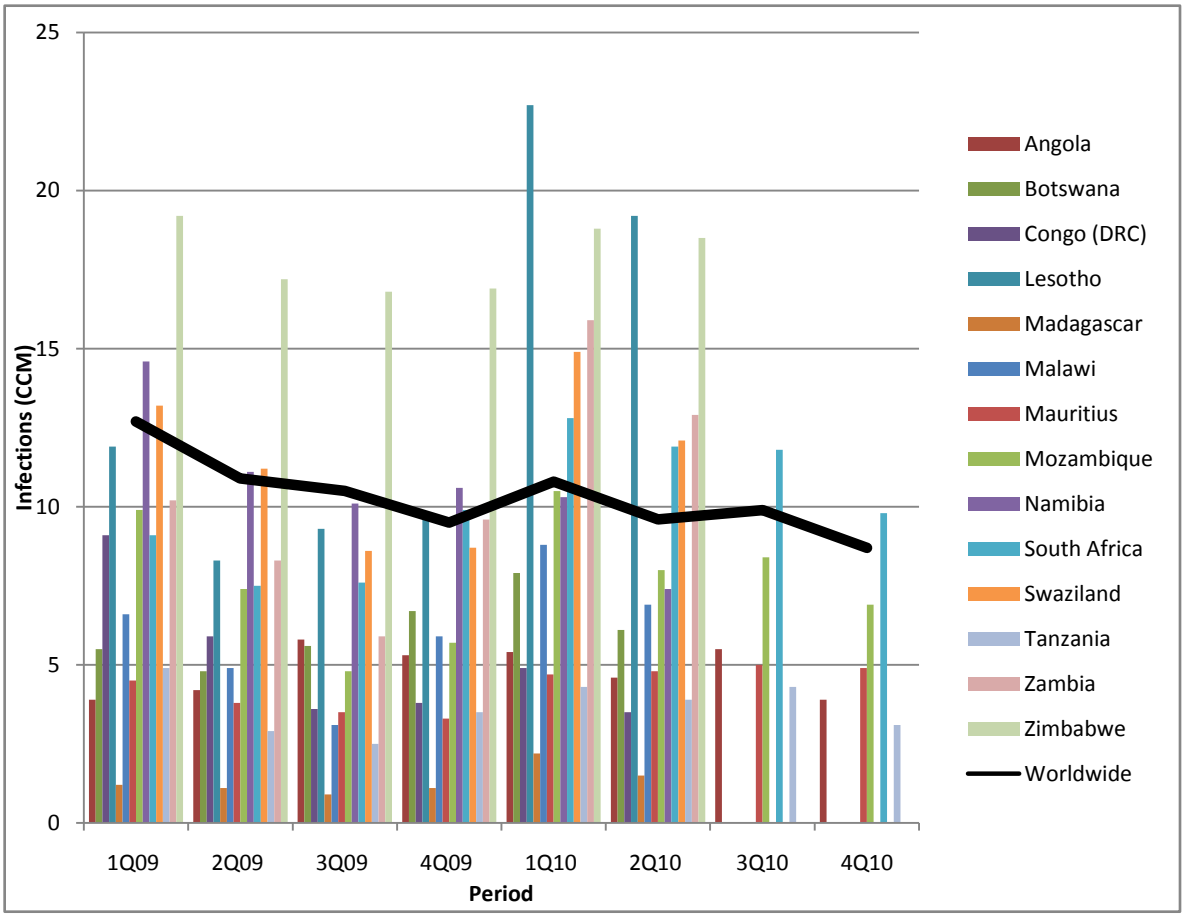


Figure 5.17: Infections of SADC Countries, source: Microsoft Security Intelligence Reports (Microsoft Corporation, 2009; 2010a; 2010b; 2011a).

Figure 5.18 shows the bot infection rates of African nations for July 2009 to June 2010. As can be seen, South Africa has high infection rates compared to the worldwide average. The other African nations listed are either close to or much lower than the worldwide average. The infection rates are again in CCM. Table 5.10 shows the ranking of the African countries out of 86 nations. This again shows that South Africa is very high in the rankings. This then confirms the potential of at least South Africa to become a cyber-weapon as stated by Carr (2010). Worms appear to be the prevalent

malware type in South Africa, miscellaneous unwanted software and Trojans; these are also higher than the worldwide average (Microsoft Corporation, 2011b).

Table 5.9: The Ranking of SADC Countries for the Highest Number of Infections of 212 Countries, source: Microsoft Security Intelligence Reports (Microsoft Corporation, 2009; 2010a; 2010b; 2011a)

Country	1Q09	2Q09	3Q09	4Q09	1Q10	2Q10	3Q10	4Q10
Angola	166	143	104	112	127	124	78	81
Botswana	136	132	108	78	90	96		
DRC	82	104	145	144	138	152		
Lesotho	52	72	53	49	14	12		
Madagascar	208	208	210	201	197	201		
Malawi	119	128	159	95	80	85		
Mauritius	155	151	149	155	143	121	81	69
Mozambique	70	88	124	102	59	68	50	53
Namibia	38	43	46	40	61	79		
South Africa	84	86	76	47	50	44	30	32
Swaziland	44	41	63	61	35	43		
Tanzania	148	175	184	152	148	142	93	90
Zambia	68	73	103	51	30	35		
Zimbabwe	22	20	19	13	22	16		

The data presented for the infection rates are only valid for legitimate Windows operating systems and not for pirated copies. Therefore the infection rates may be much higher as it is estimated that Africa had a software piracy rate of 59% in 2009 (Business Software Alliance, 2010). Usually, pirated software remains unpatched; this leaves a number of illegal systems vulnerable to infection and attack. Another concern raised by the increasing broadband access in Africa is that this may lead to increased software piracy in the region, resulting in more vulnerable systems (Fryer, Merrit, & Trias, 2010). The specific piracy rates in some African nations are as follows (Business Software Alliance, 2010):

- Algeria – 84%
- Botswana and Kenya – 79%
- Nigeria – 83%
- South Africa – 35%
- Zambia – 82%
- Zimbabwe – 92%

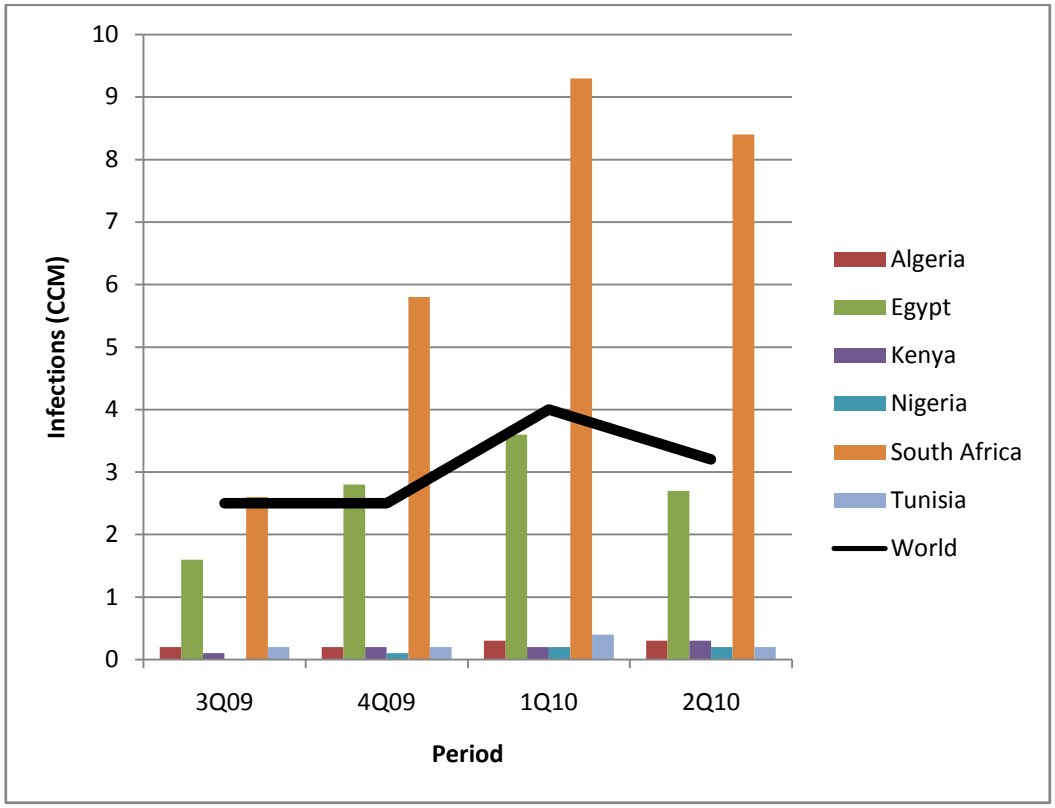


Figure 5.18: African Botnet Infections, source: Microsoft Corporation (2010c)

Table 5.10: The Ranking of African Countries for the Highest Botnet Infection Rate of 86 Countries, source: Microsoft Corporation (2010c)

Country	3Q09	4Q09	1Q10	2Q10	Avg. Inf.
Algeria	78	78	80	79	79
Egypt	49	30	42	41	44
Kenya	82	80	83	80	81
Nigeria	84	84	84	83	84
South Africa	30	6	11	6	7
Tunisia	79	81	78	84	80

Whilst South Africa had a relatively low rate it had a high commercial value of $US 324 million for the pirated software, which is ranked in the top thirty in terms of actual value (Business Software Alliance, 2010). This indicates that there are a number of vulnerable systems in Africa that have not been consider in the infection rates; and these systems are vulnerable to attack. Therefore Africa may become a launching point for cyber-attacks and cyber-crime.

In 2009 South Africa was ranked ninth by the Internet Crime Complaint Centre in terms of the number of complaints, contributing 0.15% of the total number of complaints; South Africa was also ranked seventh in terms of perpetrators, contributing 0.7% of the total (Internet Crime Complaint Center, 2010). Three other African nations appeared in the top ten perpetrators: Nigeria was ranked third and contributed 8%, Ghana was ranked sixth contributing 0.7%, and Cameroon was ranked ninth contributing 0.6% (Internet Crime Complaint Center, 2010). In 2009 there were four African nations in the top ten perpetrators, contributing 10% of the total. In 2010 South Africa dropped off this list, leaving Nigeria ranked third contributing 5.8%, and the rankings and contributions by Ghana and Cameroon remained unchanged. South Africa moved to sixth place in terms of complaints, contributing 0.2% (Internet Crime Complaint Center, 2011). The contribution and complaints originating out of Africa is considerably high compared to the generally low penetration of the Internet and computers in the region (presented in Section 2.8.4.3); this indicates that Africa may already be a launching point for international cyber-crime activity.

Figure 5.19 shows the total number of South African websites that were hacked from 1 January to 20 December 2010; Figure 5.20 shows the number of South African Government websites that were hacked in this period. A total of 19 335 websites, of which 74 were government, were hacked (HackingStats.com, 2010). This indicates there is a potential susceptibility to hacktivism and illegitimate access to websites. In the first half of 2010, there were 0.12 sites hosting malware and 0.25 phishing sites for every 1000 hosts; this decreased to 0.10 malware hosts and 0.11 phishing sites in the second half of 2010 (Microsoft Corporation, 2011b).

As the study focuses on the mobile infrastructure, specific concerns and incidents regarding the South African mobile networks should be covered. The main incident was the SMS banking scandal of 2009, presented in Section 5.5.1.3. As mentioned in Section 5.3.1, a bombing campaign in Cape Town also utilised mobile devices as detonators, similar to the IEDs used in Afghanistan (Sabasteanski, 2005). There is concern over the stability of performance of the South African mobile providers. In 2009 there were major problems with the three major mobile operators where calls were dropped and SMS were not delivered or delayed due to capacity issues (Ajam & Bailey, 2009). In June 2011 the major networks also experienced outages due to "network glitches" (Mtshali, 2011); this was followed by statement by the South African communications regulatory body that the three main mobile networks do not meet the performance requirements (South African Press Association, 2011). There have been reports of attempted intrusions into the telecommunications networks (Scheepers, 2009).

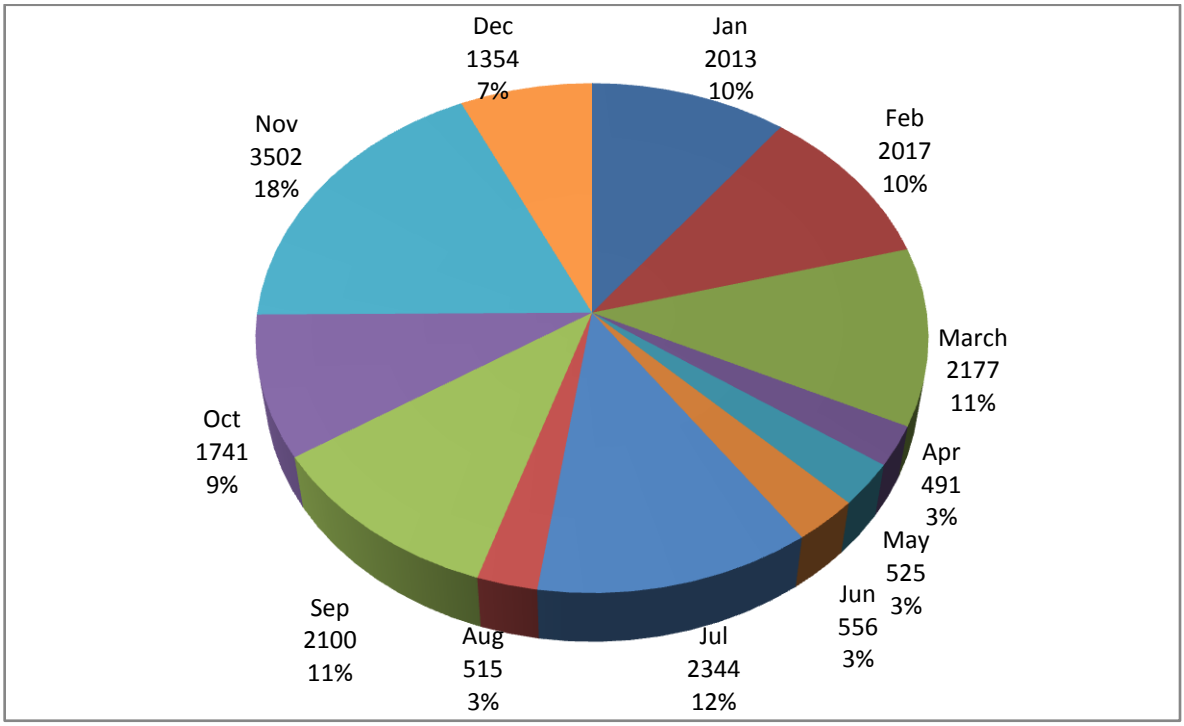


Figure 5.19: South African Webpages Hacked, source: (HackingStats.com, 2010)

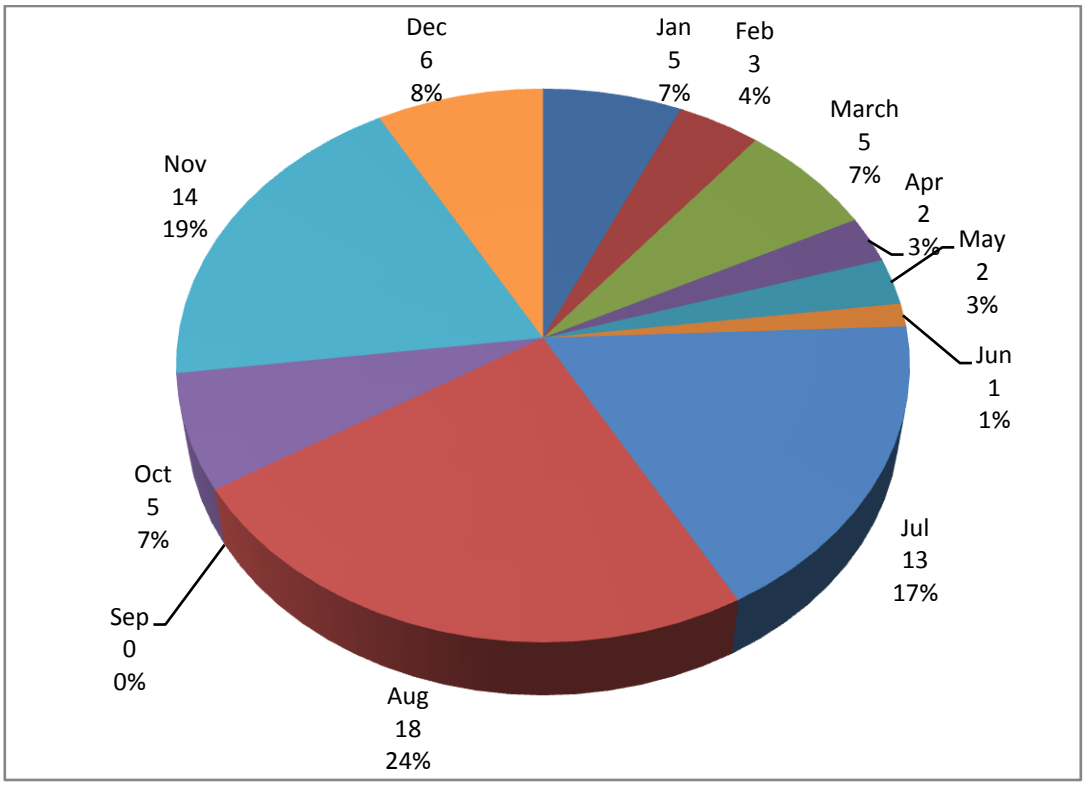


Figure 5.20: South African Government Websites Hacked, source: (HackingStats.com, 2010)

At the time of writing, South Africa has not been the target of a large-scale cyber-based IW attack. However, there have been reports of limited DoS attacks in addition to the attempted penetrations of the telecommunications networks and the SMS banking scandal; some believe a large scale attack against South Africa is unlikely unless there is an event or political decision that a group or nation takes offence to or attempts to exploit (Scheepers, 2009). Major global events may also see a rise in cyber-crime; this occurred during the 2008 Beijing Olympic Games (Dennis, 2010). In 2009 there were reports that the Dalai Lama had been refused entry into South Africa due to pressure from China (South African Press Association, 2009a); this occurred again in 2011 (Philp, 2011). The 2009 incident surrounding the Dalai Lama was during the period of the GhostNet espionage (see Section 5.4.1.7); it may have been possible that allowing the Dalai Lama entry may have upset Chinese groups, which would have resulted in cyber-attacks aimed at South Africa. There is also a contradictory view that as South Africa appears to have close political relations with China, those that oppose China may target South Africa (Jones, 2009). The economic interest in Africa shown by China and India (Broadman, 2008) may result in the continent becoming the subject of an economic information war between the two neighbours, especially as India already appears to have been a target of cyber-espionage attributed to China (Information Warfare Monitor and Shadowserver Foundation, 2010). Whilst there has been an increase in the broadband capacity in South Africa due to the new undersea cables, there measured throughput in September 2010 for the cables on the East coast was 500 to 1000 Kbps (Cottrell & Kalim, 2010). Given the magnitude of the DoS attack against Myanmar in November 2010 which peaked at over 10 Gbps (Labovitz, 2010), South Africa will be vulnerable as such an attack would severely degrade or completely network connectivity. Outages of the Seacom cable that were experienced in 2010 and 2011 illustrate the impact should one or more of these cables be forced offline through a DoS attack or by physical means; whilst websites internal to South Africa are unaffected, the international connectivity was affected (Tubbs, 2011). As more undersea cables become active, the impact of a single cable outage will not be as noticeable; however the current impact of such an outage illustrates that South Africa is vulnerable to large-scale DoS attacks.

Whilst South Africa has not experienced major cyber-related attacks, there has been activity in the surrounding region. Numerous instances of internal, politically-motivated, IW in Zimbabwe were reposted by Mavhunga (2008). These include DoS attacks on online news media, anti-government hacktivist attacks, jamming of radio stations, and monitoring of the Internet and mobile phones. It was also reported that foreign aid was received to enable the monitoring of Zimbabwe's Intelsat

gateway and the jamming of radio broadcasts (Mavhunga, 2008). As discussed in Section 5.6, the use of mobile phones and online social media in Mozambique, Tunisia, Egypt, Uganda, Swaziland, and Cameroon also shows the growing prevalence of cyber-based activity in Africa. Many of these countries are in South Africa's sphere of influence as part of the United Nations and African Union; therefore this activity is of relevance to South Africa. South Africa has also experienced internal riots and violence related to xenophobia (Karrim, 2009) and dissatisfaction due to poor service delivery (Brooks, 2009; Smith, 2009); at one stage the military was deployed in order to mitigate the xenophobic violence (BBC, 2008). This violence and frustration could be leveraged in a psychological attack through SMS services and possibly social media to further incite violence or rioting.

A concern is that there are only currently three African nations with operational computer security incident response teams (CSIRTs): Kenya, Tunisia, and Mauritius, with reports of Morocco, South Africa, and Egypt developing CSIRTs (CERT-Africa, 2010a; 2010b). The lack of an operational CSIRT in South Africa may result in vulnerabilities, as the CSIRT provides the capability of gaining a broader picture of security incidents in South Africa (Scheepers, 2009). The draft cyber-security policy released by the South African Department of Communications in 2010 allows for the development of CSIRTS (Department of Communications, 2010), however political uncertainty of mandates and operations results in delays; and in addition other circumstances have resulted in some projects to establish a CSIRT in South Africa being terminated prematurely (Grobler & Bryk, 2010). Goodman and Harris (2010) also cite the lack of national CSIRTs in Africa as being problematic, as these would aid in mitigating the predicted security issues regarding the increasing accessibility of mobile and broadband services.

5.7.1.2 South African Information Security Related Legislature

The main pieces of legislation in South Africa that cover information security are:

- The Electronic Communications and Transmissions Act (ECT, 2002): this is the basic legislation prohibiting unauthorised access to information or communications and the interception or disruption of communications.
- The Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA, 2002): this provides detailed legislation regarding the interception of communications, and makes provision for lawful intercept. It also required the registration of all mobile numbers.

- Protection of Personal Information Bill (POPI, 2009): This legislation is still to be enacted, but it aims to provide guidance regarding the security and responsibilities of personally identifiable information.
- Electronic Communications Security Pty (Ltd) Act (ECS, 2002): This provides for an organisation to provide communications security for the South African Government and related agencies.
- King III Report (King Committee on Goverance, 2009; PriceWaterhouseCoopers, 2010): This sets the standards for information governance, and states that the senior executive of an organisation is ultimately responsible for the information and its security, and that the organisation must bear the risk associated with the information.
- Draft Cybersecurity Policy (Department of Communications, 2010): this makes provision for a CSIRT, but focuses mainly on cyber-crime, and does not specifically mention a concerted attack on South Africa's information and communications infrastructure.

None of this legislation has faced a major test in court; therefore their effectiveness cannot be assured. There is also the concern that due to inequalities in international laws, those that are available in South Africa would not be applicable or enforceable should the perpetrator be located internationally. It is apparent that the need for a strong legislative framework and information-security related agencies in South Africa is recognised. As South Africa is a late-adopter, there will be the benefit of hindsight from other international attempts that may aid in the introduction of a strong legal framework; however, it is essential to introduce a strong technical framework to support it. These frameworks will provide the mechanisms with which to protect South Africa's infrastructure.

5.7.1.3 Section Summary

Mobile communications are prevalent in South Africa; however due to the undersea cables that are being introduced there may be a growth in the broadband subscriptions. This is cause for concern due to the lack of security awareness; the influx of new subscribers may result in a rise in cyber-crime and attacks. South Africa has not experienced large-scale attacks; however there appears to be high malware infection rates, particularly of bots. This could be linked to software piracy; and the concern of an African Botnet being used as a cyber-weapon may be feasible to a certain degree. There is also a degree of website hacking; this indicates that many systems are vulnerable. There

have been a number of incidents in Africa that are related to IW activities; these are relevant to South Africa due to their geographical proximity.

Concern has been raised that South Africa may become a target for attack due to apparent political leanings. There have been reports of intrusion attempts into the telecommunications infrastructure; and a cyber-crime attack has managed to compromise a mobile network provider. There are also reports of network problems with the mobile network providers; this may result in a vulnerability. At the time of writing South Africa does not have an operational CSIRT; this is also considered a problem as there is no central body to co-ordinate responses or provide a holistic view of incidents in the country. There is legislation that covers cyber-related issues; however, they focus more on cyber-crime and have not been tested in court.

5.8 Chapter Summary

The chapter presented incident and trend analysis, where the information was gained from documents. The benefits of strategic information in an asymmetric conflict were illustrated, and its application to the cases of information warfare and security was presented. Trends in conflicts show a shift towards low-intensity conflicts which exhibit asymmetry; there appears to be improvisation with the use of commercial technology. Combined with the convergence of ICT technologies this is resulting in a convergence of the IW functional areas; military IW operations may be required to target communications infrastructures that are predominantly civilian.

The incidents presented in Section 5.3 illustrate that the Internet is becoming weaponised; the majority of incidents exhibit a breach of confidentiality in the form of cyber-espionage. There is also the appearance of large-scale DoS attacks, this appears to correspond to a shift in the focus of malware to botnets. The incidents illustrate the vulnerability of systems and infrastructures to cyber-based attacks; the Stuxnet worm can be seen as a turning point as it was designed to target specific industrial control devices. The national CSIRTs show a general increase in the number of reported incidents. The most prevalent reported incident type across six CSIRTs is malware; followed by intrusions, attempts at intrusions and scanning. Denial of service attacks are not as prevalent, but do occur.

The mobile security incidents indicate that vulnerabilities in the mobile infrastructure may be found and exploited; this has been done to breach both confidentiality and to broadcast illegitimate messages, thus impacting on integrity due to uncertainty regarding the authenticity of the messages

origin. Previous research raised concerns over the possibility of a DoS attack on the mobile infrastructure. Mobile malware appears to target the most popular devices; the focus is shifting towards Google Android at the time of writing. Most mobile malware appeared to either provide direct provide financial gain through the use of SMSs to prime rate numbers, or breach confidentiality to gain account information. A worrying trend is the migration of PC-based malware to mobile platforms, and the possibility of mobile-based botnets.

Online social media combined with mobile devices has proven to be an excellent command and control tool for mass demonstrations. Web 2.0 technologies have been used as a vector for targeted attacks against individuals and communities in what appears to be an attempt at espionage; malware has also been distributed via social networking websites. There is concern that social media may result in serious information leaks; this has occurred and even affected military operations. It was shown that Web 2.0 technologies can be a versatile tool in IW as it is capable of mass communications as well as targeting individuals.

Mobile devices are prevalent in South Africa; however there have been problems with the major mobile networks. Political alignment may result in cyber-based attacks against South Africa, however none have been seen at the time of writing. There are reports of low-scale attacks and penetration attempts against the telecommunication infrastructures. Other nations in Africa have experienced IW type activity. African nations exhibit high infection trends, and South Africa has a particularly high infection rate of bot infections; this corresponds to concerns over an African botnet. The increase in broadband availability may result in higher infection and software piracy rates; and a rise in cyber-crime and attacks. The lack of an operational CSIRT and the fact that the main legislature related to cyber-incidents may result in high-level vulnerabilities.

Chapter 6. Primary Data

6.1 Introduction

The results and discussion of the primary data collected during the study is presented in this chapter. Section 6.2 presents the expert interviews, Section 6.3 presents the research workshop, and Section 6.4 presents the pilot survey of the informal sector. The findings of these sections are summarised in Section 6.5.

6.2 Expert Interviews

This section presents the results and discussion of the interviews conducted with experts. As described in Section 3.4, the interviews were semi-structured according to the respondents' specific area of speciality and whether they were international or South African. Email was used to facilitate the interviews. The interview responses are to be anonymous; therefore any quotes will refer to the respondent as either I1, I2, to I5 for international respondents, and SA1, SA2, to SA7 for South African respondents. The objectives of the interviews was to solicit opinions regarding CIIP in South Africa and threats to CIIP, the role of the mobile infrastructure in the national critical information infrastructure, and threats specific to mobile communications and the mobile infrastructure. These opinions will be used in determining the criticality of the mobile infrastructure, and vulnerabilities due to the level of implementation of CIIP in South Africa, as well as the perceived threats.

A total of twelve responses were received; five from international respondents and seven from South African respondents. Table 6.1 gives a breakdown of the sectors the respondents are currently employed in. There is an even split between the total number of those with an academic and industry background (five each), with two South African military respondents. Some respondents also provided additional documents to support their responses. The respondents were identified by their publications, or were professional acquaintances that are employed in the information security, critical infrastructure protection, or IW fields. All of the international respondents have authored a book or report. The military respondents and one South African industry respondent are professional contacts and are employed in the IW and information security fields. The remaining South African respondents were identified by their research output, and have at least a master's degree.

Table 6.1: Respondent Breakdown				
Location	**Industry**	**Academic**	**Military**	**Total**
International	3	2	0	**5**
Local	2	3	2	**7**
Total	**5**	**5**	**2**	**12**

An initial analysis of the responses was conducted by coding the responses into very negative, negative, positive, very positive, or unsure. The very negative or very positive responses are where the respondent placed emphasis on their response. Unsure indicates that the respondent did not give a clear negative or positive response (they discussed both positive and negative aspects), or indicated they were unable to comment. A summary of responses for each question will be provided in pivot tables, following the initial analysis. This is followed by a more detailed analysis specific to individual answers. The following sections present the responses and the analysis.

6.2.1 Awareness of Critical Information Infrastructure Protection in South Africa

Respondents were requested to indicate if they are aware of any CIIP efforts and policies in South Africa. There is an even split between South African respondents who are and are not aware of CIIP (three each); one is unsure. The lack of awareness of CIIP in South Africa is not unexpected due to the international respondents, who will most likely be more concerned with CIIP in their respective nations. The responses are summarised in Table 6.2.

Table 6.2: Awareness of CIIP in South Africa				
Location	**No**	**Unsure**	**Yes**	**Total**
International	4	0	1	**5**
Local	3	1	3	**7**
Total	**7**	**1**	**4**	**12**

The one international respondent who is aware of CIIP in South Africa had contact with a corporation in South Africa "which started a pilot research project for CII identification and protection in 2007" (I5).

Two South African respondents are aware of CIIP, but could not provide specific details. The other mentioned the laws and standards: "The Electronic Communications Act, RICA, King III, Privacy Bill" (I1). The laws referred to here are (in order): the Electronic Communications and Transmissions Act (ECT, 2002), The Regulation of Interception of Communications Act (RICA, 2002), The King Report on Governance for South Africa (King Committee on Goverance, 2009),

and the Protection of Personal Information Bill (POPI, 2009). The respondent who is unsure has not investigated the issue, however mentions references to CIIP made by the Draft Cybersecurity Bill of South Africa.

The mix of awareness of the South African respondents is more ominous; this indicates there is no major consolidated effort for CIIP in the country, or alternatively it is not public knowledge. Should there be a major project that is not public, it defeats the purpose as the majority of private organisations will not be able to benefit or contribute. The sufficiencies of the South African CIIP efforts that are known are investigated in Section 6.2.2.

6.2.2 Sufficiency of CIIP Efforts in South Africa

The respondents were asked to comment on the sufficiency of any CIIP efforts in South Africa, and to compare South African CIIP to international efforts and policies. The objective is to solicit perceptions from experts of possible shortcomings; these may result in a vulnerability from a legal or governance perspective of critical systems.

The South African respondents were asked if the CIIP efforts in South Africa are sufficient; however, one international respondent provided a comment that is relevant, and will be considered. One South African respondent did not wish to comment and two were unsure; the majority responses were that the efforts are not sufficient. The responses are summarised in Table 6.3.

Table 6.3: Are the CIIP Efforts in South Africa Sufficient

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	1	0	0	0	0	**1**
Local	0	5	2	0	0	**7**
Total	**1**	**5**	**2**	**0**	**0**	**8**

When asked to compare the South African CIIP efforts to international efforts, three responses indicated that it was not as good, one was positive, two were unsure and one chose not to answer. Table 6.4 summarises the responses.

Table 6.4: Comparing SA to International CIIP

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
Local	1	3	2	1	0	**7**

The specific responses for the summaries presented in Table 6.3 and Table 6.4 overlap, and are presented in more detail here. The very negative response and one negative response in Table 6.4 both considered a lack of a computer security incident response team (CSIRT) as reasons for the poor comparison of South Africa's CIIP to those internationally:

- "Very bad - we do not even have a proper CSIRT" (SA7);
- "Lack of a national CSIRT (or CERT) makes it harder to coordinate potential cyber attacks both internally and internationally" (SA2).

The negative responses to the sufficiency of South African CIIP and the poor comparison to international efforts yielded many comments regarding the slow adoption by the relevant stakeholders:

- "Unclear and overlapping mandates in government departments (NIA, DOC, DPSA, SITA, SANDF); slowness in adopting national CIIP policies and strategies" (SA2). The agencies referred to in the quote are (in order) the National Intelligence Agency, the Department of Communications, the Department of Public Service and Administration, the State Information Technology Agency, and the South African National Defence Force;
- "No, not sufficient yet. It must be a much more overt and coordinated effort to involve all the role players in government and industry" (SA2);
- "The increase of regulation and legislation in SA has been slow" (SA1);
- "South Africa needs a decent (CIIP) policy and national strategy" (SA6).

However, there is indication that South Africa is moving in the right direction:

- "With the increased importance of IT governance in recent times the impact should be felt in a greater manner in industry" (SA1);
- "The SABS [South African Bureau of Standards] does make an effort to keep track of standards implemented by ISO regarding IS, and has continued to show support of standards that enhance the security framework" (SA1);
- There are many organisations in SA that are making efforts to improve security due to the ever present threat of reputation loss" (SA1);
- "The new National Cybersecurity Policy of the Dept of Communications (publish[ed] in the recent Government Gazette for public comment) will, if implemented, create a forum for better national cooperation on this" (SA2).

The National Cybersecurity Policy referred to in the last point was released for public comment in February 2010, and allows for the implementation of national CSIRTs and forming partnerships both internationally as well as locally (Department of Communications, 2010). A response comparing South Africa in an international context indicates that the overall attitude towards cyber-space in general is incorrect: "RSA [Republic of South Africa] lacks a cyber mindset" (SA6). A negative comment indicates there is no specific reason for thinking that the South African CIIP is insufficient and does not compare favourably with international efforts; this therefore can be considered as a perception. Another negative response regarding the sufficiency of South African CIIP also appears to be perception based: "Whatever exists, I think we are far from sleeping soundly about CIIP in SA" (SA7).

The positive response regarding the comparison of South African CIIP to international policies was from the view that South Africa is considered as a developing country; however poor implementation is still a concern:

> "Considering SA's position as a developing country, our regulatory and legislative framework for information security compares well against developed countries. However, the implementation of good practice is still lagging, particularly in the SMME space where, until recently, the regulatory framework did not apply" (SA1).

The international response was making an assumption regarding the CIIP in South Africa based upon the CIIP in another country: "I am not aware of any but if they are like those in the U.S – they fall way short of what is required!" (I1).

From the number of negative comments, it is apparent that the perception of CIIP efforts in South Africa is that they are not sufficient; particularly regarding the lack of a CSIRT and slow deployment of regulations. This corresponds to the document analysis of the South African information warfare and security landscape, as discussed in Section 5.7. The international response implying that the efforts of the U.S. fall short is telling, in that the U.S. have had an operational CSIRT for many years; this indicates that South Africa has a long way to go before having sufficient protection of the critical information infrastructure. There is a definite need for CIIP in South Africa, as is indicated by the following comments:

- "All countries must develop strategies which are centralised or decentralised or both that need to identify what are the critical elements, the treats to them, their vulnerabilities and what needs to be done to ameliorate those vulnerabilities" (I2);

- "SA has been plagued by exploitations of Internet banking sites, loss of personal data by the financial industry etc. However, developed countries have suffered the same problems. The lack of promulgated privacy laws in SA might be an obstacle to further investment by other economies as the legislative framework is not strong enough to enforce organisations' compliance with stricter CIIP efforts" (SA1).

The responses indicate that the perception is that CIIP in South Africa falls short; the lack of a CSIRT and coordinated national strategy is a common theme. This results in a lack of situational awareness of the incidents, threats, and vulnerabilities that are prevalent in the country. There is some indication that the legislation revolving around information security is moving in the right direction; however it can be considered imperative that more effort is made in South Africa towards safeguarding the CIIP. Section 6.2.3 provides responses for possible solutions to improving CIIP.

6.2.3 Suggested Solutions for CIIP in South Africa

Respondents were asked to provide possible solutions (with particular reference to international policies already in place) for improving CIIP in South Africa; four South African respondents expanded on their answer given in Section 6.2.2.

A response states that all international policies would be relevant and beneficial to South Africa (SA6). Two responses indicate that EU policies are beneficial (SA1, SA2); one is very complimentary of the EU policies: "The directives promulgated by the EU, in my opinion, are typically ahead of their counterparts across the world. For example, their privacy and information security directives preceded local legislation by far" (SA1).

Other opportunities to improve CIIP that have been suggested include international and local co-operation:

- "South Africa should become part of international collaboration" (SA2);
- "We should also have national conferences to develop joint government / industry policies and plans in the same vain as the 'disaster management centres'" (SA2);
- "There are many examples internationally, and many CERTs and CSIRTs from which we can learn and re-use information. Many has indicated their willingness to help" (SA7).

From the shortcomings and strong points mentioned in Section 6.2.2, and the policies and solutions suggested above, South Africa should focus on the following activities:

- Further development of cyber-related laws;

- Development of CSIRT(s);
- International and internal collaboration and capacity building.

The recommendations and solutions will be discussed in more detail in Sections 8.7 and 9.7.

6.2.4 Threats

This question intended to solicit a range of responses regarding IW and information security threats to the critical information infrastructure, and the potential impact should these threats be realised. All twelve respondents provided one or more threats. The responses were categorised into broad themes; the number of occurrences for each theme are summarised in Table 6.5.

Table 6.5: Broad Themes for IW and Information Security Threats

Theme	No.	Theme	No.
Unawareness and complacency	5	Cyber-war and cyber-terrorism	2
Cyber-crime, hacking, and fraud	4	Denial of Service	1
Surveillance	2	Illegitimate control	1
General vulnerabilities	2	Image of corruption in South Africa	1

Eighteen threats were organised into eight themes. The most common theme was the lack of awareness and education of the end user (SA1, SA7), complacency and lack of awareness by the government (SA5, SA7); therefore the 'human' can be considered as a vulnerability (I4). Cyber-crime was also a common theme, where fraud (SA3), "general hacking" (SA4), criminal activity through the use of botnets (I3), and the financial implications of cyber-crime (I5) were raised. Surveillance (I2) with specific use of botnets to conduct the surveillance (I3), undetected software vulnerabilities (I1) and architecture vulnerabilities (I4) were also raised. Other themes include cyber-war and cyber-terrorism (I5, SA6), DoS attacks (SA2), illegitimate control (I2), and an image of corruption in South Africa with no repercussions for wrongdoing (SA7).

It was mentioned that the lack of education and awareness by business owners may lead to a lack of compliance, especially amongst the SMMEs as "no such compliance was necessary" (SA1) compared to those that larger organisations where compliance was required to regulatory frameworks. "The King III principle of 'apply or explain' might lead to explanations of 'lack of skills and experience, lack of funds'," which may result in an "opt-out reaction to something SMME's are not comfortable or familiar with" (SA1). In South Africa there appears to be a focus on business and "there is currently a great demand for connectivity this lead to the creation of a

security threat as the role out does not have the necessary imbedded security measures in place. The security measures seem to be additional add-ons" (SA5).

The concern with general hacking is that it "could seriously influence power, water and communications grids availability" (SA4). Cyber-crime can be considered to have the largest financial impact (I5), and in particular botnets could " be very lucrative sources of income through identity theft, fraud, blackmail and intelligence trafficking/espionage" (I3) and are described in more detail with methods to counter this threat:

> "These botnets are semi automated and spread quickly. Increasingly, they will run undetected for weeks to months to years because anti-virus signatures cannot keep pace. CI will increasingly become penetrated by bots. Once inside they can remain dormant until required for any range of applications. The source of these threats is very difficult to trace, but more important than attributing sources is simple mitigation. Put out the fire before looking for the arsonist. We are rapidly advancing techniques in this area which do not rely on traditional, fallible (but still important and necessary) signature-based systems" (I3).

More concern was raised over cyber-crime related activities, as opposed to cyber-war and cyber-terrorism. This could be due to the high prevalence and ever-present cyber-crime threat, as opposed to the occasional large-scale attacks on (or attributed to) nations, which are termed by the media as cyber-war.

These themes were then aligned to the IW models as described in Chapter 2 and Chapter 4; the occurrences for each category of the model is summarised in Table 6.6. From Table 6.5 and the content above, confidentiality can be seen to comprise of the surveillance and cyber-crime in terms of identity theft. Infrastructure availability concerns arise from malicious hacking and DoS attacks. Fraud impacts on the integrity of information, and illegitimate control reduces the integrity of systems. The attitudes and awareness of humans provides a broader context as incorrect attitudes towards information security may hinder efforts to improve security measures. The "other" category is comprised of software and architecture vulnerabilities and general cyber-crime.

Poor attitudes and awareness can be seen as a large threat, as these may result in insufficient protection for critical systems. Together with existing vulnerabilities, the integrity of these systems may then suffer, allowing breaches of confidentiality and possible denial of services. It should be noted that the lack of awareness came primarily from South African respondents; this corresponds

Table 6.6: Aligning Threats to the IW Models	
Theme	**No.**
Confidentiality / Interception	3
Availability / Denial and degradation	2
Integrity / Corruption	2
Human attitudes and awareness	6
Cyber-war	2
Other	3

to the same concerns discussed in Section 5.7. Cyber-war was cited to be the greatest threat in terms of effects (I5); the impact of a cyber-war was illustrated by the examples of Estonia, Georgia, and Myanmar/Burma in Chapter 4 and Chapter 5. South Africa has not been the victim of such attacks: "We seem to have been spared any significant attacks" (SA2), however due to the focus on business and not on security (SA5), the nation may be severely affected should such an attack occur due to lack of preparedness. However, it was mentioned that the security measures for both cyber-crime and cyber-war are the same (I5). What was unexpected was the omission of social engineering from the threats related to the critical information infrastructure; this however was raised as a threat related to the use of mobile communications, presented in Section 6.2.7.

6.2.5 Mobile Phones as Part of the Critical Information Infrastructure

The question aimed to solicit the opinions of the respondents regarding the inclusion of the mobile phone infrastructure and devices into the critical information infrastructure. This aids in establishing the criticality of the mobile infrastructure. Table 6.7 summarises the responses.

Table 6.7: Is Cell Phone Infrastructure Part of the Critical Information Infrastructure?						
Location	**Very Negative**	**Negative**	**Unsure**	**Positive**	**Very Positive**	**Total**
International	0	0	1	3	1	**5**
Local	0	0	1	5	1	**7**
Total	**0**	**0**	**2**	**8**	**2**	**12**

The vast majority of the responses indicate that cell phones and the related infrastructure can be considered as part of the critical information infrastructure; some reasons for the mobile phone infrastructure being considered as critical is due to the fact that they are part of the telecommunications infrastructure, which is considered as one of the five critical infrastructure sectors:

- "Information space, cyberspace, are CII. As part of this cyberspace, cell phones are part of the CII too" (I4);
- "A communications grid is essential to the survival of modern society; as such cellular telephony infrastructure can be seen as critical" (SA4);
- "Yes, it is Cyber Space peripherals" (SA6);
- "I believe that cell phones are an integral and essential component of the critical infrastructure and as such need [to be] protected: (I1).

Another reason that the mobile infrastructure can be considered as critical is that essential services and businesses make use of them, and may even be solely reliant on mobile communications: "Without question cell phones are part of the critical infrastructure. Many people and businesses have cut the copper line and only use cellular technology" (I1), who goes on to say that some "municipalities and some emergency services organization use the same cellular technologies as part of their dispatch and emergency communications systems." This falls under the concept of critical infrastructure interdependency, discussed in Section 2.6.2. The high usage of mobile communications services by industry and essential services implies that a major disruption of the mobile infrastructure could have serious negative consequences for a nation. The use of mobile phones by emergency services is echoed by other respondents:

> "Cellphones are definitely part of critical infrastructure. Much of government and industry are dependent on voice comms, but increasingly also and data communications via cellphone networks. Even security forces (police, defence force) are heavily dependent on cellphones and don't always have alternative systems in place." (SA2)
>
> "Yes. But not just 'phones' per se but mobile devices using cellular networks. In the case of 2G and 3G cell networks and phones, civilian (consumer) cell services often become the fall-back communications vehicle for first responders (a critical infrastructure sector) when their older radio systems are overloaded or insufficient for the task. Cops will routinely use private cells for police business because the radios can['t] manage data fast enough.
>
> With the deployment of 4G HSPA and LTE services, LAN-type speeds are available wirelessly at low cost with a range of simple interfaces (USB sticks, WiFi bridging, etc). These cellular services have superior range and telco-grade resilience, and will be

adopted by CI sectors for critical communications, where before they may have leased fibre, pulled cable or established private wireless networks using various technologies." (I3)

The prevalence of mobile devices compared to fixed line telecommunications in Africa was raised, indicating that the mobile infrastructure may be considered as more critical than other areas with higher fixed-line telecommunications infrastructures: "Cell phone play a critical role in connectivity especially within Africa. The demand for fixed line communications (Tellecom) is not the huge" (SA5).

The responses listed as unsure indicated that the criticality of the infrastructure would be determined by the use, and the definition of criticality used: "this depends on the definition of criticality that you use. I would argue that cell phones as physical entities do not per se count as CII. It depends who uses them to what ends" (I5).

With ten of the twelve responses being positive, the mobile infrastructure can be classified as critical. Reasons given are that it forms part of the telecommunications sector, which is considered as one of the five critical sectors, and the reliance of essential services on the mobile infrastructure. There are indications that due to the prevalence of mobile services in Africa, this infrastructure may be more critical than in other parts of the world.

Respondents were asked to expand on their answers and indicate if they believe there should be explicit CIIP policies for mobile infrastructure and devices. There were seven responses, which are summarised in Table 6.8.

Table 6.8: Explicit CIIP policies for cell phones

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	0	2	0	2	1	**5**
Local	0	0	0	2	0	**2**
Total	**0**	**2**	**0**	**4**	**1**	**7**

The five of the seven responses were positive, indicating that there should be explicit policies, and two indicated that there should not be explicit policies. Two responses cited the fact that the mobile phone infrastructure is essential, and should be explicitly considered in critical infrastructure protection policies:

- "I believe that cell phones are an integral and essential component of the critical infrastructure and as such need [to be] protected. Security practices and policies must incorporate cell phone infrastructure to protect nations and economies" (I1);
- "Of course, it would be foolish not to consider an integral part of the infrastructure especially one that is the main carrier of formal and informal information flows" (I2).

A negative response indicates that as the "cell phone infrastructure is part of the telecommunications infrastructure and should therefore already be covered by CIIP" (I5); the other indicates that policies may not be effective: "I am not sure they should. Security is a technical problem. I am not sure that “policies” are useful to address technical issues [as] such" (I4).

A response queries the suitability of current critical infrastructure policies in taking certain characteristics of the mobile infrastructure into account: "New cell phone technology does allow for Internet connectivity faster and easier. It is also not limited to one location/position. It allows for mobile connectivity. I am not sure if the CIIP policies do take this into consideration" (SA5). The fact that voice services have been operational for two decades indicates that there might not be a need for policies regarding those services; however, the newer data technologies may need explicit policies:

> "For cellular voice services - probably not. That paradigm has been operational for 20 years without the need arising. For 3G/4G data service through cell: absolutely. It should at the very least be policy that wireless threats be taken into account during design. Similarly, the types of subscriptions purchased from carriers for cellular data can be limited in policy (and even ISO [International Standards Organisation] standard[s])" (I3).

Of the seven responses considering explicit policies for the specific protection of the mobile infrastructure, five were positive. The change of technology brought about by the prevalence of mobile connectivity introduces new threats and vulnerabilities; whilst the CIIP policies should cover the mobile infrastructure, these new threats and vulnerabilities need to be taken into account. Therefore either existing policies need to be reviewed and updated, or additional policies need to be introduced to address the new threats and vulnerabilities.

6.2.6 Importance of Mobile Phones for Various Sectors

This section presents and discusses the responses regarding the importance of mobile phones for various sectors, namely: small businesses, large businesses, governments, militaries, intelligence and security services, and criminal or terrorist organisations. The objective of soliciting this information is to aid in establishing the perceptions of the respondents regarding the criticality of the mobile phone infrastructure. The responses are summarised in Table 6.9 to Table 6.14, with more detail given below the summary for each sector.

Table 6.9: Importance of Cell Phones to Small Business

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	0	0	1	2	2	**5**
Local	0	0	0	3	4	**7**
Total	**0**	**0**	**1**	**5**	**6**	**12**

Eleven of the twelve responses were positive, and one was unsure; this indicates that mobile phones are important for small businesses. A response commented that the mobile phones are "very important in terms of insecurity: vulnerability of data, conversation" (I4) for small and large businesses and government. Multiple responses considered the importance of cell phones to small business as critical as it is often their primary means of communication:

- "Very important it allows for communications and connectivity any time and virtually anywhere in the world by dialling only one number" (SA5);
- "In some cases the only communication tool that becomes vital to the business, especially in the case of informal entrepreneurs" (SA1);
- "Somewhat important for businesses that are geographically based, like shops. However, for some really small businesses (eg free-lance painters) and service industries like plumbers, it is often their ONLY means of being contacted" (SA2).

Table 6.10: Importance of Cell Phones to Large Business

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	0	0	1	1	3	**5**
Local	0	0	0	4	3	**7**
Total	**0**	**0**	**1**	**5**	**6**	**12**

As with small businesses, there were eleven positive and one unsure response; this indicates that mobile phones are important for large businesses. A response indicated that mobile phones are "to a large extent a communication tool" (SA1). The importance of global connectivity and communications (SA5) and insecurity (I4) was repeated; however, the importance in terms of business competitiveness and access to applications was raised:

- "Critical for competitiveness. 4G data services will become fundamental for future competitiveness and resiliency" (I3);
- "Extremely important - both voice communications and access to enterprise applications" (SA2).

From the responses, mobile phones are very important to business. Small businesses may be solely reliant on mobile phones for their communications; however larger businesses should have access to fixed-line telecommunications. However, mobile phones may prove to be very importance for competitiveness of both small and large businesses.

Table 6.11: Importance of Cell Phones to Government

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	0	1	0	2	2	**5**
Local	0	0	1	4	2	**7**
Total	**0**	**1**	**1**	**6**	**4**	**12**

Ten of the twelve responses are positive, with one negative and one unsure; this indicates that mobile phones do have importance to governments. A response indicated that mobile phones are "not so important" to the functioning of government as "there are many other ways to communicate" (I5); another echoed this, but indicated that for rural areas mobile phones may be more suitable: "government has established infrastructure in place including fixed-line technology. However, in more remote areas plagued by fixed-line theft, cell phones may prove more effective, but is clearly more costly" (SA1).

A response indicated that it is important, but should only be used "with special security contingencies" (I2); this was echoed by (SA5): "Important but it is a security risk. Additional security measures needs to be put in place." The security concern was repeated by (I4); however, another response considered mobile phones as an "extremely important means of communication, accessibility, provision of e-Government services to people and industries across the country.

Possibly the biggest growth area for e-Gov[ernment] in South Africa" (SA2). An alternative was suggested in that the government "will probably be more reliant on TETRA [terrestrial trunked radio] infrastructure than traditional cellular infrastructure in the near future" (SA4).

These responses indicate that there is some importance of mobile phones to government, however, they are unlikely to be solely reliant on this form of communications, and additional security may be required. An incident discussed in Section 5.5.1.6 indicates there are concerns over military use of potentially insecure mobile infrastructures in stability or peace-keeping operations.

Table 6.12: Importance of Cell Phones to the Military

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	0	1	0	2	2	**5**
Local	0	1	0	5	1	**7**
Total	**0**	**2**	**0**	**7**	**3**	**12**

Ten of the twelve responses were positive and two were negative, indicating that mobile phones have some importance to the military. A response indicated that the mobile communications infrastructure is important for the military as it provides a cheap communications medium that is automatically upgraded for commercial reasons:

> "Very important. It remains a basically secure means of communication over wide areas where the infrastructure is in place, and it enables relatively cheap access to state of the art data communications and encryption systems (the GSM networks do all the upgrading for commercial reasons and the defence force does not have to upgrade their proprietary networks all the time)" (SA2).

Given that a number of incidents presented in Section 5.5 indicate that the mobile infrastructure is not necessarily secure, this response is somewhat surprising. The networks providers do upgrade their infrastructure, which does provide for a communications platform for the military; however the security of the networks may need to be complemented by other encryption methods. Other responses also indicate that additional security measures are required for the military to make use of the mobile infrastructure:

- "With special security contingencies" (I2);
- "Military will retro-fit commercial equipment and 4G technology in dedicated spectrum, but it will be operationally critical" (I3);

- "It is a major security risk as the service provider is not run by the military itself. Additional security measures and devices need to be added on" (SA5).

The possible future reliance on TETRA was repeated (SA4); and two respondents indicated that the military should rather rely on their own communications systems:

- "Hopefully NOT important! They should a) have a policy for use of mobile phones in military operations/service and b) have their own communication networks" (I5);
- "The military has in the past made use of radio and satellite networks effectively. The continued use of these technologies could prove more effective in the long term as cell phone usage is so dependent on available BSC towers" (SA1).

From the responses, it can be seen that there is some perception that mobile phones are important to the military; however it was raised that additional security mechanisms need to be in place, and that the military's own communications infrastructure should reduce the reliance on commercial communications systems.

Table 6.13: Importance of Cell Phones to Security and Intelligence Services

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	0	1	0	2	2	**5**
Local	0	0	1	3	3	**7**
Total	**0**	**1**	**1**	**5**	**5**	**12**

Ten of the twelve responses were positive, indicating that mobile phones will be important for security and intelligence services for both operational reasons and to be able to intercept communications:

- "Extremely important since it can be used for covert communications and almost any country in the world" (SA2);
- "… regarding RICA, cell phones pose a threat to security services. The registration of SIM [subscriber identity module] cards is viewed by some as an attempt at a local "Echelon", however for day-to-day operations, mobile communication may prove extremely important to security and intelligence services" (SA1);
- "Very important in terms of exploitation (intelligence)" (I4);

- "…it will be critical for operations. They will eventually adopt dedicated spectrum like military. They will also need the ability to intercept and perform surveillance on 4G voice and data traffic" (I3).

Despite its importance, security concerns of using mobile phones for operations were also raised:

- "With special security contingencies" (I2);
- "Big risk as the security cannot be trusted" (SA5);
- "Very important in terms of insecurity: vulnerability of data, conversation" (I4).

The use of mobile phones can therefore be seen as important to intelligence and security services as a source of intelligence through lawful interception of communications. For operational reasons (primarily for security services, as discussed in Section 6.2.5) it is still important, however extra security measures need to be taken.

Table 6.14: Importance of Cell Phones to Criminals and Terrorists

Location	Very Negative	Negative	Unsure	Positive	Very Positive	Total
International	0	0	0	2	3	**5**
Local	0	0	0	3	4	**7**
Total	**0**	**0**	**0**	**5**	**7**	**12**

All responses indicated that mobile phones are important for criminal and terrorist operations:

- "VERY they use them to detonate IEDs [improvised explosive devices]" (I1);
- "Very important. It is cheap and dispensable communications which allows for communications and connectivity anywhere. Due to the low level of security on the system it creates relative easy access into networks for criminal and or terrorist activities" (SA5);
- "Organized crime has already adopted the 4G technology and have history of remaining one-step-ahead generally. Terrorists and insurgents - though I have no experience dealing with them - are known to rapidly adopt technology in clever ways, but not in sophisticated manners. (They don't have the money or skills)" (I3);
- "Extremely important because it provides built-in security and cheap ways to change SIM-cards to avoid detection or by using multiple phones. It is only risky if the cellphone / device number is known to the security forces" (SA2);
- "Very important in terms of possibilities offered to attackers" (I4).

The use of additional security measures by these elements was raised by (I2). The use of mobile devices by criminal elements, and legislation attempting to curb this, was discussed in more detail:

> "The RICA act's attempt at registering all SIM cards, for example, is an attempt at reducing the anonymity of cell phone usage in the country, as internationally the use of unregistered SIMs have proven challenging to crime prevention activities. In SA, with a high crime rate, this is surely also a concern. However, the long awaiting Privacy Act and RICA seems at loggerheads as registering your SIM may reduce the privacy of your communication. Telecoms operators, similar to banks, should make the effort to secure their infrastructure and the devices used by consumers to protect their personal information, communication and any financial transactions occurring across the network" (SA1).

From the responses, it is obvious that the perception is that mobile phones are very important for criminal and terrorist elements. They have a rapid uptake of new technologies, and mobile communications provides mobility and is difficult to track. The Regulation of Interception of Communications Act (RICA, 2002) is attempting to mitigate the anonymous use of mobile phones, and reduce the effectiveness of swapping SIM-cards; however there is a concern that it may also contradict privacy legislation.

When considering the importance of mobile phone communications to various sectors, it is apparent from the responses that there is a perception that mobile communications is important to all sectors; however the military, government, and security services will probably not rely solely on the mobile phone infrastructure and would introduce additional security mechanisms when using them. The corporate sector is probably the most reliant on mobile phones; as criminal and terrorist elements make use of these technologies it is probably unlikely that the mobile infrastructure of their host nation would be targeted with a DoS attack, unless it would further their objectives.

6.2.7 Threats Related to the Mobile Phone Infrastructure

This question was intended to solicit a range of responses regarding threats related to the mobile infrastructure and use of mobile phones. The responses were categorised into broad themes; the number of occurrences for each theme are summarised in Table 6.15.

Table 6.15: Broad Themes for Mobile Phone Threats			
Theme	**No.**	**Theme**	**No.**
General vulnerabilities	4	Lack of awareness	2
Espionage/surveillance	4	Phishing and social engineering	1
Dependence & unavailability	3	SIM cloning	1
Cyber-crime / information theft	2	Lack of data verification	1
Malware	2	Cyber- and terrorist- attacks	1

A total of twenty-one threat concerns were grouped into ten themes. The most prevalent theme was general vulnerability concerns due to remote access to devices and infrastructure (I3, SA7), and vulnerabilities of the mobile infrastructure itself (SA5), particularly the home location register (HLR) (SA1). The concern of remote access to infrastructures through mobile devices is also raised in the research workshop (Section 6.3.2); mobile devices with wireless networking capability could be connected to the internal network and act as a wireless access point, bypassing the controls of the network perimeter. As the HLR contains subscriber information, particularly for the pre-paid billing (SA1; Enck, Traynor, McDaniel, & La Porta, 2005), penetration of this system may result in direct financial loss to the network providers (SA1). Corruption of these databases may also prevent subscribers from utilising the mobile services if their account balances are reset to reflect outstanding payments or no airtime. The HLR is also a central component, and overloading it may prove to be an effective DoS attack; this is assessed in more detail in Section 7.4. Espionage and the interception of communications was also raised four times (I1, I2, I4, SA2); a related theme of data and identity theft from a cyber-crime perspective was raised twice (I5, SA2). As there are a number of incidents presented in Section 5.5 which relate to attacks on the mobile infrastructure and malware that breaches confidentiality, these concerns are to be expected.

The reliance on the mobile infrastructure, and the problem of unavailability was raised three times (I2, SA2, SA5); this indicates a relevance to DoS attacks. If there is a heavy reliance on an infrastructure which is subjected to a DoS attack, the social and possibly economic impacts could be severe, as seen in the Estonia and Georgia attacks (Hart, 2008; Landler & Markoff, 2007). Malware was raised twice (I1, SA2); given the growing prevalence of mobile malware (presented in Section 5.5.2), more prominence of the malware threat was expected. However, mobile malware is still overshadow in numbers by traditional PC-based malware, and may therefore not be considered a major threat at the time of the interviews. The lack of user awareness (I5, SA1), with particular reference to phishing and social engineering (SA1), was also raised. The threat of social engineering

was surprisingly not raised for the general concerns in Section 6.2.4; its inclusion here indicates that it is still some recognition of its prevalence. Cloning of SIM cards (SA4), the inability to verify data or its origin (I2), and the use in terrorist and cyber-attacks (SA6) were also raised. The inability to verify the origin of data has implications for integrity through authenticity; the physical sender is assumed from the originating device, or who the communication claims to be. Concern of cyber-attacks with regards to the mobile devices and infrastructure was also illustrated; the relevance was illustrated in Section 5.5.1.6, where military activity gained access to national telecommunications systems.

These themes were then aligned to the IW models as described in Chapter 2 and Chapter 4; the occurrences for each category of the model is summarised in Table 6.16. The espionage and data theft combine to form six occurrences of confidentiality concerns; the integrity is a combination of the SIM card cloning, phishing, and poor data and origin verification. The availability and dependence concerns correspond to the availability in the IW model. Malware and use in attacks combine to form the misuse category, and the general vulnerabilities and awareness combine to form the "other" category. These concerns may result in breaches of confidentiality, availability, or integrity.

Table 6.16: Aligning Threats Related to Mobile Phones to the IW Models

Theme	No.
Confidentiality / Interception	6
Availability / Denial and degradation	3
Integrity / Corruption	3
Other misuse / use in attacks	3
Other	6

It was stated that mobile phones "are a real threat to any country's cyber security and CII" and that "their wide usage increase all forms of cyber risks" (SA7). Another concern raised was that "the security levels are decreased as the amount of users increases via the same tower to allow more simultaneous users" (SA5). It was suggested that during large events "the security is switched off" (SA5) to maximise the usage of the mobile infrastructure for the large crowds. Furthermore, it was stated that mobile infrastructures may be targeted due to the "significant impact of telecoms operators on the economies of the world" and that a DoS attack on these infrastructures "could cause great damage" to a telecommunications company (SA1). These responses indicate that there

is a concern that the widespread use of mobile phones and security issues surrounding this is a threat that could be leveraged to damage a nation's economic and social well-being.

There is also a concern that the introduction of mobile devices and technologies (including wireless technologies) into networks that contain industrial processes, such as supervisory control and data acquisition (SCADA) systems, may make them more susceptible to "autonomous bots" and other "anomalous traffic" which could cause damage (I3). This indicates a potential threat to critical industrial systems.

Solutions suggested by the respondents include:

- "We must develop me [new] technologies and techniques to catch software vulnerabilities and validate hardware and firmware are free of malicious circuitry or firmware" (I1);
- Awareness campaigns and improved organisational attitude and attention to mobile phone security (I5);
- "Increased situational awareness" of threats (SA6);
- Improve privacy legislation (I4).

The first response also indicates a possible concern over pre-installed malicious code or hardware in devices; this corresponds to incidents discussed in Section 5.5.1.6 regarding concerns over malicious content of devices and hardware.

The greatest perceived category of threat is to confidentiality; this could be due to the fact that many of the mobile phone incidents, discussed in Section 5.5, were related to breaches of confidentiality. The reliance on mobile phones raises the concerns of unavailability of the mobile networks; and the difficulty in verifying the validity of communications over mobile networks raises concerns of information integrity, particularly with regards to phishing attacks. Suggested solutions include improving awareness, legislation and technologies to mitigate these threats.

6.2.8 Summary

Twelve interviews were conducted to solicit opinions on the CIIP efforts in South Africa, the criticality of the mobile phone infrastructure, and threats to the critical information infrastructure and specifically the mobile phone infrastructure. The responses indicate that the CIIP effort in South Africa is not sufficient, and in general it falls short of international efforts. In particular the lack of a CSIRT was raised as a concern. The development of a CSIRT, international collaboration, and internal capacity were cited as possible solutions to improve CIIP in South Africa. The main

concern raised was the lack of awareness and incorrect attitude regarding information security and CIIP; this corresponds to findings from the document analysis in Chapter 5. By classifying the threats, confidentiality of information appears to be of greatest concern, followed closely by integrity and availability. The confidentiality concern is not surprising considering the rise of the concept of protecting personal identifiable information. The impacts of cyber-war were illustrated in Chapter 5.

The opinion is that the mobile infrastructure and phones do form part of the critical information infrastructure. Only seven responses provided opinion on explicit CIIP policies regarding mobile phones and infrastructure; these indicated that explicit policies may be useful and cover gaps created by smart mobile devices; however existing policies should cater for the mobile infrastructure to some degree. Of the specific sectors considered, the opinion was that mobile phones had some importance to all; however, the governments, military, and intelligence or security services would not be solely reliant on mobile phones, and additional security mechanisms would probably be put in place. It was indicated that mobile phones were important for gathering intelligence; and were widely used by criminal and terrorist groups. As with the threats to general CIIP, confidentiality is of great concern regarding mobile communications; this is due to the perceived ease of intercepting the wireless transmissions. Given that a number of the incidents discussed in Section 5.5 are related to breaches of confidentiality, this is again not surprising. Availability and integrity again appear to raise equal concern, and the misuse of mobile devices in attacks was also explicitly raised.

6.3 Research Workshop

The research workshop was held at The Riverside Hotel in Durban, South Africa, on the 9 June 2011. The objective of the research workshop was to discuss vulnerabilities and threats that are relevant to South Africa, from both an information security and risk perspective. Three main aspects were to be considered: general threats and vulnerabilities, those specific to mobile devices, and those specific to Web 2.0 technologies. This data was used to corroborate the data from the incidents and trend analysis and the interviews. Other relevant discussions also occurred.

There were seven participants, the candidate's supervisor, and the candidate, who facilitated the workshop and discussion. Three sessions were held of approximately 90 to 120 minutes each; the breaks between sessions corresponded with tea and lunch. The discussion was recorded by multiple

devices for redundancy and generation of the report and results; however the reporting of the discussion is de-identified.

6.3.1 General Vulnerabilities and Threats

The focus of these discussions was on the protection of personally identifiable information; this corresponds to confidentiality in the IW models. Concerns over incorrect attitudes and a lack of understanding and awareness of information security and risk management issues were also raised; this was cited as a major contributor to the lack of progress made in these areas in South Africa. A participant also raised the fact that it was reported that in the region of R195 million was stolen through cyber-related crime during 2008 to 2009. This figure may have been underestimated; a report indicated that the financial loss in South Africa during 2010 to 2011 was R10.9 billion (Symantec Corporation, 2011b). Even if the amount cited by the participant is underestimated, the intent is still clear: the financial loss due to cyber-crime is significant.

A concern raised was that organisations only introduce security and risk management measures to comply with mandatory standards and regulations; they do not appear to want to know or care about information security issues. In addition, SMMEs appear to have an attitude that the compliance for security and risk management does not apply to them and is only relevant to larger organisations; this was also raised in the interviews in Section 6.2.2. These incorrect attitudes may result in insufficient measures being introduced to safeguard information and protect systems; this contributes to the financial losses mentioned above.

Concern was raised that organisations and the employees do not fully understand risk; examples were given where employees and organisations assume that security and IT risk management was automatically handled by service providers to which they were outsourcing their requirements. Risk cannot be outsourced, and is carried by the owner of the information; therefore unless there is specific contractual obligations, the service providers will not provide security measures for the corporation. Chapters 3 and 4 of the King Report on Governance for SA 2009 (King III) (King Committee on Goverance, 2009) cover the audit and risk management responsibilities. An example was given where organisations do not understand the audit process, and mistakenly assume that auditing financial systems to ensure integrity of the financial information is a full security audit; they then believe they have had a security audit and have a false sense of security. It was concluded that the IT governance of South African organisations is generally weaker than those of international organisations. An example was provided of a talk where the speaker admitted that the

company had found personal information on random computers while becoming compliant with an international standard. The new requirements and legislation, such as King III and the Protection of Personal Information (POPI) Bill (Bill 9 of 2009) should improve IT governance by forcing organisations into taking responsibility and managing the risk of the information they have ownership of. A concern that organisations will move data to their facilities in other countries with more relaxed privacy laws may also be circumvented by the fact that Chapter 9 of POPI will require any data moving out of the physical boundaries of South Africa must be protected by equivalent laws or be contractually bound to the relevant South African legislation (POPI, 2009). The discussion indicated that these documents require the organisations, and in particular senior management, to take responsibility for the information stored or used by the organisation. The information needs to be classified by the data owner; they are responsible for the classification so that the relevant security measures are put in place to protect it. The IT departments do have responsibility in that they need to ensure that the technological security measures are performing correctly. It was suggested that there also be improved communications regarding the limitations of security measures, as listing the measures in place may give the impression that the information cannot be breached. As discussed above, risk cannot be outsourced, and service providers should be explicitly bound by contract to provide security services; however, it was suggested that providers, for example cloud computing service providers, should be responsible for the integrity of their infrastructure.

The participants confirmed that cyber-based corporate espionage and DoS attacks do occur in South Africa. The example of DoS attacks was that they usually occurred prior to major events, and specific online gaming or gambling websites were targeted. The high rates of malware infection and hosting in South Africa was also raised; it was commented that South Africa appears to be a staging point for malware attacks originating in Eastern Europe. The concern was raised that the increase in broadband availability without an increase in security awareness will probably result in an increase in the prevalence of malware infections and successful scams; this corresponds to the document analysis presented in Section 5.7. It was indicated that the concept of the African Botnet (Carr, 2010), presented in Section 5.7, may be realised. An example provided of circumventing the threat of keyloggers was to use biometrics in addition to passwords; thereby negating unauthorised access due to compromised logons. The biometrics, however, are expensive, and the additional security may not be necessary on many personal home computers. They will also not circumvent the impact of the botnets. Should infected systems in Africa be used to conduct large scale DoS attack, the

performance of the national information infrastructures (NII) on the African continent will also be degraded due to the traffic volumes.

In addition to the lack of awareness, it was raised that organisations and service providers do not always have the capability to prevent or detect attacks. In the DoS example, it was stated that the service providers were unable to assist or mitigate the attacks. It was stated that in many cases organisations only discover that their security has been breached when there is a noticeable irregularity, such as a large telephone bill that exceeds actual usage. It was also noted that many organisations were unable to implement basic information security controls correctly and are therefore unlikely to be able to implement more advanced security measures. An example provided was that organisations do not have proper system logging, or do not monitor the logs; this contributes to the inability of detecting security breaches. The Verizon Data Breach Report (Verizon, 2011) was cited as claiming that many breaches were avoidable, and occurred to incorrect implementation of security measures. This lack of awareness, combined with the apathy mentioned above, contributes to the significant financial losses due to malicious cyber-activity. Awareness training and proper management of security controls could therefore reduce the financial impact at a corporate level, and the national economy.

The main threats discussed were insider threats from current and ex-employees, crime-syndicates, and targeted attacks. It was indicated that employees who have recently left an organisation, or are about to leave, often feel dissatisfied and intentionally copy or release sensitive information as revenge. An example was given where an employee was selling information from a client database. It was raised that in most instances of fraud the perpetrator was eventually traced to a residential address and was an associate of an employee in the victim organisation. The rise in targeted attacks appears related to cyber-crime syndicates; the criminals themselves do not necessarily have the technical skills, but they target one or more individuals who do have the necessary access or skills. The information or capabilities provided by the targeted individuals allows the syndicate to access account information and funds; an example of this is the Vodacom SMS hack (Dingle, 2009), presented in Section 5.5.1.3. Examples were also given where CEOs are followed to the airport and their laptops are stolen, and a specific computer with was repeatedly targeted and stolen, despite other computers that were available to be stolen; it appears the theft was for the information and not the hardware. These targeted attacks show susceptibility of organisations and infrastructure; and could be used in intelligence gathering and planting of malicious software as part of a cyber-attack. These targeted attacks through insiders may result in an incident similar to the Athens Affair

(Prevelakis & Spinellis, 2007), where a Greek mobile infrastructure was penetrated, enabling the attackers to monitor the communications of high-ranking officials (Section 5.5.1.2).

It was proposed by a participant that the reason why organisations see large losses to cyber-crime is that older generations, who could hold senior management positions, fall for phishing scams more easily due to their habit of following requests without questioning the validity. However, examples were given where phishing scams are becoming so advanced that technical users also are caught; the RSA SecurID hack (Poulsen, 2011) is an example of this. It was also noted that during penetration testing, the workshop participant's organisation has a success rate of over 90% for social engineering tests. Social engineering was raised in the interviews for threats related to mobile communications, but not general threats. The inclusion of social engineering here indicates that it is indeed a highly successful threat in South Africa, and should not be discounted. It was also noted that vulnerabilities of specific organisations are inadvertently published by individuals who consult their peers online, and post configuration settings allowing potential attackers to identify the vulnerability; an example of a website dedicated to search and classify information on such online help-lines was given.

Solutions proposed by the participants include data classification; the de-identification of data; the introduction of security into the systems or software development cycle; and the introduction of a CSIRT. Data classification may be a suitable way of determining the security measures that need to be applied to the data; new legislation will require data classification, and the participants expect this to improve the protection of confidential information. Data classification can also be used to decide what information can be stored on cloud computing services, and what data needs to be kept on secure internal networks. It was suggested that instead of trying to protect all the data, it should be de-identified by assigning a unique identifier to the data; this identifier, and any data identifying individuals, should then be stored with high security and the remainder can be stored on the cloud or with reduced security as it is just random data. The introduction of security into the development cycle was proposed as being more efficient; an example of this was provided where security was the responsibility of the development team, however security experts were made available for consultation. This may reduce the number of vulnerabilities in software. The introduction of a national CSIRT will provide more effective co-ordination of incident response, and an improved warning and view of the bigger picture. This corresponds to the document analysis in Section 5.7 and the interviews in Section 6.2. However, a concern was raised that a CSIRT may be used to cut off or censor Internet access. It will therefore be important that the CSIRT is a public entity separate

from any agencies that may misuse it. Segregation of duties was also highlighted, where one person is not responsible for an entire process, which may aid in mitigating breaches and fraud.

It was also noted by the participants that there is a lack of information security related content in many academic degrees; it was also perceived that the degrees were inconsistent between different institutions. The lack of a professional or regulatory body overseeing the industry and academic degrees was also noted. Such a body, similar to the Engineering Council of South Africa, may aid in ensuring academic quality and consistency by accrediting degrees; and allow registration of professionals in the field. In particular, the concern was over many self-taught web-developers who do not have the necessary skills or understanding to effectively implement security. Providing for apprenticeships and registration of professionals will ensure the quality of those in the field, and reduce the number of vulnerabilities due to sub-standard development. Such a professional body may be able to address a number of issues: lack of awareness or understanding, apathy, aid in improving the inclusion of security in the development lifecycle, and improve education.

The protection of personally identifiable information appears to be the greatest concern measured by the time spent discussing it. This indicates that confidentiality is of primary concern; this corresponds to the results of the interviews presented in Section 6.2. As with the interviews, the focus appears to be on cyber-crime; however the examples illustrating susceptibility to attacks can also be exploited by a state or state-sponsored attacker. Awareness and incorrect attitudes was again raised; social engineering was illustrated to have high success rates. Other threats included insider threats and targeted attacks by criminal syndicates. New legislation and standards are expected to improve information security in general by forcing organisations into taking responsibility for the security and risk management of their systems and information; whilst this is aimed at mitigating cyber-crime, it will also aid in mitigating concerted cyber-attacks. The prevalence of malware in South Africa, and the concerns that South Africa is being used as a staging post for attacks, indicates that the concept of Africa becoming a cyber-weapon may be realised to some extent. The infection rates are expected to worsen as Internet access becomes more readily available. Proposed solutions include the continued introduction of relevant legislation and a CSIRT at a national level; at an organisational level solutions include data classification, segregation of duties, and de-identifying data. The use of biometrics in addition to passwords was suggested to mitigate unauthorised remote access. The formation of a regulatory body to oversee the industry was proposed as a method of ensuring quality and consistency in academic degrees and in professionals working in the field; thereby reducing vulnerabilities.

6.3.2 Mobile-Related Discussion

This section presents the workshop discussion that considered mobile-related issues. The perception of the participants was that the introduction of mobile devices into the organisations has been ad-hoc. Organisations may provide devices that are cheaper, with more flaws and less functionality; therefore employees may prefer to use their own better quality devices. Organisations have less control over the personal devices, therefore the security cannot be assured; this may introduce vulnerabilities into the organisation's network. It was raised that employees will still have their personal devices even if organisations force them to use supplied devices. It was noted that the use of personal laptops is often restricted, however there is less restriction on personal smart-phones; it was suggested that in these cases there is no realisation that the smart-phones have similar capabilities to laptops. Introducing mobile devices into the organisation's networks may result in a breakdown of the network's perimeter security. An example was provided where a penetration testing application was installed on a smart-phone, which was subsequently used to gain insider access to the corporate network. Mobile devices may provide rogue access points inside the network perimeter, thereby circumventing the perimeter security controls. The difficulty in managing the security settings and installed applications on mobile devices was also raised.

A suggested solution to these problems is that organisations employ MAC address filtering on the wireless network access points; should an employee wish to connect a personal device, it needs to be registered with the IT department who will ensure the relevant security measures are in place on the device. MAC address filtering will not aid in mitigating cases where users connect wireless capable mobile devices to computers on the internal network; continuous monitoring will be required to detect any rogue wireless access points. Shielding may be used to contain the wireless signals within the physical boundaries of the building; however, this may prove to be expensive.

Many smart-phones also have the capability of using wireless access points to make voice-over-IP (VOIP) calls, similar to Skype, as an alternative to the standard GSM or 3G mobile networks. These calls are susceptible to interception as they are carried by open IP networks; it was suggested that policies or requirements be introduced to encrypt or restrict VOIP calls to mitigate accidental breaches of information. Other peripheral devices, such as printers, also utilise wireless networks to communicate; poor security settings and allowing the wireless signal to penetrate beyond the organisation's physical boundaries may result in the information being intercepted. An example was provided where the wireless security was breached during a penetration test and the information being transmitted to the printer. Public wireless access points provided for convenience, or live in-

store device demonstrations, may also provide attackers with a method of accessing networks. An example was provided where demonstration devices were used to access online chat rooms; it is possible malicious activity could be conducted using these devices with no way of tracking the perpetrator.

Malware on mobile devices is also a concern; an example was provided of a mobile botnet utilising geo-location information to flood base stations with requests in specific locations; this can be seen as an example of a mobile DDoS attack. In response to a query by the candidate regarding reports of pre-installed malware on mobile devices (as described in Section 5.5.1.6), it was stated by a participant that some countries randomly sample imported components and devices for malicious code. In Section 5.5.1.6 it was presented that mobile infrastructure components from countries were banned due to concern of pre-installed malware. It was also stated that it is impossible to check for all possible pre-installed threats or previously unseen malware; a warning was also given that often the labels stating where a device was manufactured often means it was assembled there and individual components could be manufactured in another country. This suggests that restricting devices by manufacturing origin may not be successful in preventing pre-installed malware.

A concern was raised over the fact that RICA will not be as effective as intended. An example was provided where pre-registered SIM cards are being sold; these are apparently registered using false documentation and are being sold at a higher price. This was subsequently corroborated when arrests were made in conjunction to the selling of these SIM cards (Nair, 2011). Using in-store demonstration devices may also effectively circumvent the RICA process. It was agreed during the discussion that the act did not target the correct population; criminal elements will attempt to circumvent the required SIM card registration process, whereas law-abiding citizens will register their mobile numbers. It was noted that while the act requires service providers to make provision for intercepting communications, it does not specify requirements or methods to do so. This may result in sub-standard intercept methods that are ultimately ineffective. A potential problem that was raised is that of lawful interception of VOIP: this is a layered service, and providers of each layer may claim that it is the responsibility of other layers to make provision for the lawful intercept. Concern was also raised regarding the security of the information registered during the RICA process; it was noted that there is probably a repository of information that may be an attractive target for an attacker. Such information may potentially be used to clone SIM cards to pre-registered numbers. These concerns are similar to one raised in the interviews, where RICA and privacy legislation may contradict each other. These concerns indicate that the legislation may not

be effective; as presented in Section 5.7.1.2, the legislation may not be updated or corrected until it is tested by a court case.

From the outcomes of the discussions in the workshop related to mobile devices, the potential for cyber-based attacks through mobile devices is illustrated. Examples of mobile devices being used to circumvent perimeter controls and gain insider access could be used to compromise networks controlling critical infrastructure. The example of the mobile-based DDoS illustrates these devices could potentially be used in network warfare on the mobile infrastructure; in the document analysis presented in Section 5.5, experts are expecting a mobile worm equivalent to the PC-based Slammer worm (Hyppönen, 2010). There appears to be an under-estimation of smart-phone capabilities, and difficulty managing the security on these devices. The concerns raised regarding the effectiveness of RICA indicate potential legislative vulnerabilities. Unsecured VOIP communications and wireless communications to peripheral devices may provide opportunities of maliciously accessing information; and the possibility of pre-installed malware illustrates the potential for mobile devices to be utilised in a network warfare scenario.

6.3.3 Web 2.0 Related Discussion

This section presents the discussion related to Web 2.0 technologies. It was noted that employees are expecting the social connectivity in the workplace that is afforded by social media; this is consistent with the document analysis in Section 5.6. An example was provided where employees were provided with social media style connectivity internal to the organisation; however this was not utilised as the employees preferred external access to their existing friends. This tendency to be connected online socially raises concerns that corporate information may inadvertently be posted online, or employees could post something that harms the corporate image. The example presented in Section 6.3.1 of users posting configuration settings seeking advice may become more pronounced with users actively seeking social media connectivity and communications. Even if the universal resource locators (URLs) of social media websites are blocked, an example was provided of websites that are allowing users to access the websites by acting as a proxy. It was also noted that organisations check employees' activities through their social media profiles; this is also done during the recruiting process. This suggests a potentially persistent human threat where control mechanisms and policies are subverted intentionally in order to interact socially with persons external to the organisation, where sensitive information could be leaked. As the issue is related more to the user than any technical issues, awareness training may be the best solution to mitigate this behaviour.

It was noted that the nature of Web 2.0 sites is that content is often referenced from other sources; therefore it is difficult to determine the actual origin of the content. This content may be images, video, code, or applications; often Real Simple Syndication (RSS) is used. The problem is that this provides for rapid propagation of malicious content; and even if the website is reputable, it does not mean that the original source of the content is. Web 2.0 based malware was described in Section 5.6. It was also noted that application programming interfaces (APIs) on a social media site provided access to more information than what a user gave permission to access. These vulnerabilities may provide indirect methods of delivering malicious content or accessing information.

From the outcomes of the workshop discussions related to Web 2.0, it is apparent that these technologies can act as attack vectors. Their use as social communication mediums may also provide avenues for accidental information leaks. Examples of this are provided in Section 5.6.

6.3.4 Summary

The objective of the workshop was to solicit information regarding prevalent threats and vulnerabilities in South Africa from information security and risk perspectives. The discussion focussed on cyber-crime, and the protection of personally identifiable information. Social engineering, insiders, and criminal syndicates were identified as threats. Cases of corporate espionage and DoS attacks against specific websites do occur in South Africa; and a rise in targeted attacks has been noticed. Incorrect corporate attitudes towards information security were raised in addition to the lack of awareness and understanding. The prevalence of malware in South Africa was noted, and the concept of an African botnet was considered feasible. Proposed solutions again include the introduction of a CSIRT and legislation. At an organisational level, data classification, de-identifying the data, segregation of duties, and introducing security into the development cycle were suggested solutions. The use of biometrics as an additional security layer was also suggested. It was also proposed that a professional body be formed to regulate the industry and ensure quality of the academic offerings and professionals working in the field.

Examples provided in the discussion related to mobile devices indicates the possibility of these device being used to perform network warfare operations; infected devices may be used to conduct DDoS attacks against the mobile infrastructure, spread malware, or bypass perimeter controls of networks and provide insider access to potential attackers. MAC address filtering was suggested to mitigate unauthorised access to networks via mobile devices. Concerns were raised regarding the

effectiveness of RICA; malicious elements are able to circumvent the requirements of the act, indicating that RICA may only provide a false sense of security. There is concern regarding the information access of APIs in social media sites, and the difficulty in determining the origin of content; this may also be used to propagate malicious content. The use of social media by employees raises concerns over accidental information leaks. It is apparent that these technologies can act as attack vectors.

The perception of the respondents is that South Africa is behind on implementing the protection of systems and the information that reside on them. It is apparent that modern technologies have changed the threat and vulnerability landscape, and organisations have not fully come to terms with these changes. The human still appears to be a major vulnerability in information security. The aspects of the workshop that relate to the findings from the interviews (Section 6.2) and document analysis (Chapter 5) are consistent.

6.4 Survey

The objective of the survey was to determine the reliance on mobile communications by the informal sector. This focus combines with the interview focus on the government, military, and corporate sectors, providing coverage of a variety of sectors in South Africa. This corresponds to the research objective of determining the criticality of the mobile phone infrastructure; the reliance of the informal traders on mobile communications will be compared to their reliance on the other communication technologies. Only a pilot study was performed; this research is a project on its own and should be conducted as future research with the attention it deserves. It was expected that the informal sector would be overwhelmingly reliant on mobile phones; however this pilot indicates that this may not be the case. This dynamic deserves a more in-depth investigation that does not fall into the realm of this project. As described in Section 3.6, the pilot was conducted in central Durban, and the guide selected the participants. Nine prospective respondents were approached; one did not wish to participate, providing eight responses. Section 6.4.1 provides the demographics of participants, and Section 6.4.2 provides the results of the questions aimed at determining the reliance on mobile communications. Section 6.4.3 summarises this section.

6.4.1 Demographics

This section presents the demographics (age, race, and gender) and basic information regarding the business of the participants. These are summarised in tables, with brief descriptions. Categories in

the tables where there were no answer are left blank for clarity. Table 6.17 to Table 6.19 provide the demographics of the respondents.

Table 6.17: Age

Under 20	21-40	41-60	Over 60	Prefer not to answer
	5	1	2	

Table 6.18: Race

African	Indian	Coloured	White	Other
6	1		1	

Table 6.19: Gender

Male	Female	Prefer not to answer
5	3	

Some information regarding their business was solicited; this is presented in Table 6.20 to Table 6.22, and Table 6.23 presents the perceived monetary usage by the participant's on their mobile phones.

Table 6.20: Do you have employees?

No	No – it is a family business	Yes
4	1	3

Table 6.21: How many customers do you serve per day?

Less than 20	21-50	51-75	76-100	More than 100
3	2	1	1	1

Table 6.22: What do customers usually spend each visit?

Less than R10	R10-R50	R51-R75	R76-R100	More than R100
1	6	1		

Table 6.23: How much do you spend per day on your cell phone?				
Less than R10	R10-R20	R21-R50	R50-R100	More than R100
2	3	3		

In future research, the categories in Table 6.22 and Table 6.23 should be revised; where the categories below R50 are expanded, and have a single category of More than R50.

As the participants state they use less than R50 per day, the financial impact of a widespread services outage of the mobile service providers may not seem large; however, taking this over the entire informal sector the impact may become greater. The longer the outage lasts, the greater the impact. Should the informal sector be reliant on the mobile communications, then there will be a greater financial impact on the social well-being of the informal sector, their suppliers and their customers. Section 6.4.3 presents the gathered data from the pilot to indicate the possible reliance on mobile communications.

6.4.2 Access, Usage, and Reliance on Mobile Communications for Business

This section presents the perceptions of the pilot sample on their usage and reliance of mobile phones. Information was solicited on the access of the sample to various communications technologies (mobile voice, SMS, fixed-line, Internet and email) and the perceived usage and importance of each of these technologies.

Table 6.24 presents the access to communications technologies. All participants have access to their own mobile phone. Only one had access to their own fixed-line telephone, Internet, or email; seven had no access to these technologies at all, even from borrowed or public access points. This indicates prevalence in the penetration of mobile devices to the informal market.

Table 6.24: Access to Communications Technologies				
	I do not have access	I have my own	I borrow from someone else	I use a public or community one
How do you access a cell phone?		8		
How do you access a landline telephone?	7	1		
How do you access the Internet?	7	1		
How do you access emails?	7	1		

Table 6.25 presents how the participants perceived the majority of their of the communications technology use between private or business purposes. In some cases, two responses were provided; this was taken as equal use, and assigned 0.5. Six participants felt they used their mobile phone more for private reasons, one for business reasons, and one was equal between business and private use. The single responses for the other technologies indicated equal use for fixed-line telephone; and private reasons for both email and Internet use. These responses in indicate that a widespread outage of mobile communications may have a more profound social impact than a business impact for the informal sector.

Table 6.25: Perceived Use between Business and Private

	I do not have access to this	For my business	For private reasons
I mostly use cell phones for:		1.5	6.5
I mostly use landline telephones for:	7	0.5	0.5
I mostly use the Internet for:	7		1
I mostly use emails for:	7		1

Table 6.26 presents the view of the importance of the communication technologies for their informal business. The importance of mobile phones was mixed: three responses each for No difficulty and Very difficult, and one response each indicating it is not required or there will only be a small difficulty. No participants required email or Internet access for their business, and the respondent with access to the fixed-line telephone felt that it was important to the running of the business.

Table 6.26: Perceived Importance of Communication Technologies for Business

	It does not require this	No difficulty	Small difficulty	Very difficult
How difficult would it be to conduct your business without a cell phone?	1	3	1	3
How difficult would it be to conduct your business without a landline telephone?	7			1
How difficult would it be to conduct your business without Internet access?	8			
How difficult would it be to conduct your business without email access?	8			

The distribution of the responses according to the categories for mobile phones indicates that there may not be an overwhelming reliance on the mobile communications. However, due to the higher penetration of mobile phones, there will be more reliance on the mobile communications than fixed-line telephones.

The participants were asked to rate their usage of various communication technologies. The responses are summarised in Table 6.27. One respondent each listed never and less than once a week for using mobile phones for making business calls, two listed everyday and four listed more than once a day. For private use, mobile phones were divided one response each for less than once a week and a few times a week, and six for more than once a day. The responses rating the use of SMS services were the same for both business and private reasons: two listed never and three each for a few times a week and more than once a day. One participant did not wish to respond to the their use of mobile money functions; three listed that they did not have access, one each for never and less than once a week, and two listed that they used mobile money a few times a week. The response with fixed-line access indicated it is used a few times a week for business, and every day for private use. The response with Internet and email access indicated they use email a few times a week for private reasons, but never for business; the Internet access was listed as never being used.

The use of communications technologies in general appears to have a slightly higher frequency for private use than business use. This indicates that an outage may have a more immediate social impact than a business impact for the informal traders. The longer an outage lasts, the greater the impact will be on the business. The impact of a possible failure or outage of the communications technologies was rated by the participants; the responses are presented in Table 6.28. The responses related to the mobile phones were spread evenly amongst the four categories (two each); this does not correspond to Table 6.26, where the difficulty was split three each for no difficulty and very difficult and one each for small difficulty and not used for business. This will be discussed more below. One response regarding the impact of a fixed-line outage indicates badly affected and seven listed that they do not use it; this corresponds with the responses for fixed-line telephones in Table 6.26. One response regarding the email and Internet facilities indicated that there will be no affect on their business should there be a service outage; seven indicated that the technology is not used for their business. In Table 6.26 all responses indicated their business did not require these facilities. Therefore these responses do not correspond perfectly; however the meaning is not altered in that as they are not required, there will be no affect.

Table 6.27: Usage of Communications Technologies

	I do not have access	Never	Less than once a week	A few times a week	Everyday	More than once a day
How often do you use a cell phone to make calls for your business?		1	1		2	4
How often do you use a cell phone to make calls for private reasons?			1	1		6
How often do you use the SMS function for business purposes?		2		3		3
How often do you use the SMS function for private reasons?		2		3		3
How often do you use a cell phone to use mobile money (M-PESA etc)?	3	1	1	2		
How often do you use a landline telephone for your business?	7			1		
How often do you use a landline telephone for private reasons?	7				1	
How often do you use email for your business?	7	1				
How often do you use email for private reasons?	7			1		
How often do you use the Internet for your business?	7	1				
How often do you using the Internet for private reasons?	7	1				

Table 6.28: Perceived Impact of Failure of the Communication Technology

	I do not use this for my business	No affect	Small affect	Badly affected
How badly will your business be affected if the cell phones stopped working?	2	2	2	2
How badly will your business be affected if the landline telephones stopped working?	7			1
How badly will your business be affected if the Internet stopped working?	7	1		
How badly will your business be affected if the emails stopped working?	7	1		

Participants were asked to elaborate on what the purpose of making mobile phone calls for the business was. There reply was they check the market prices, or place orders. They were then asked what they would do if they could not make the phone call; their reply was they would walk to the market. The reason for the discrepancies between Table 6.26 and Table 6.28 is that it may be difficult to run the business without mobile phones; however, if there is a major service outage the respondents will make other arrangements and the business will not be badly affected. It was expected that the informal sector would be overwhelmingly reliant on mobile communications. From the responses it is clear that whilst there is more reliance on mobile communications than other technologies due to penetration, there does not appear to be a perception of reliance by the respondents themselves. To accurately determine the role of mobile communications and the reliance on these technologies in the informal sector, an in-depth study that deserves the attention of a full research project is required.

6.4.3 Summary

A pilot survey was conducted, where information was solicited from informal traders; the objective of the full survey was to ascertain the level of reliance on mobile phone communications. The results of the pilot study indicate that the informal traders appear to use mobile phones more for private communications than for business purposes. It was expected that this sector would be overwhelmingly dependent on mobile communications; however the participant's responses were mixed. This indicates that there is some reliance; however, their businesses are not solely dependent on mobile communications. The high penetration of mobile phones compared to fixed-line telephones can be seen in that all respondents had access to mobile phones. This indicates that the mobile phone infrastructure has penetrated all levels of business; whereas fixed-line communications have not. Therefore it can be said that the mobile infrastructure is as critical as the fixed-line infrastructure, if not more so.

6.5 Chapter Summary

This section summarises the key findings of this chapter. Three primary data gathering techniques were employed: expert interviews, a research workshop, and a pilot survey. The objectives were to solicit information that could be used in assessing the criticality of the mobile phone infrastructure, and assessing the prevalent threats and vulnerabilities in South Africa.

From the interviews, the perception is that the CIIP in South Africa needs to improve. In both the interviews and workshop issues regarding the governance of IT were raised, and the lack of a functional CSIRT in South Africa was identified as a problem, as there is no centralised source of information to give a clearer view of the big picture regarding cyber-crime and cyber-based attacks in South Africa. The introduction of new legislation and standards in South Africa is expected to improve the governance by forcing organisation into compliance and taking responsibility. However, as raised in the interviews, the focus is on increasing the availability of Internet connectivity for business and economic reasons, and security is still a side-issue. The concerns that were raised in the interviews and the workshop show consistency with the document analysis in Chapter 5.

Cyber-crime came across strongly in both the interviews and workshop; both the financial impact and issues of privacy and the protection of personally identifiable information were raised. This is not surprising given the prevalence of cyber-crime attacks on personally identifiable information. Fraud was raised in both the interviews and workshop; the workshop indicated that most fraud was traced back to residential addressed of persons associated with employees of the victim organisation. Examples were provided in the workshop of insider threats and targeted attacks by crime syndicates; this is consistent with examples in the document analysis presented in Chapter 5. The susceptibility to the threats related to cyber-crime indicates that there will be susceptibility to similar attacks originating from nation-states, who potentially have more resources than cyber-criminals. Such incidents are discussed in Chapter 5. There may therefore be a high susceptibility to cyber-based attacks against South Africa.

In both the interviews and workshop it was raised that there is a lack of awareness and understanding, and improper attitudes toward information and IT security. The introduction of new legislation is expected to improve the situation regarding organisational compliance. User awareness is still an issue. In the workshop it was indicated that social engineering has very high success rates. Many users are expecting access to social networking within the organisation; concerns are therefore against leaks and damage to corporate image due to careless posting; this is consistent with the document analysis in Chapter 5. An additional problem with Web 2.0 technologies is that the original source of the content is difficult to determine due to the cross-referencing of websites; this provides for rapid propagation of malicious content.

From the workshop it was indicated that cases of cyber-based corporate espionage do occur in South Africa. An interview response indicated that DoS attacks are a major threat, but South Africa

has not been targeted as of yet. In the workshop, an example was given of small-scale DoS attacks against specific websites in South Africa. The prevalence of malware in South Africa was raised in the workshop; it was indicated that it appears that South Africa is being used a launching point for attacks. This is consistent with the malware infection rates and the concept of an African Botnet as presented in Chapter 5. This indicates there is susceptibility to malware infection and to DoS attacks, as using infected computers in Africa to launch attacks will impact on the international bandwidth of the hosting nations as well as the target. A concern is that the growth of access without the corresponding security and awareness will magnify the problem. An example was given where biometrics are being used in conjunction with passwords; this may be useful in preventing malicious access to critical infrastructure systems.

The interviews indicate that the mobile infrastructure is part of the critical information infrastructure. Reasons for this are given as reliance of other sectors on mobile communications, and the fact that the mobile infrastructure is included as part of the information and communications sector, which is considered as critical. The heavy reliance of society on mobile communications was raised in the interviews; in the workshop an example was provided of a mobile DDoS attack on the base stations, resulting in local loss of services. Concerns were also raised over the effectiveness of RICA in the workshop; examples were provided of how the process is being circumvented. This could indicate potential legislative weakness, where it is possible to continue malicious use of the mobile communications.

The survey considered the informal sector, and the interviews consider small and large businesses, government, military, intelligence and security services, and criminal and terrorist elements. From the responses, it is apparent that mobile communications has some importance for all sectors. It was indicated that the military, governments, intelligence and security services should implement additional security measures, and should have other means of communication. It was noted in the interviews that mobile communications may be the only form of communications available to small businesses; the results from the pilot survey indicates that this is probably the case for the informal sector. However, the participants did not perceive their businesses as being completely reliant on mobile communications; it appears to be used more for private reasons, and the results of the impact of a potential outage were spread evenly across the categories. The results indicate that there may not be an immediate impact on the informal sector should there be an outage of the mobile communications. The penetration of mobile phones into all levels of society was hinted at as all participants had access to their own mobile phones.

The potential use of mobile devices in attacks was raised in both the interviews and the workshop; a particular concern was the fact that the devices can circumvent the network perimeter controls. Examples were provided in the workshop of this being conducted during a penetration test. Confidentiality is also a concern regarding mobile devices; the ease of intercepting communications was mentioned in both the interviews and workshop. An example of intercepting wireless communications during a penetration test was provided during the workshop; the susceptibility of using a mobile phone's VOIP capability over open networks to interception was also raised. This is consistent with the document analysis, where incidents of unauthorised access to mobile communications were presented.

Solutions suggested in both the interviews and workshop is the introduction of CSIRTs and continued introduction of cyber-relevant legislation. Data classification and segregation of duties, anonymising or de-identifying data, MAC address filtering in the organisation to aid in preventing unauthorised devices accessing the network, and the introduction of security into the development cycle were also identified in the workshop; international collaboration and internal capacity building was identified in the interviews. Biometrics in addition to passwords may aid in mitigating unauthorised access to critical systems. Due to the large issue with awareness, measures should be taken to improve awareness of users and organisations regarding cyber-threats. Developing new technologies and techniques to counter the security issues surrounding mobiles was also suggested.

It should be noted that the data gathered in the three methods are not sufficient on their own to prove any theory; however they support the theories and trends that were discussed in Chapter 5, and give indications of the specific scenario in South Africa. The outputs from this chapter and Chapter 5 will be used in conjunction with the mathematical and simulation results in Chapter 7 as input for the vulnerability assessment, presented in Chapter 8.

Chapter 7. Simulations and Calculations

7.1 Introduction

This chapter presents the simulations and calculations to determine critical points in the mobile infrastructure, and the feasibility of attacking these nodes. Section 7.2 conducts a graph theory analysis of the mobile infrastructure; this identifies possible singularities or central nodes that may be vulnerable to attack. Section 7.3 calculates the capacity of the wireless channels of mobile networks to assess the feasibility of performing a DoS attack on channels. Section 7.4 presents simulations of mobile worms, and assesses the capability of the physical infrastructure hardware to carry these loads. Section 7.5 calculates the range at which wireless communications can be detected and jammed; this illustrates the feasibility of electronic warfare tactics against the mobile infrastructure. Section 7.6 simulates the correlation accuracy required for eavesdropping or jamming 3G signals; this illustrates the complexity of electronic warfare operations against 3G communications.

7.2 Graph Theory Analysis

As described in Section 2.7.1.10, graph theory analysis can be done on networks and infrastructures to determine critical nodes; if any singularities or centralised systems are discovered, these may be considered as vulnerabilities. These systems may serve as choke points, or failure of the device may result in failure of the overall infrastructure. This section presents an analysis of the mobile infrastructure to identify possible singularities, centralised systems, and critical nodes in the mobile infrastructure. For this analysis, a simplified mobile infrastructure will be used; the information flow under consideration is the requests for connection from the towers to the core infrastructure, therefore devices that provide additional mobile services are ignored; these are usually associated with the mobile switching centres (MSC), base station controllers (BSC), or home location register (HLR). Therefore the SMS switching enter (SMSC) can be considered as part of the MSC, the authentication centre can be considered as part of the HLR, and the GPRS gateways can be considered as part of the BSCs. From Traynor *et al*. (2009), there can be up to 200 towers (BTS) per MSC, and up to ten MSCs per HLR; for the purposes of this analysis, it will be assumed that each BSC can operate twenty BTSs.

Figure 7.1 shows the graph, where the dashed lines indicate devices not shown (only BSC 1 and BSC 10 are shown for each MSC, likewise only MSC 1 and MSC 10 are shown). From this it can be determined that the HLR node has ten edges (one for each MSC); the MSC nodes have twenty edges (ten to the BSCs, nine to the other MSCs, and one to the HLR). The BSC nodes have 21 edges, twenty to the BTS, and one to the MSC; the BTS nodes have one edge to the BSC.

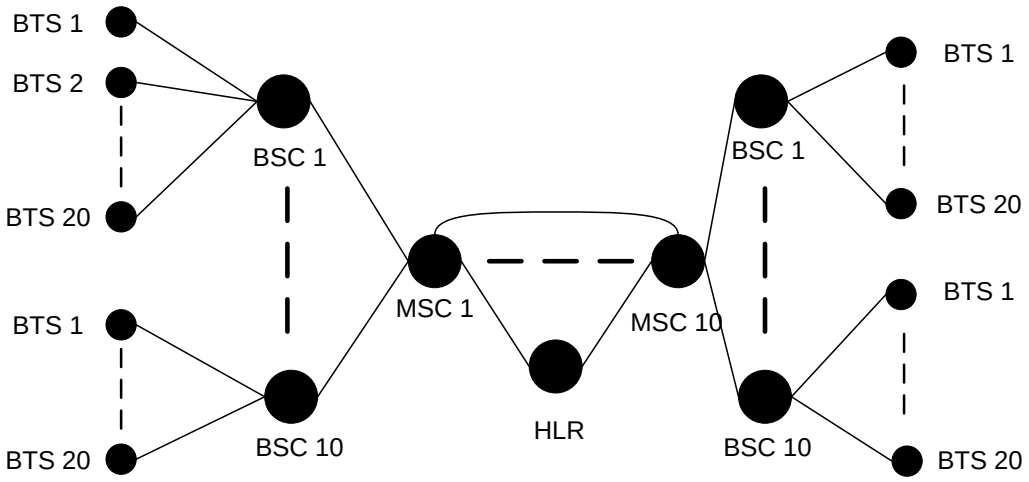


Figure 7.1: Graph of a Simplified Mobile Infrastructure

Table 7.1 shows the numbers of devices and the degree of the nodes for the graph shown in Figure 7.1. For the case of three HLRs, the HLR nodes have a higher degree to allow for connection to each other. As discussed in Section 2.7.1.10, the graph scale type is determined by the relationship between the frequencies and the degree of the nodes.

Table 7.1: Frequencies and Degrees of Nodes for a Simplified Mobile Infrastructure

Node (Hardware device)	Frequency (Number of devices)	Degree of Node (Number of connections)
For one HLR		
BTS	2000	1
BCS	100	21
MSC	10	20
HLR	1	10
For three HLRs		
BTS	6000	1
BCS	300	21
MSC	30	20
HLR	3	12

By inspection of Table 7.1, it can be seen that the node distribution is not governed by a power law, which indicates that the mobile infrastructure is not a scale-free network (Lewis, 2004). From this graph, it can be seen that there are critical nodes based on geographical location: each BSC is critical to the connectivity of a small geographic area, and the MSCs are critical to the connectivity of larger geographic areas. Due to the nature of the HLR, upon which the infrastructure relies for authentication and billing information, this is a critical node as its malfunction will render the infrastructure inoperable.

Due to the clustering of nodes in geographical locations, it is theoretically possible to target specific nodes deny services in these areas; however certain nodes may have a larger load capacity than others. For example, the MSC will be able to carry larger loads than a localised BSC. There is also the possibility that the channels themselves become overloaded due to a DoS attack; Enck *et al.* (2005) investigate this possibility by assessing the capacity of the stand-alone dedicated control channel (SDCCH) to carry SMSs. This research is expanded by Traynor *et al*. (2009) to investigate a potential DoS attack on the HLR. Section 7.3 applies the study of Enck *et al*. to the South African situation. Fleizach *et al*. (2007) investigate the propagation of mobile malware; this is expanded upon in Section 7.4, where the network loading and time to failure due to aggressive mobile malware is simulated.

From the interviews presented in Section 6.2, the HLR handles billing. As contract fees can also be paid in-store, this indicates that there is some form of transfer of subscriber billing information from the stores to the mobile infrastructure. Therefore there is the potential that the billing systems may be attacked through insecure systems in stores. Corruption of the billing database may result in affected subscribers having mobile services denied should all the billing information be set to indicate there are outstanding fees or no airtime. It will also be possible to breach the confidentiality of subscriber account and residential information through the store interface.

The graph theory analysis of the mobile infrastructure indicates that there is clustering in geographical areas, and the network is not scale-free. Therefore there are critical nodes that govern specific geographical areas; BSC control localised areas, MSCs control larger areas, and the HLR controls much larger geographical areas. By targeting these nodes, it may be possible to deny services to the relevant geographical area. It may also be possible to perform a DoS attack on the channels themselves. The following sections analyse the feasibility of attacking the nodes and channels.

7.3 Calculations to Determine Message Capacity of Mobile Network Channels

As with computer networks, the mobile infrastructure will have a maximum operating capacity; should the infrastructure be bombarded with large amounts of illegitimate traffic, the mobile services will be denied. This is essentially a network warfare attack on the mobile infrastructure. Enck *et al*. (2005) calculated the number of messages required to saturate the stand-alone dedicated control channels (SDCCHs) of a mobile network; as the SDCCH channels are used for authentication and delivery of SMSs, both voice and message services will be denied due to a saturation of these channels. In their paper, the cities of Washington D.C. and Manhattan were used as an example for the calculations; this section presents similar calculations are performed for four metropolitan areas of South Africa. Enck *et al*. (2005) calculated that the size of a sector was 0.5 mi^2 to 0.75 mi^2, which equates to approximately 1.3 km^2 to 2 km^2. Table 7.2 shows the relevant statistics for four metropolitan areas in South Africa, with the calculated number of sectors based on the sector sizes above.

Table 7.2: South African Metropolitan Statistics and Calculated Number of Mobile Phone Sectors

Metropolitan Area	Population*	Area*	Population Density*	No. of Sectors	
				1.3 km^2	2 km^2
eThekwini (Durban)	3 161 844	2 291km²	1 379	1762	1146
Cape Town	2 969 458	2 460km²	1 207	1892	1230
Johannesburg	3 295 088	1 644km^2	2 003	1265	822
Tshwane (Pretoria)	2 040 517	2 174km^2	938	1672	1087

*Source: South African Cities Network (2011a)

Enck *et al*. (2005) suggest that there are typically two SDCCHs per mobile carrier for a GSM network; however, this may increase for areas of dense population. The paper also indicated that each SDCCH could carry approximately 900 messages per hour. The following equation then may be used to calculate the message capacity limit of the mobile networks in a metropolitan area (adapted from Enck *et al*. (2005)):

$$C = (\text{No. of sectors}) \times (\text{SDCCHs per sector}) \times (\text{messages per second per SDCCH}) \quad \textbf{7.1}$$

where C is the overall capacity in messages per second. Table 7.3 shows the capacity for four South African metropolitan areas, for the number of sectors (determined in Table 7.2), and various numbers of SDCCHs per sector. The number of SDCCHs per sector was determined assuming three

and five carriers, and taking the case of two and three SDCCHs per carrier; this gives six, nine, ten, and fifteen SDCCHs per sector.

Table 7.3: Message Capacity (messages/second) of Mobile Networks for Metropolitan Areas

Metropolitan Area	No of Sectors (Sector Size (km^2))	SDCCHs per Sector			
		6	9	10	15
eThekwini (Durban)	1762 (1.3)	2643	3964.5	4405	6607.5
	1146 (2)	1719	2578.5	2865	4297.5
Cape Town	1892 (1.3)	2838	4257	4730	7095
	1230 (2)	1845	2767.5	3075	4612.5
Johannesburg	1265 (1.3)	1897.5	2846.3	3162.5	4743.8
	822 (2)	1233	1849.5	2055	3082.5
Tshwane (Pretoria)	1672 (1.3)	2508	3762	4180	6270
	1087 (2)	1630.5	2445.8	2717.5	4076.3

From the results shown in Table 7.3, the maximum quantity of messages the SDCCHs would be able to process is 7095 messages per second (this is for fifteen SDCCHs and 1892 sectors in Cape Town). After that figure has been reached, both voice and messages services will be severely degraded, if not denied, due to the SDCCHs being overloaded. If the infrastructure is operating close to its capacity limits, fewer messages may be required in order to disrupt services. An example is the backlog of BlackBerry messages after the initial outage in 2011 resulted in continued disruptions (Press Association, 2011). Mobile service disruptions in South Africa were also attributed to high operating loads (Ajam & Bailey, 2009).

A possible method for attacking a mobile phone infrastructure by saturating services with illegitimate SMSs is to compromise web-based SMS services and employing them to transmit the SMS (Enck, Traynor, McDaniel, & La Porta, 2005). For this to occur the Internet would need to carry the equivalent data that would be sent in the SMSs; Table 7.4 shows the required Internet capacity for the message rates in Table 7.3 assuming each SMS is 1500 bytes as described in Enck *et al*. (2005).

From the Internet capacity required shown in Table 7.4, the worst case scenario for attacker is a required capacity of 81.2 Mbps. As the three-digit prefix of South African mobile phone numbers is arranged according to network provider rather than geographical area, it may be difficult to target one area; it may be necessary to attempt to deny services nation-wide. Taking the maximum

Table 7.4: Internet Capacity Required (Mbps)					
Metropolitan Area	**No of Sectors (Sector Size (km^2))**	**SDCCH**			
		6	**9**	**10**	**15**
eThekwini (Durban)	1762 (1.3)	30.2	45.4	50.4	75.6
	1146 (2)	19.7	29.5	32.8	49.2
Cape Town	1892 (1.3)	32.5	48.7	54.1	81.2
	1230 (2)	21.1	31.7	35.2	52.8
Johannesburg	1265 (1.3)	21.7	32.6	36.2	54.3
	822 (2)	14.1	21.2	23.5	35.3
Tshwane (Pretoria)	1672 (1.3)	28.7	43.1	47.8	71.8
	1087 (2)	18.7	28	31.1	46.6

capacity required for each of the four metropolitan areas, a total of 282.9 Mbps is required to saturate the four largest metropolitan areas of South Africa. Considering the DoS attack against Myanmar (Burma) reached 14 Gbps (Labovitz, 2010), the Internet traffic required to conduct the attack is feasible. However, there may be a limitation regarding the capacity of the web-based SMS services to carry such a load; multiple providers of such services may need to be compromised in order to achieve the desired result. Given that the aggressor is attempting such an attack in the first place, compromising multiple web-based SMS providers should be feasible.

7.4 Simulations of Mobile Network Traffic Load due to Mobile Malware

This section provides simulation results for the message traffic load on a mobile phone infrastructure due to the spreading of a mobile-based worm. The simulations will hold for similar situations; but as not all infection characteristics of mobile worms are the same, it will not hold for all. The section is intended to give an indication of the potential severity of mobile worms in a DoS-style network warfare attack on the mobile infrastructure. The section also intends to illustrate the importance of computer simulations in analysing potential attacks and the effect on infrastructures.

Simulations conducted by Fleizach *et al*. (2007) focussed on the topology of the address book of mobile devices and the capacity of the links between nodes on the malware propagation for the cases of voice over IP and MMS. The simulations presented in this section intend to illustrate the impact on the hardware nodes, and the time taken to overload those nodes.

Section 7.4.1 provides simulation based on the Beselo worm that targeted Nokia's Symbian OS; and Section 7.4.2 provides a simulation for a hypothetical scenario where a mobile worm is

intentionally used to infect devices in attempt to perform a DoS attack. The purpose of these simulations is to provide an estimate on the load that the hardware of the mobile infrastructure will bear from such an attack. Section 7.4.3 provides a summary and some additional analysis of the simulation results. As these are simulations, they comprise of multiple equations and decisions; the flow diagrams for the simulations are presented in Appendix D.

7.4.1 Simulations Based on the Beselo Worm for Symbian Platforms

The simulations in this section are based upon the Beselo worm that infects the Symbian OS. This worm propagates by sending MMSs to the entire contact list of an infected device every two minutes (Cisco, 2009). The simulations are conducted using the Matlab software.

An artificial limit on the device population is set, so there are a maximum number of devices that can be infected; this is done as in the real world there is a finite number of devices. One minute is allowed for the transmission of the message and the installation of the worm on the next device, prior to that device beginning to transmit. Therefore there will be three minutes between the time a message is sent to a device and the time it begins transmitting (assuming it is infected). It is assumed that there are on average 100 contacts in a device's contact list. The Monte-Carlo simulation randomises the probability of infection; initially, it is assumed that 1% of the recipients will be infected, thereafter the probability is decreased according to the number of devices in the maximum population that have not been infected, and this is randomised using Matlab's built-in random number generator. Each time point is an average of 1000 iterations of the simulation; as the random number generator returns a four-digit number between zero and one with three decimal places (an example is 0.495), the number of iterations allows each number between zero and one an equal probability of being randomly generated. For the purposes of the simulation, it will be assumed that there is only one initial infection.

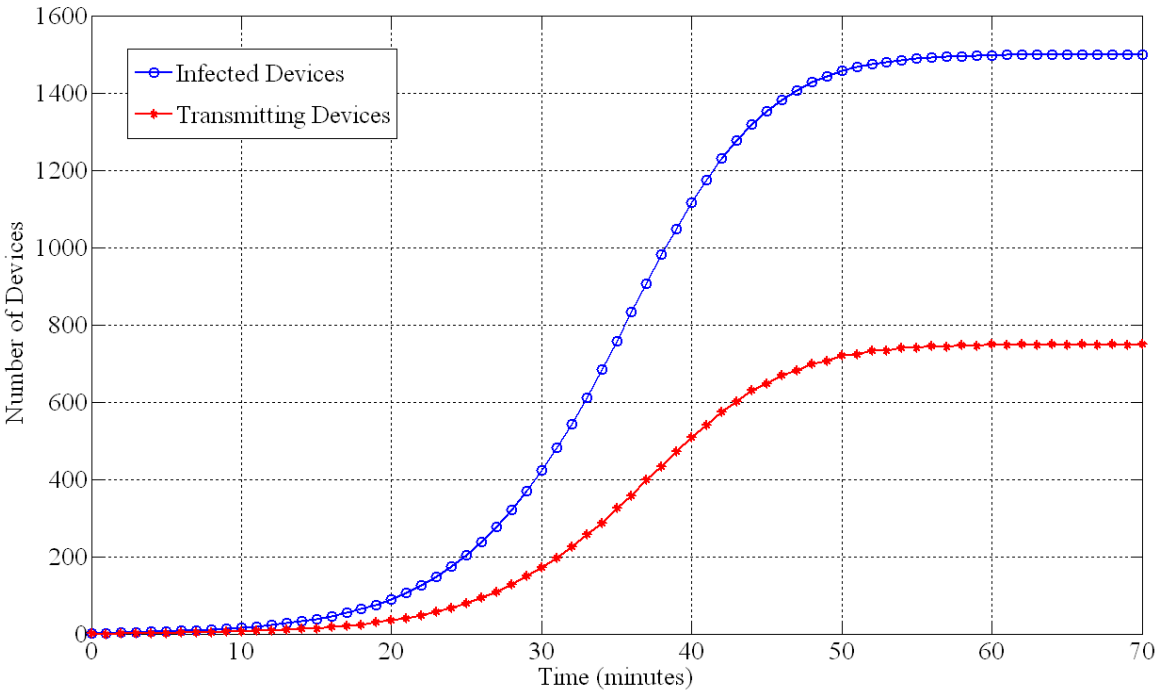


Figure 7.2: Number of Infected and Transmitting Devices with Time for a Population of 1500 Devices

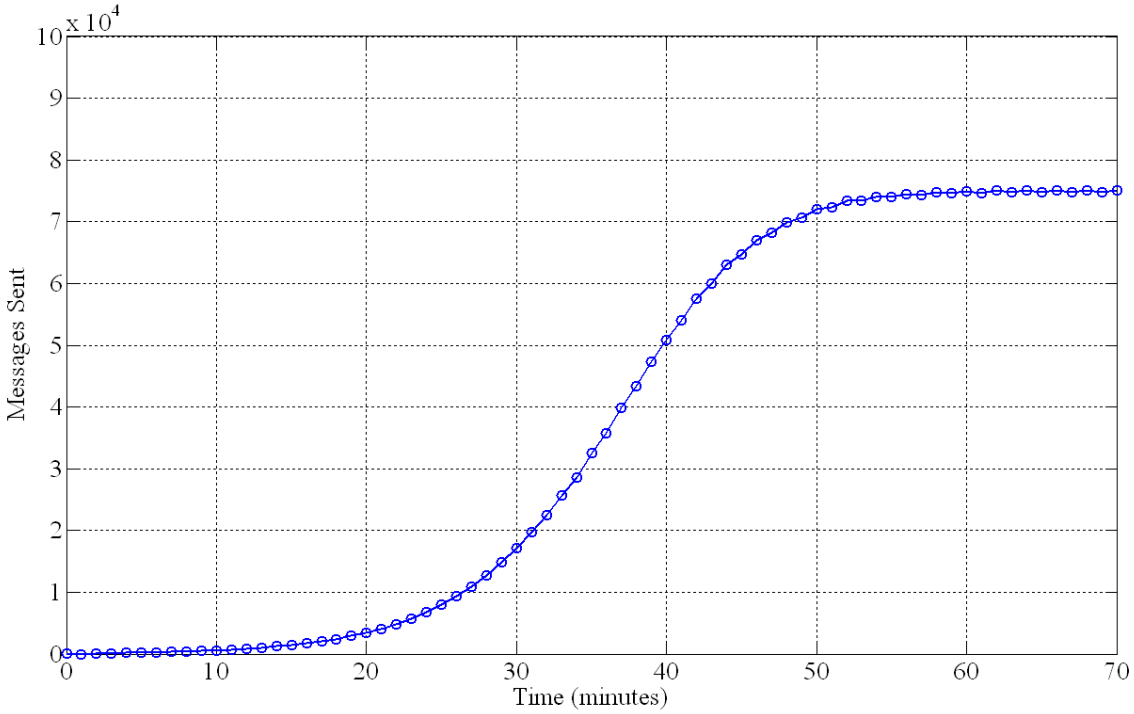


Figure 7.3: Number of Messages Sent with Time due to Infected Devices with a Maximum Population of 1500

Figure 7.2 shows the growth in the number of infected devices and the devices transmitting infected MMSs to propagate as time progresses for a maximum population of 1500 devices. The lag between the time the devices are infected and when they begin to transmit can be seen. As each device only transmits every two minutes, and given the one-minute delay for new devices to become infected, approximately half of the population transmits each minute; this reduces the maximum possible effect of the worm. Figure 7.3 shows the graph of the number of message sent. Assuming that each device has 100 contacts listed in the address book, there will be approximately 75000 messages being sent every minute. The S-shaped curve is a result of the initially slow spreading of the infections due to a small number of transmitting devices; this gathers momentum, and then tapers out as the number of clean devices decreases, reducing the likelihood of new infections.

Figure 7.4 compares the infection and transmission characteristics of the worm spreading for various population sizes. The difference in time for the maximum infection to be reached is slight; doubling the population size does not double the time taking to reach maximum infection. This characteristic is due to the non-linear nature of the infection rate; as more devices are infected, the more transmission are made and the higher the chance of subsequent infections. The delay between the device infection and transmission is again visible. For a population of 4500, the delay between 2000 devices being infected and 2000 devices transmitting is slightly in excess of ten minutes; however, when considering incident response on a national scale, this delay is negligible. Figure 7.5 compares the number of messages sent; these follow the same trends as in Figure 7.4. What is significant is that for a population of 1500 devices that are infected, that within fifty minutes the infected phones will be sending 75000 MMSs; for a population of 4500, the number of MMSs exceeds 200000 within an hour. This indicates that a virus targeted at a popular mobile device will have a significantly greater impact in a relatively small amount of additional time. This additional load on the infrastructure may hamper legitimate traffic. In addition, it will be frustrating for the individuals receiving an MMS every two minutes, and expensive for those whose phones are infected and sending the MMS. The continuous transmission or reception of messages may also drain the battery of the device (Enck, Traynor, McDaniel, & La Porta, 2005).

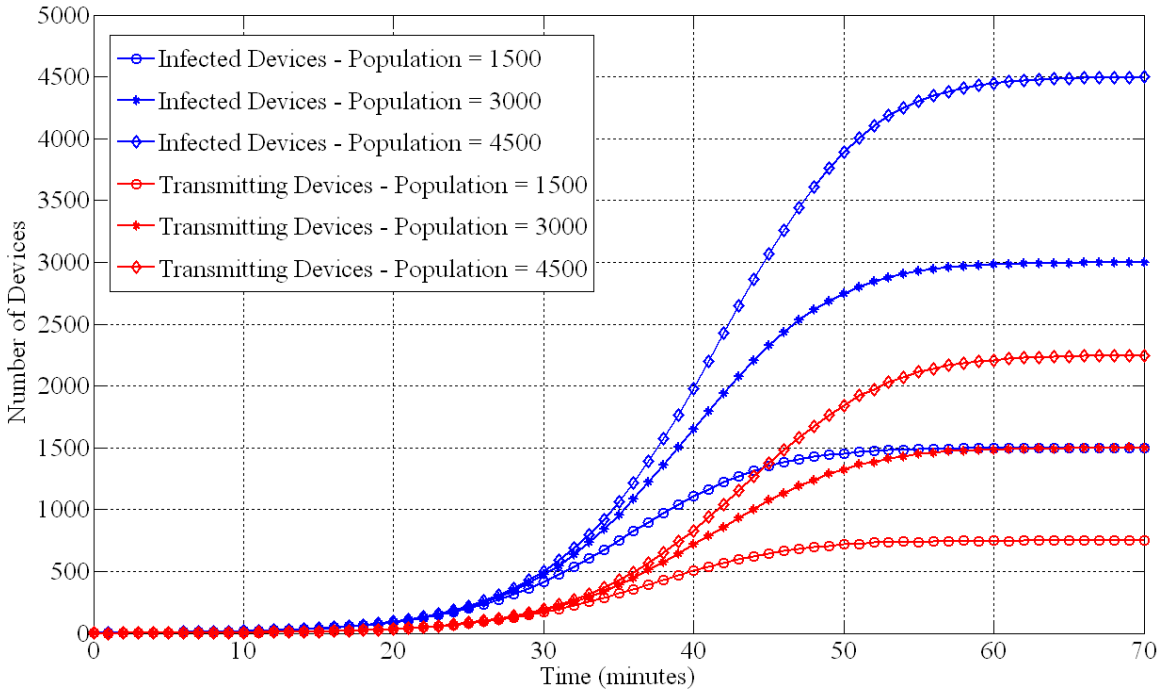


Figure 7.4: Comparison of Infected and Transmitting Devices for Various Populations

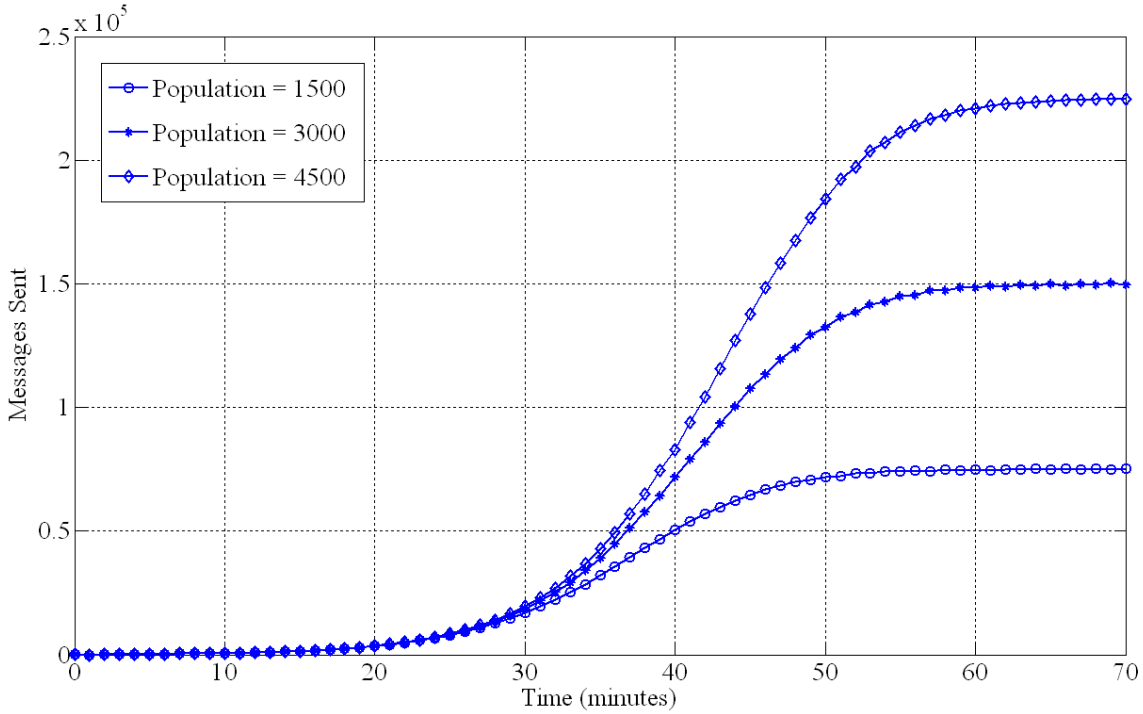


Figure 7.5: Comparison of the Number of Messages Sent per Minute for Various Populations

7.4.2 Simulations for a Hypothetical Worm and the Impact on the Cellular Phone Infrastructure

This section simulates a hypothetical worm with multiple propagation vectors: Bluetooth, SMS, and MMS. The Beselo worm described in Section 7.4.1 can also propagate via Bluetooth (Cisco, 2009), therefore the ability of mobile worms to have multiple propagation vectors is feasible. For this example it will be assumed the intention is to create a DoS attack on the cellular infrastructure. For the purposes of the simulations, it will be assumed that infected devices will send messages every minute to all contacts in the address book of the device. Device and channel limitations will be ignored as the purpose of these simulations is to investigate the theoretical loading such a virus will place on the hardware of the mobile network infrastructure. To initiate the spread of infections, an infected device can be intentionally been left in an area with large quantities of human traffic, such as a shopping mall, to transmit and infect nearby devices via Bluetooth. As with the simulation in Section 7.4.1, the results are averaged over 1000 iterations, and the address book is set to 100 contacts.

Figure 7.6 shows the number of infected and transmitting devices over time for various maximum populations. Figure 7.7 shows the number of messages sent per minute, and Figure 7.8 shows the number of infected and transmitting devices for various initial infections. All figures are for a maximum population of 3000, one initial infection, and no additional load unless otherwise stated. For these simulations, infrastructure hardware limitations are not considered.

The shape of the graphs showing the increase in infected devices is similar to those in Section 7.4.1, except that as there is a transmission every minute, the infection can spread faster resulting in a steeper curve. In Figure 7.6, the time delay between a specific number of infected devices and the same number transmitting is reduced and the number of transmitting devices can approximate the maximum number of infected phones, compared to the Beselo worm in Section 7.4.1. As shown in Figure 7.7, the number of messages transmitted per minute by the infected devices will be maximised, which will increase the load on the infrastructure hardware. From Figure 7.8, it is apparent that increasing the number of initial infections does accelerate the spread of the infection, however only by a few minutes for this case.

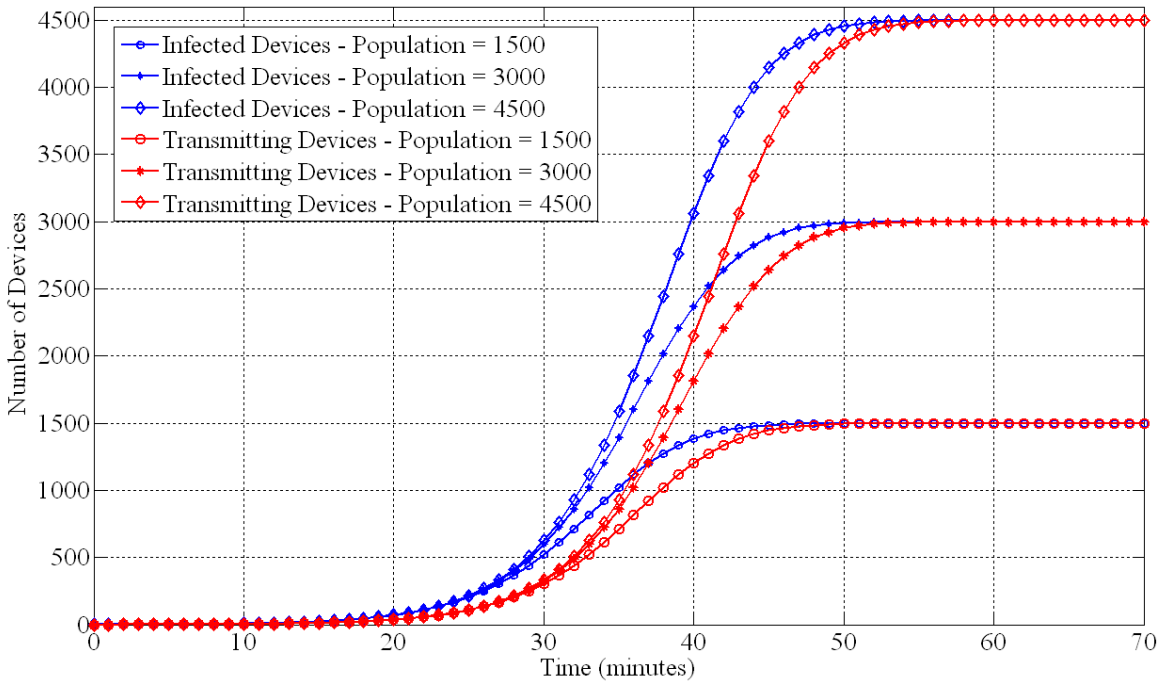


Figure 7.6: Infected and Transmitting Devices for Various Populations with no Additional Load or Hardware Limitations and one Initial Infection

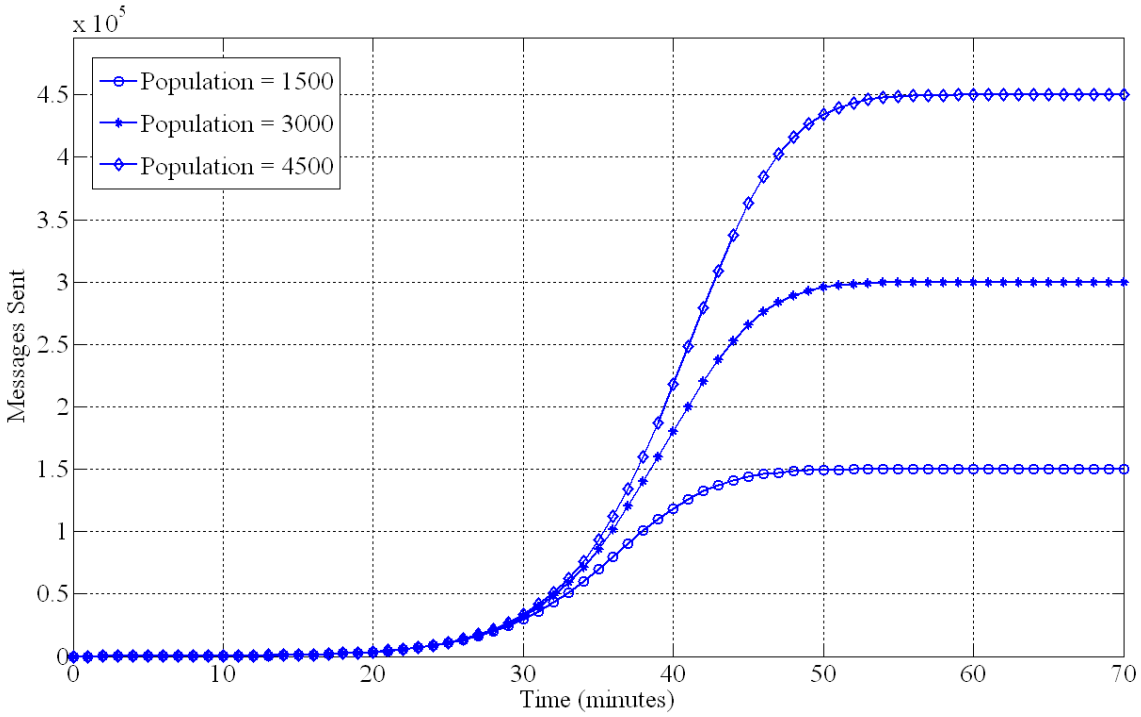


Figure 7.7: Messages Sent for Various Populations with no Additional Load or Hardware Limitations and one Initial Infection

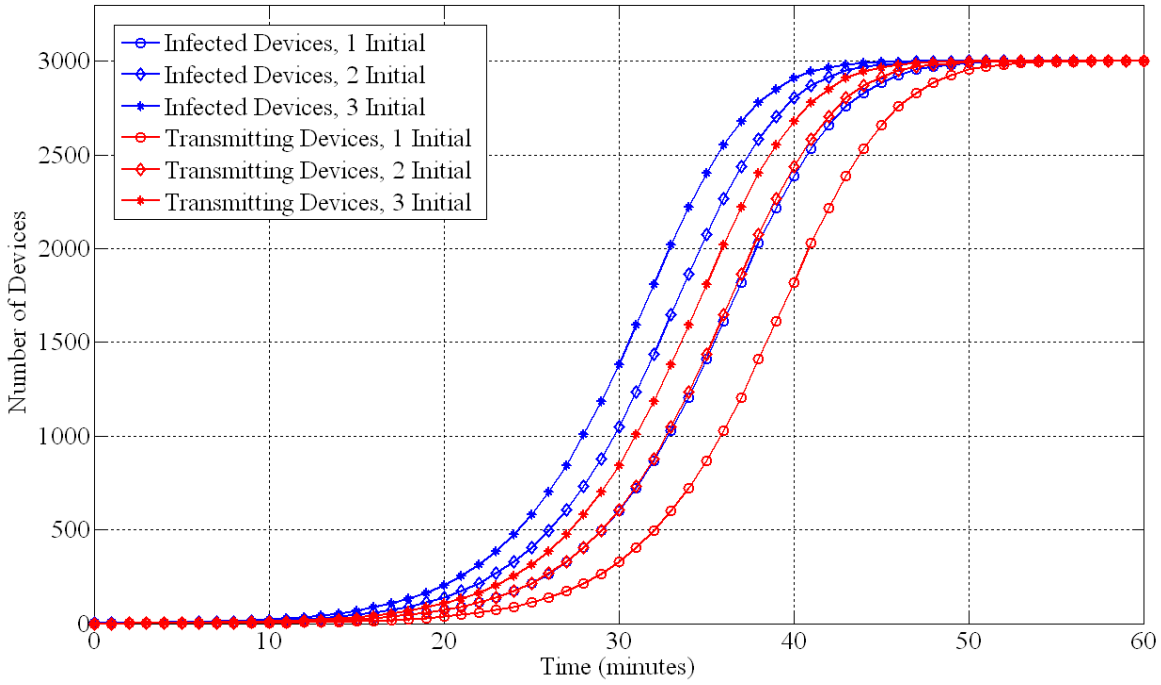


Figure 7.8: Infected and Transmitting Devices for Various Numbers of Initial Infections with no Additional Load or Hardware Limitations for a Maximum Population of 3000 and one Initial Infection

Figure 7.9 to Figure 7.11 repeat the above simulations, but account for hardware limitation and additional loading from legitimate traffic. According to Enck *et al.* (2005), a short message switching centre (SMSC) from the year 2000 could process 2500 SMS messages per second. This figure will be used as a more recent capacity of the switching centres was not found; the simulations can be repeated in future when this data is available and compared to the results presented here. These simulations will also allow for additional loading on the infrastructure; this can be assumed to be continuous legitimate traffic. Once the simulation has reached a point where the hardware is saturated, the probability of new infections is reduced by a factor determined by dividing the number of messages handled by the total number of messages this (this is the probability that a message will be successfully sent).

Figure 7.9 shows the increase in infected and transmitting devices for various additional loads. Figure 7.10 shows the number of messages sent, the number that can be handled by the SMSC, and the number of messages rejected or failed due to network saturation for various additional loads. Figure 7.11 shows the impact of the number of initial infections. Table 7.5 gives times taken to overload the infrastructure hardware for various maximum populations, loads, and initial infections.

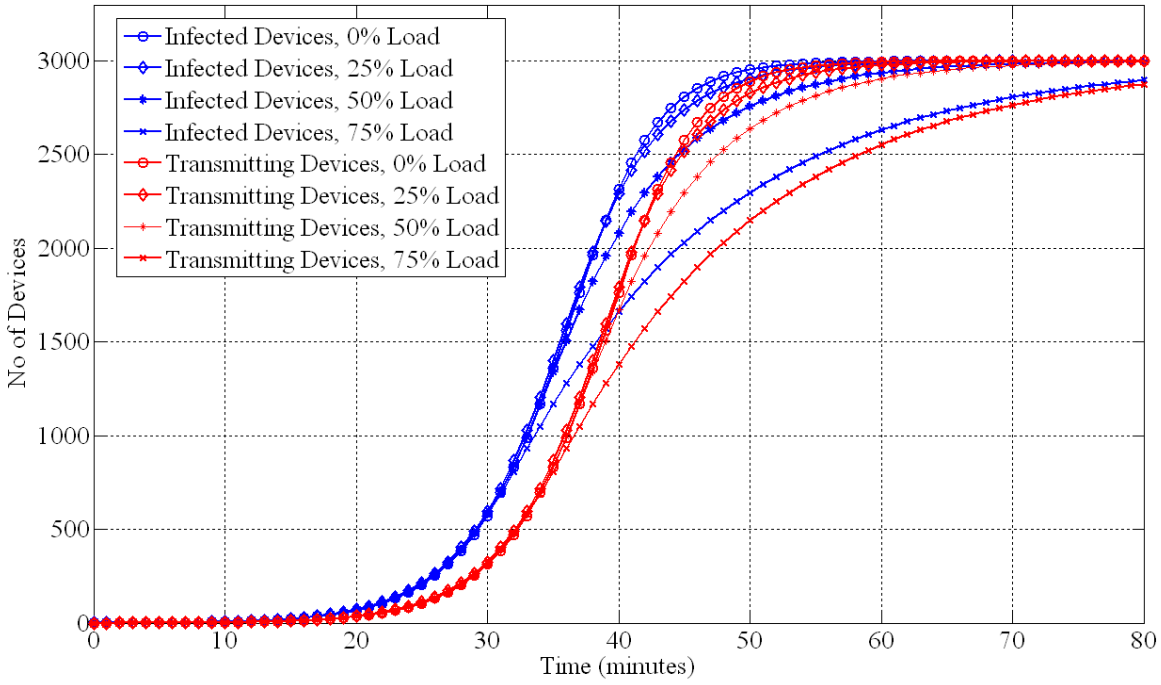


Figure 7.9: Infected and Transmitting Devices for Various Additional Loads, with Hardware Limitations of 2500 msgs/sec for a Maximum Population of 3000 and one Initial Infection

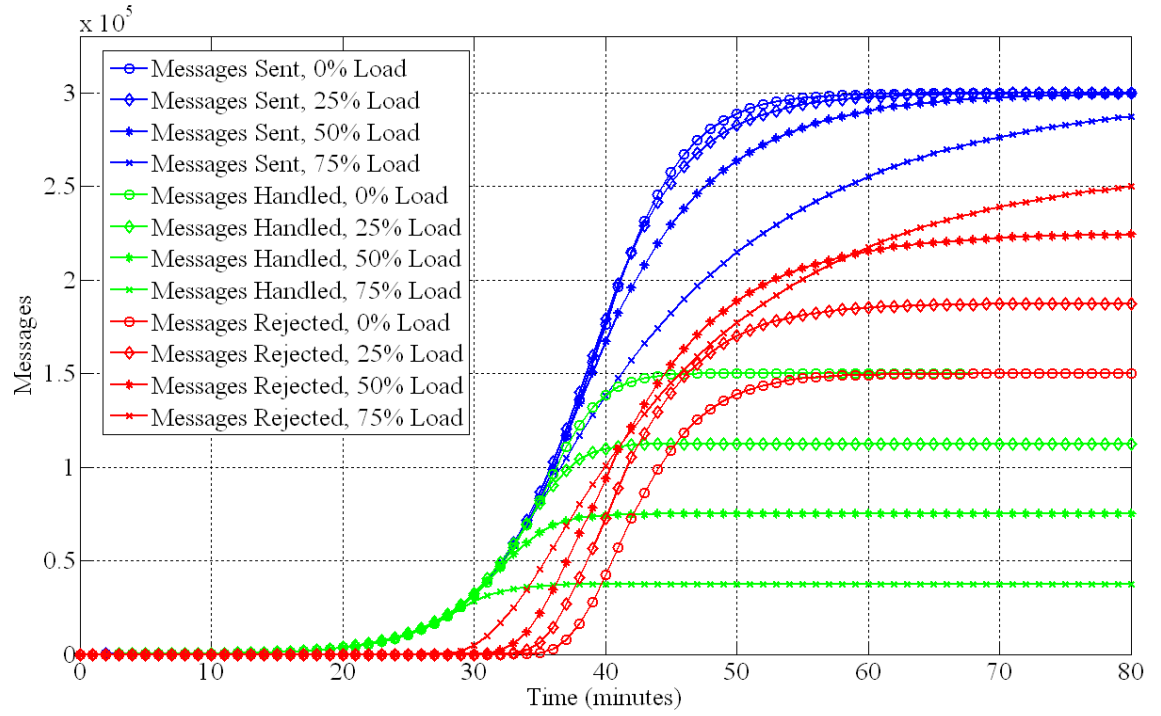


Figure 7.10: Number of Messages Sent, Handled, and Rejected for Various Additional Loads, with Hardware Limitations of 2500 msgs/sec for a Maximum Population of 3000 and one Initial Infection

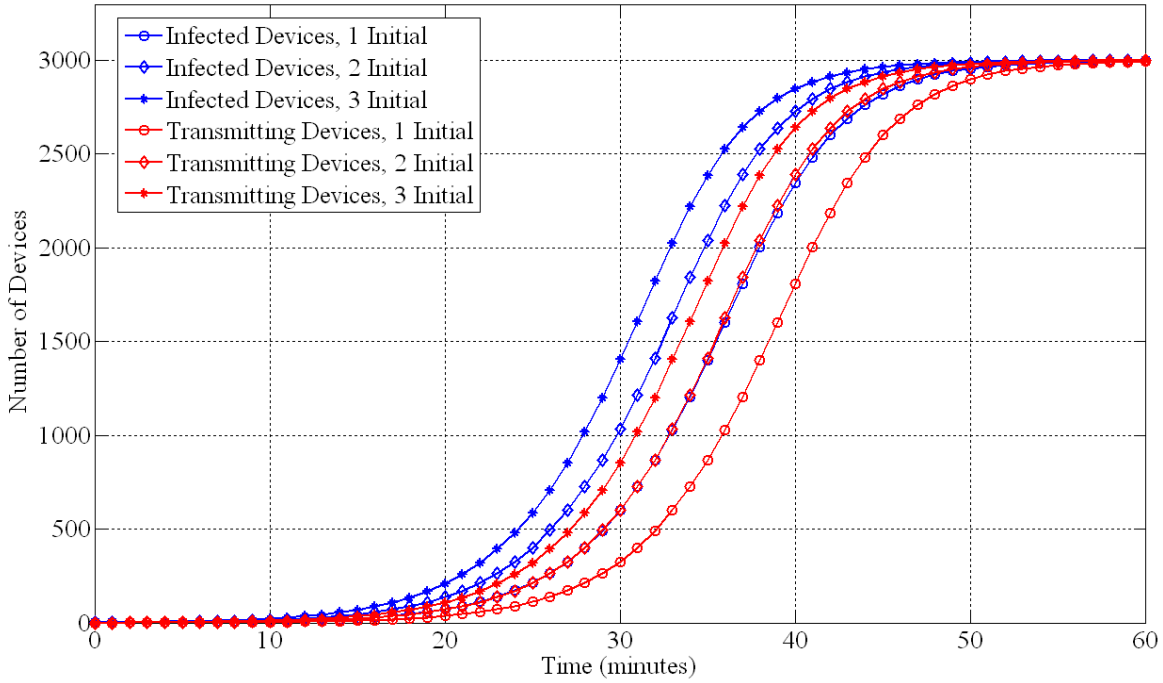


Figure 7.11: The Impact of Initial Infections, with no Additional Load and Hardware Limitations of 2500 msgs/sec for a Maximum Population of 3000

Table 7.5: Time to Network Saturation (minutes) for Various Initial Infections and Additional Loads

Population	Initial Infections	0% Load	25% Load	50% Load	75% Load
1500	1	49.2	38.6	35.1	31.0
	2	46.2	35.1	31.9	28.0
	3	44.1	33.3	30.0	26.1
3000	1	38.2	36.4	34.2	30.7
	2	35.1	33.2	31.0	27.6
	3	33.2	31.4	29.1	25.6
4500	1	37.7	36.1	34.0	30.8
	2	34.3	33.0	30.7	27.5
	3	32.6	30.8	28.9	25.5

From Figure 7.9, it is apparent that high additional loading on the infrastructure will impair the ability of mobile worms to propagate and spread; the plot for a 75% additional load does not reach its theoretical maximum within eighty minutes. However, the higher the additional load, the less time it takes for the infrastructure hardware to reach a saturated state, as is shown in Figure 7.10 and Table 7.5. A continuous existing additional load was assumed, in order to clearly illustrate that

more messages will fail as opposed to being successfully processed. Figure 7.11 and Table 7.5 show that more initial infections results in the infections spreading faster.

The above simulations were done for smaller populations, approximating 0.1% of a metropolitan area. The simulations in Figure 7.12 to Figure 7.14 increase the maximum number of devices that can be infected to 30000, which is approximately 1% of a metropolitan population in South Africa. As there are five mobile networks, the simulations will use five SMSCs, each with a processing capability of 2500 messages per second.

Figure 7.12 shows a comparison of number of infected and transmitting devices for various loads; the corresponding number of messages sent, handled and rejected for various loads are shown in Figure 7.13. Figure 7.14 shows the impact of the initial number of infections. Table 7.6 provides the time until the mobile infrastructure is overloaded for various populations, loads, and initial infections.

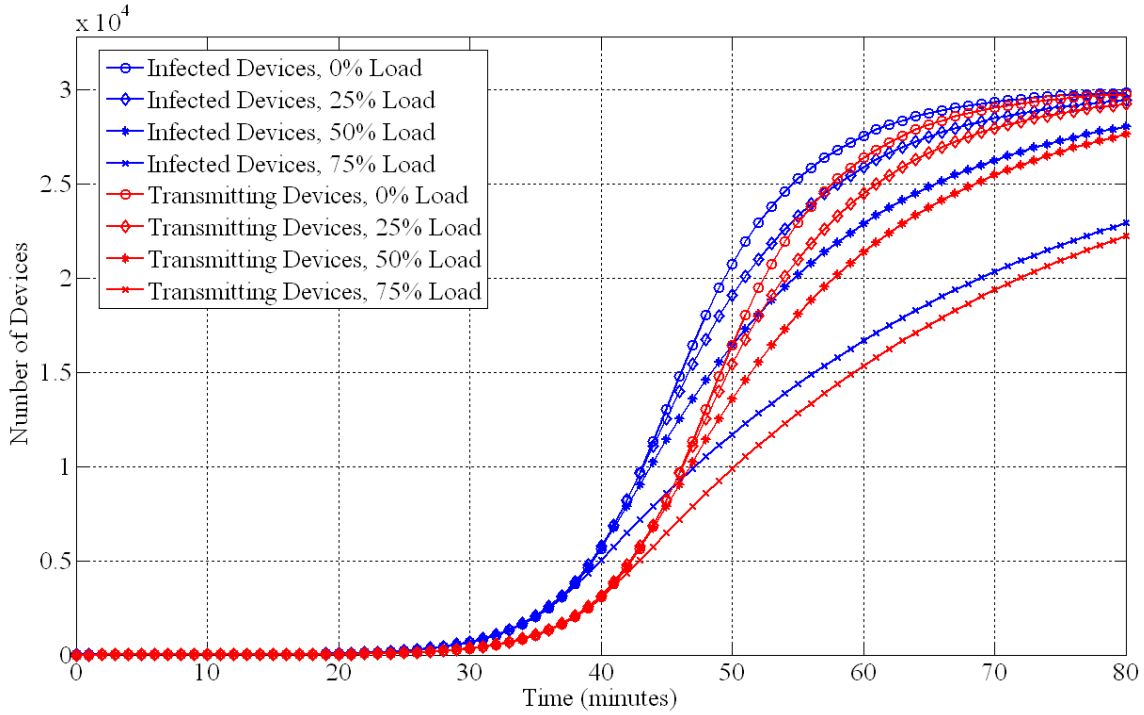


Figure 7.12: Infected and Transmitting Devices for Various Additiona1 Loads, one Initial Infection, Hardware Limitation of 2500 msgs/sec (using five SMSCs), and a Maximum Population of 30000

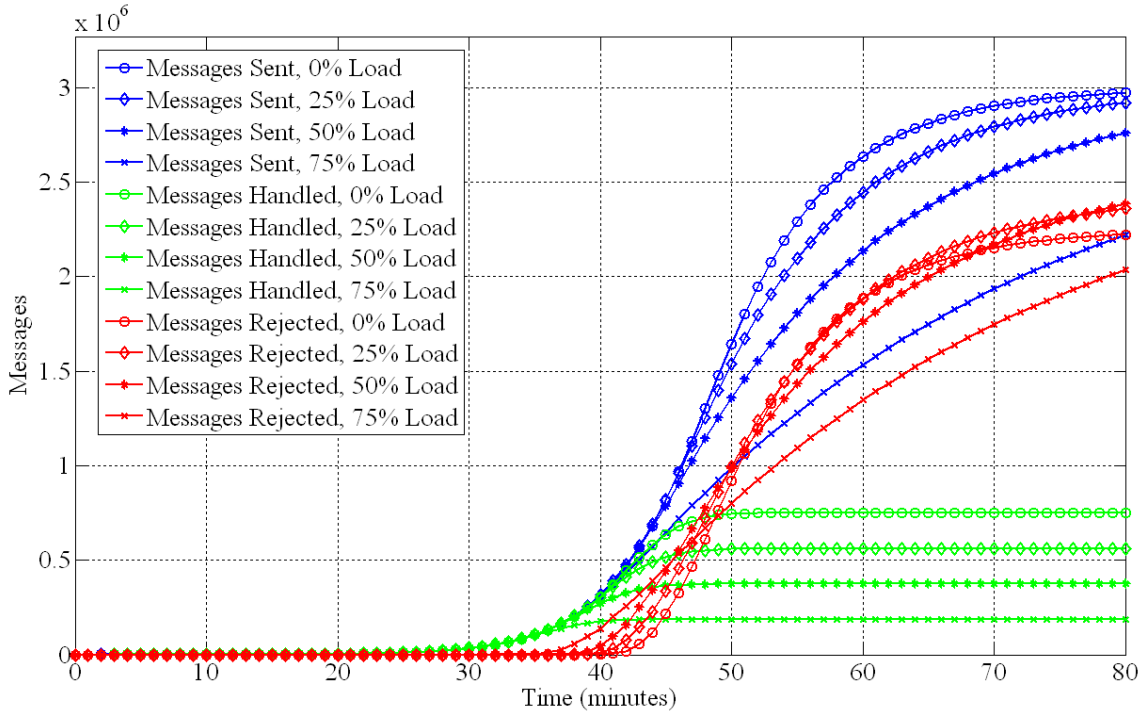


Figure 7.13: Messages Sent, Handled and Rejected for Various Loads, one Initial Infection, Hardware Limitation of 2500 msgs/sec (using five SMSCs), and a Maximum Population of 30000

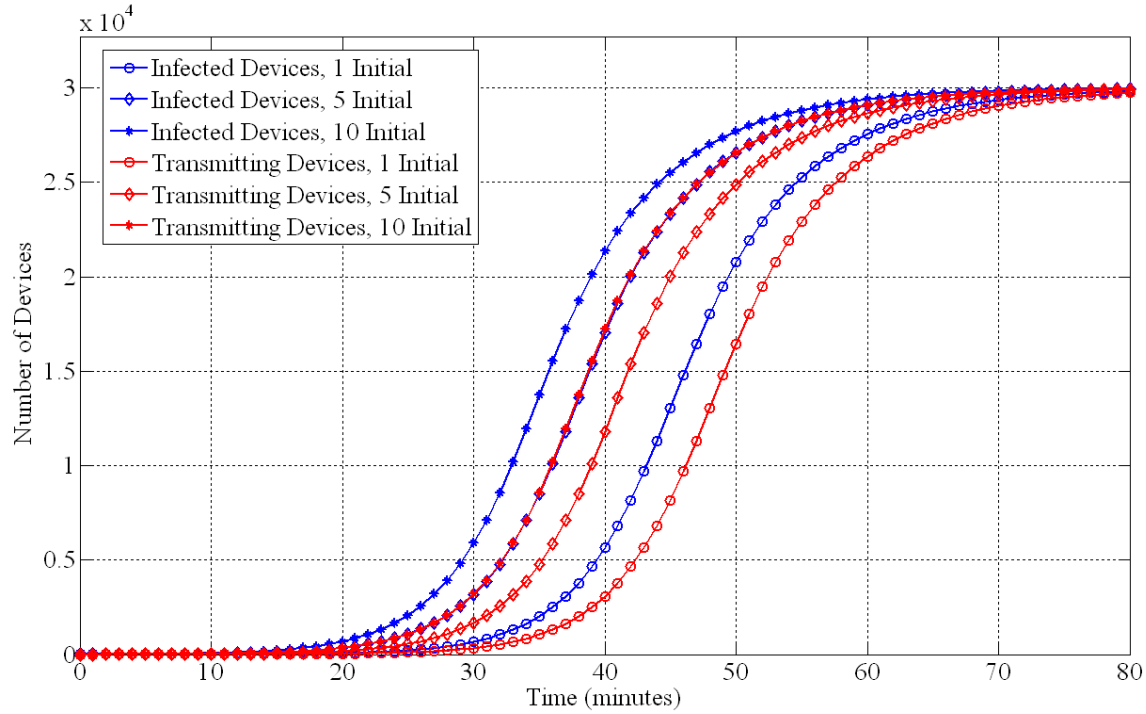


Figure 7.14: The Impact of Initial Infections, no Additional Load, Hardware Limitation of 2500 msgs/sec (using five SMSCs), and a Maximum Population of 30000.

Table 7.6: Time to Network Saturation (minutes) for Various Initial Infections and Additional Loads, with Hardware Limitations of 2500 msgs/sec

Population	Initial Infections	0% Load	25% Load	50% Load	75% Load
15000	1	45.4	43.8	41.4	37.8
	5	38.1	36.3	34.0	30.6
	10	34.9	33.1	30.9	27.5
30000	1	44.6	43.1	41.0	37.8
	5	37.2	35.7	33.6	30.4
	10	34.1	32.4	30.6	27.4
45000	1	44.4	43.0	41.0	37.8
	5	37.1	35.4	33.6	30.3
	10	33.9	32.3	30.4	27.2

Figure 7.12 again illustrates that higher loads impair the ability of the mobile worm to spread infections, however these loads result in reduced times to infrastructure saturation, as shown in Figure 7.13 and Table 7.6. Figure 7.14 again shows that larger numbers of initial infections tend to accelerate the propagation of the worm. Based on the times for a metropolitan area shown in Table 7.6, assuming 1% of that population has devices that can be infected, the mobile infrastructure could become saturated with illegitimate message in approximately twenty-seven to forty-five minutes. For this given scenario in the simulations, it may take a few hours for the worm to infect the maximum possible number of devices.

Traynor *et al*. (2009) show that 23 500 infected devices should be sufficient to reduce the ability of HLRs to carry legitimate traffic by 75%, or 141 000 infected devices for higher capability HLRs. Given the malware propagation illustrated in Figure 7.12, this will be achieved in an hour. This indicates that should the concentration of the infections be too widespread to perform a DoS attack on an SMSC or the control channels, the impact on the HLR may still deny services. From Section 6.3.2, the example of a mobile botnet using geo-location to instruct all infected devices to flood the mobile network in a specific geographic region may easily be used to deny mobile services given the results of the simulations.

7.4.3 Summary of Mobile Network Traffic Simulations

Basing the SMSC processing capacity as 2500 messages per second, and one SMSC per mobile network in a metropolitan area, 12500 messages per second would be required to overload all

mobile networks in a metropolitan area. From Section 7.3, it was calculated that 7095 messages per second would be required to saturate the SDCCHs in a metropolitan area. Therefore it is more likely that the SDCCH would become overloaded prior to the SMSC, however the overall impact will be the same; mobile services in the metropolitan area would be denied or severely degraded. From the simulation results and calculations in Section 7.3, it would be safe to assume that the degradation or service denial will become noticeable within an hour. This lends legitimacy to the Cyber Shockwave scenario presented by CNN (Cable News Network, 2010), and discussed in Section 5.5.2.6; where city-wide mobile communications were being lost due to the spread of a mobile worm.

The limitations of mobile devices may also impact on the propagation of mobile malware. Devices may not be able to process the quantities of messages the malware is attempting to send. For example, if the malware attempts to send a message to everyone on the contact list every one minute and there are a hundred contacts, that could result in the device trying to send more than one message a second. This could render the device unusable, and the user may simply switch off the device to prevent financial loss due to the sheer number of messages. This will still effectively deny mobile service to those users, and there will still be the psychological impact of the frustration due to the incoming and outgoing messages on the device.

7.5 Calculations for Jamming and Detection Ranges

This section calculates the range at which wireless signals, both from mobile infrastructure, and wireless networking, can be effectively detected and jammed. This will therefore be primarily related to the electronic warfare functional area. These calculations are done in such a way that the maximum theoretical jamming or detection range is calculated, assuming perfect conditions. However, these ranges may be reduced according to local geography and built environment.

Section 7.5.1 calculates the maximum range at which mobile phone signals can be effectively jammed, and Section 7.5.2 calculates the maximum range for which these signals can be detected. Section 7.5.3 calculates the jamming range for wireless networking, and Section 7.5.4 calculates the range for which these signals can be detected. Section 7.5.5 summarises the section.

7.5.1 Jamming Mobile Phone Channels

This section calculates the maximum range for which a jammer of given power can effectively jam the channels between the mobile device and the base station. Mobile communications using GSM

operate on four main frequencies: 850MHz, 900MHz, 1800MHz, and 1900 MHz (Adamy, 2009; Ojanpera & Prasad, 1998).

For the purpose of these calculations, we can assume the height of the base station is 30m, the height of the mobile device is 1.5m, and the height of the jammer's antenna, h_j, is 3m. The distance between the mobile device and the base station is 1km. The effective radiated power (ERP) of the base station is typically 10W to 50W (Adamy, 2009), which corresponds to 40dBm to 47dBm. The ERP of the mobile device is typically 1W to 6W (Adamy, 2009), corresponding to 30dBm to 37.8dBm. From the list of radio frequency power sources for communication jammers surveyed in Holt (2010), an output power of 100W (50dBm) is typical for a jammer that can operate across all four frequencies of the mobile phones.

Equation 2.10 in Section 2.5.5 provides the equation for the jammer-to-signal ration (JSR):

$$JSR = ERP_j - ERP_s - L_j + L_s + G_{rj} - G_r$$

For the purposes of these calculations, the antenna gains, G_{rj} and G_r, can be ignored. For digital communications, such as GSM and WCDMA that is used in South Africa, the JSR should be equal to or greater than 0dB to successfully jam the channel. To calculate the maximum jamming range, the JSR is set to zero, and the channel loss for the jamming signal, L_j, is replaced with the relevant equations for line of sight propagation and two-ray propagation. Equation 2.6 in Section 2.5.4.1 gives the calculation for line of sight propagation:

$$L = 32.44 + 20\log_{10} d + 20\log_{10} f$$

Equation 2.7 in Section 2.5.4.1 gives the calculation for two-ray propagation:

$$L = 120{+}40\log_{10} d - 20\log_{10} h_T - 20\log_{10} h_R$$

The general equation to calculate the maximum jamming distance becomes:

$$d_j = 10^{A/B} \quad \textbf{7.2}$$

where d_j is the maximum jamming range. The numerator (A) and denominator (B) of the exponent for line of sight propagation are:

$$A = ERPj - ERPs + Ls - 32.44 - 20\log_{10} f \text{ and } B = 20 \quad \textbf{7.3}$$

where L_s, is the channel loss of the desired signal, ERP_j is the ERP of the jammer, and ERP_s is the ERP of the desired signal. The equation for the case of two-ray propagation becomes:

$$A = ERPj - ERPs + Ls - 120 + 20\log_{10} h_j + 20\log_{10} h_R \text{ and } B = 40 \quad \textbf{7.4}$$

where h_j is the height of the jamming antenna and h_R is the height of the targeted antenna.

The first step is to calculate the Fresnel Zone of the desired signal. Equation 2.5 in Section 2.5.4.1 is used:

$$FZ = \frac{f \times h_T \times h_R}{24000}$$

Table 7.7 gives the Fresnel Zone figures for the four frequencies. As the distance between the mobile device and base station is 1km, line of sight propagation occurs for all four frequencies; the channel loss is also provided in Table 7.7.

Table 7.7: Fresnel Zone and Channel Loss for the Desired Signal

f (MHz)	850	900	1800	1900
FZ (km)	1.59	1.69	3.38	3.56
L_s (dB)	91.03	91.52	97.55	98.02

Two strategies can be employed: jam the downlink (base station to mobile device) or the uplink (mobile device to base station). The Fresnel Zones for the cases of jamming the downlink and uplink are shown in Table 7.8. To jam the downlink, the mobile device is targeted, and the base station is targeted to jam the uplink.

Table 7.8: Fresnel Zones for Jamming Signals

f (MHz)	850	900	1800	1900
FZ (km) Jamming downlink	0.16	0.17	0.34	0.36
FZ (km) Jamming uplink	3.19	3.38	6.75	7.13

As the range is not known before the calculation, the ranges need to be solved for both line of sight and two-ray propagation using Equations 7.2 and 7.4; these ranges are shown in Table 7.9. The ERP of the base station was set to 10W. The figures for the line of sight propagation are larger than that of the corresponding Fresnel Zone, therefore they are incorrect, and two-ray propagation occurs. The irrelevant distances are formatted with the strikethrough.

Table 7.9: Jamming Ranges for Targeting the Downlink for a Jammer Output Power of 100W

Freq (MHz)	850	900	1800	1900
d_j (km) Line of sight	~~3.16~~	~~3.16~~	~~3.16~~	~~3.16~~
d_j (km) Two-Ray	0.71	0.72	1.05	1.07

This process is repeated for the case of jamming the uplink, and the results are shown in Table 7.10. The ERP of the mobile device was set to 1 W. Again, the line-of-sight propagation figures are proven to be incorrect, and two-ray propagation occurs. The irrelevant distances are formatted with the strikethrough.

Table 7.10: Jamming Ranges for Targeting the Uplink for a Jammer Output Power of 100W

Freq (MHz)	850	900	1800	1900
d_j (km) Line of sight	~~10~~	~~10~~	~~10~~	~~10~~
d_j (km) Two-Ray	5.66	5.82	8.32	8.51

By comparing the two sets of results for the downlink and uplink, it can be seen that the maximum jamming for the case of targeting the uplink is greater; therefore that is the most effective strategy. These results give the case for the maximum jamming range for a jammer with 100 W ERP, resulting in a JSR of 0 dB, which will allow the jammer to jam only one channel at any given time. To jam more channels, the jammer will either have to reduce the distance to the target, or radiate more power. The maximum jamming range of all cases is 8.5km for a frequency of 1900 MHz. At this range, nine devices are required to cover a metropolitan area of 2000 km^2.

The largest output power of the devices listed by Holt (2010) that can cover all four mobile frequencies is 300 W (54.77 dBm). Table 7.11 provides the maximum jamming range for a device with this output power. As it was established that two-ray propagation was applicable to both the downlink and uplink, only these figures are calculated.

Table 7.11: Jamming Ranges for a Jammer Output Power of 300W

Freq (MHz)	850	900	1800	1900
d_j (km) Downlink	0.94	0.96	1.36	1.40
d_j (km) Uplink	7.45	7.66	10.84	11.14

The maximum range is extended to 11.14 km for the case of the jammer with an output power of 300 W. For this range, six devices would be required to cover a metropolitan area of 2000 km^2. Given that a DoS such as described in Sections 7.3 and 7.4.2 could be launched from any location with access to a mobile phone signal or Internet access, the range limitation of the jammers make

them ineffective if a large scale DoS is intended, unless there are electronic warfare assets in the region, such as in a peace-keeping operation.

There are commercial mobile phone jammers that are available which can be used for both GSM and 3G mobile phones (Nichols & Lekkas, 2002). Assuming a power output of 300W, and a maximum range of 11km; each device will be able to cover an area of 390 km^2. For the South African metropolitan areas, this will require between four and seven devices. For an output power of 100W and a maximum range of 8.5km, each device will be able to cover an area of 227 km^2; therefore between seven and eleven device would be required. Given the strength of the device output signals, it will not take long to triangulate the position of these devices using electronic warfare direction finding equipment, and neutralise them. The effects therefore will be temporary.

7.5.2 Detecting Mobile Channels

For these calculations, the height and ERP of the base station and mobile device will be the same as those in Section 7.5.1. As with jamming, the first step is to calculate the Fresnel Zones; Table 7.12 provides these for detecting the downlink and uplink. To detect the downlink, the target is the base station transmission, and the target is the mobile device to detect the uplink.

Table 7.12: Fresnel Zones for Detecting Signals

f (MHz)	850	900	1800	1900
FZ (km) Detecting Uplink	0.16	0.17	0.34	0.36
FZ (km) Detecting downlink	3.19	3.38	6.75	7.13

To calculate the distance at which a signal can be detected for line of sight propagation was given in Section 2.5.4, Equation 2.8:

$$20\log_{10} d = P_T + G_T + G_R - 32.44 - 20\log_{10} f - S$$

To calculate the distance at which a signal can be detected for two-ray propagation was given in Section 2.5.4, Equation 2.9:

$$40\log_{10} d = P_T + G_T + G_R - 120 + 20\log_{10} h_T + 20\log_{10} h_R - S$$

Solving for *d* gives the range at which the signals can be detected. For the calculation a receiver that can work with GSM, CDMA and EVDO (data) variations will be used; it can operate over a

frequency range of 80MHz – 3GHz, and has a sensitivity of -131dBm (Holt, 2009a). This is also one of the most sensitive receivers listed, which will provide a truly maximum range for which these signals can be detected. A typical SIGINT antenna will have a gain in the region of 5dB to 20dB (Holt, 2009b); for the purposes of these calculations a mid-range figure of 12dB will be used. Table 7.13 provides the detection ranges for the downlink and uplink of mobile phones; as with the jamming, the range was calculated for both the line of sight and two-ray propagation.

Table 7.13: Detection Ranges for Mobile Phones

f (MHz)	850	900	1800	1900
Downlink Detection Range (km) Line of Sight	~~39681~~	~~37476~~	~~18738~~	~~17752~~
Downlink Detection Range (km) Two-Ray	356.55	356.55	356.55	356.55
Uplink Detection Range (km) Line of Sight	~~12548~~	~~11851~~	~~5926~~	~~5614~~
Uplink Detection Range (km) Two-Ray	44.83	44.83	44.83	44.83

Given the results of for line of sight propagation, which are clearly incorrect as they are too large, two-ray propagation occurs between the intercept antenna and the mobile device or base station. The irrelevant distances are formatted with the strikethrough. The downlink signal can therefore be detected at a range of 356.55 km, and the uplink can be detected at a range of 44.83 km. These ranges are for all frequencies, and two-ray propagation is frequency independent (for the case of the jamming, channel loss between the device and base station was frequency dependent, therefore the range would not be the same for all frequencies). If both parts of the conversation need to be intercepted, then both the uplink and downlink would be required; the range will then be limited to 44.83 km.

Given the Athens Affair incident discussed in Section 5.5.1.2, where the actual infrastructure was compromised in order to eavesdrop, the electronic warfare option is not the most efficient. As with jamming, it will only be practical where electronic warfare assets are present, such as in peacekeeping operations.

7.5.3 Jamming WLAN and Bluetooth

The process and formulae for calculating the jamming range are the same as those in Section 7.5.1. Both WLAN and Bluetooth operate on a frequency of 2.4GHz and have similar power outputs, therefore they present a similar target from an electronic warfare perspective. Bluetooth devices with a class 2 power output (which will be used for connecting devices and peripherals) have an ERP of 2.5mW (4dBm). It can be assumed these devices will be at a height of 1.1m, and connect over a distance of 9m. Bluetooth devices with a class 1 power output (such as access points) have an output power of 100mW (20dBm), and can be assumed to be located at a height of 2m and connect at distances of 90m. A jamming output power of 100W and 300W will be used for the calculations. As in Section 7.5.1, the ranges are calculated for the case when the devices are operating near their maximum range in order to estimate the maximum distance at which jamming will be effective. Table 7.14 provides the details and results of the calculations.

Table 7.14: Calculation Results for Jamming WLAN and Bluetooth

	Two devices (9m separation)	Access point to device	Device to access point	Two access points (90m separation)
FZ for the desired channel (km)	0.12	0.22	0.22	0.4
Loss for the desired channel (dB)	59.13	59.13	59.13	79.13
FZ for the jamming channel (km)	0.33	0.33	0.6	0.6
Range for line of sight (km), 100W	~~1.8~~	0.28	~~1.8~~	~~1.8~~
Range for two-ray (km), 100W	0.77	~~0.31~~	1.04	1.04
Range for line of sight (km), 300W	~~3.11~~	~~0.49~~	~~3.11~~	~~3.11~~
Range for two-ray (km), 300W	1.02	0.40	1.37	1.37

From the results in Table 7.14, it can be seen that in all cases, except for the case of an access point transmitting to a device and a jammer with an ERP of 100W, that two-ray propagation will occur as the distances for line of sight are larger than the Fresnel Zone. For the case of the access point to the device and a jammer ERP of 100W, the two-ray propagation calculation yields a distance less than the Fresnel Zone; therefore line of sight propagation will occur. The irrelevant distances are

formatted with the strikethrough. The maximum jamming range for all cases is 1.37 km. Assuming commercial jamming devices with an output of 300W; each device will cover an area of 5.9km^2. For this coverage, over three hundred devices will be required to cover a metropolitan area of 2000km^2.

As WLAN and Bluetooth utilise frequency hopping, there may be additional complexities, as the signal never remains on the same frequency for long. The jammer may be able to track the hopping, and therefore ensure that the majority of the transmitted signal is unreadable. However, in an environment that has multiple WLAN connections it may be difficult to track the exact signal, therefore it may be a better strategy to distribute the jammer ERP over all signals detected at that location.

7.5.4 Detecting WLAN and Bluetooth Transmissions

This section calculates the maximum range for which WLAN and Bluetooth signals can be detected. The equations and detection specifications are the same as Section 7.5.2: the receiver has a sensitivity of -131dBm, and the antenna has a gain of 12dB. The operating frequencies, ERPs, heights, and distances are the same as in Section 7.5.3. Table 7.15 shows the relevant Fresnel Zones and detection ranges. As before, the range was calculated for both line of sight and two-ray propagation.

Table 7.15: Calculation Results for Detecting WLAN and Bluetooth

	Device (2.5mW)	Access Point (100mW)
FZ (km)	0.33	0.63
Line of Sight	~~222.73~~	~~1405.4~~
Two-Ray	8.60	29.11

As before, the line of sight calculations yields distances which are larger than the Fresnel Zone, and are therefore incorrect; two-ray propagation occurs. The irrelevant distances are formatted with the strikethrough. For the calculations, it can be seen that the presence of a signal originating from a device with an ERP of 2.5mW is 8.6km; and 29.11km for an access point with an ERP of 100W.

For eavesdropping the issue of frequency hopping is different; the signal needs to be tracked for all its hops. Many commercial and free WLAN detection software versions are available for devices with wireless network interface cards; coupling sensitive detection equipment to a notebook may facilitate improved performance. Given the ranges calculated, this option would be expensive, and

having someone in a position nearby the target will be more cost effective and achieve the same results.

7.5.5 Discussion and Summary of Jamming and Detection Range Calculations

For eavesdropping on WLAN or Bluetooth, using specialist sensitive equipment may not necessarily improve the effectiveness of intercepting the signal; given the ranges, having someone near the target to intercept the signals will achieve the same results with no real extra complexity. For the case of jamming WLAN and Bluetooth signals, it may be difficult to track a single signal in a highly populated environment. Therefore jamming all signals in the target's location may be simpler and achieves the desired effect, even if it is not as efficient. A significant problem in using electronic warfare attacks to target these signals in an urban environment, is trying to locate and lock onto the correct signal in a very highly populated electromagnetic spectrum. Jamming will prove to be a simpler exercise; however any devices radiating enough power to jam the signals over a large area will be easily located by direction finding equipment.

Given the ranges for eavesdropping and jamming, targeting a choke point where large quantities of traffic related to the target may be more efficient. This allows the attacker to disrupt or intercept multiple communications with less control; to target the mobile devices will require more assets. For example, if an organisation's mail server is targeted, the relevant emails will be intercepted as long as the target is using the organisation's email system, even if the target is at a remote location. Targeting these network components may also be done from any location with an Internet connection, whereas targeting the wireless channel requires proximity to the target. Electronic warfare attacks therefore will probably be less effective than network warfare attacks unless there are military electronic warfare assets in the vicinity.

7.6 Simulations for CDMA Eavesdropping and Jamming

This section provides simulations for the case of using an intercepted spreading sequence to eavesdrop or jam a CDMA signal. A previous version of this section was published in van Niekerk and Maharaj (2010b).

In 3G mobile communications, the signal is modulated with CDMA spread-spectrum technology. As discussed in Sections 2.5.5 and 2.8.4.2, CDMA uses a unique spreading sequence for the transmitting and reception of the signals. These signals are difficult to detect and are jam resistant due to the correlation characteristics of the spreading sequence. A method of circumventing this is

to estimate the sequence used for spreading by analysing the signal; for commercial applications such as mobile phones the spreading sequences are relatively short and this may be possible, however long spreading sequences used in military communications may prove to require large computing resources (Adamy, 2009). Yao and Poor (2001) proposed a process that uses an expectation-maximisation algorithm to estimate the spreading sequence, and was aimed at primarily eavesdropping applications (Yao & Poor, 2001); however, the estimated sequence may also be used to improve jammer performance by mitigating the processing gain. By estimating the spreading sequence, information is gained which will allow for correlated jamming (Shafiee & Ulukus, 2009).

Simulations were performed using the Matlab software to investigate the effects of the correlation between the estimated sequence correlation and the actual sequence on jammer and detector performance. The simulations were done for a specific SNR and JSR, and performance is determined by the BER. The simulations were Monte Carlo simulations, where the data streams and channel noise was randomly generated; the simulations results were averaged over 100 iterations. The generated data streams consisted of 100000 bits for each user, and the generated channel noise was additive white Gaussian noise at a SNR of 10 dB. No other channel characteristics were modelled. A total of six users were simulated, and all signals had equal strength at the receiver. The simulations are based on Equations 2.18 and 2.19 in Section 2.8.4.2, which describe multiuser environment of mobile communications. The channel is described by:

$$\mathbf{y}(i)=\mathbf{S}\mathbf{A}\mathbf{b}(i)+\mathbf{n}(i),$$

and the output of the detector is described by:

$$\mathbf{r}=\mathbf{R}\mathbf{b}+\mathbf{n}.$$

Length-31 Gold codes were as spreading sequences to generate the correlation matrix; the values of this matrix were then adjusted to test the impact of correlation between the estimated and actual sequences. Various values for the JSR at the receiver were used for the jamming simulation, and the jammer was considered as one of the six users. Figure 7.15 shows the results of the jamming simulation. A 30% bound is shown in the figure, as for digital signals approximately 30% of the signal needs to be jammed for the jamming to be effective (Adamy, 2009; Poisel, 2004).

For low values of JSR, high correlation is required to have an impact on the target signal. As the JSR increases, the correlation value required to effectively jam the signal decreases. This indicates that powerful jammers (or jammers close to the target receiver) may overcome spread spectrum communications. However, for jammers with limited ERP, using an estimated sequence can

improve the effectiveness of the jammer. The estimated sequence will need to be accurate, as a JSR of 5 dB (the signal is three times stronger) requires a correlation of 0.6 between the estimated sequence and actual sequence.

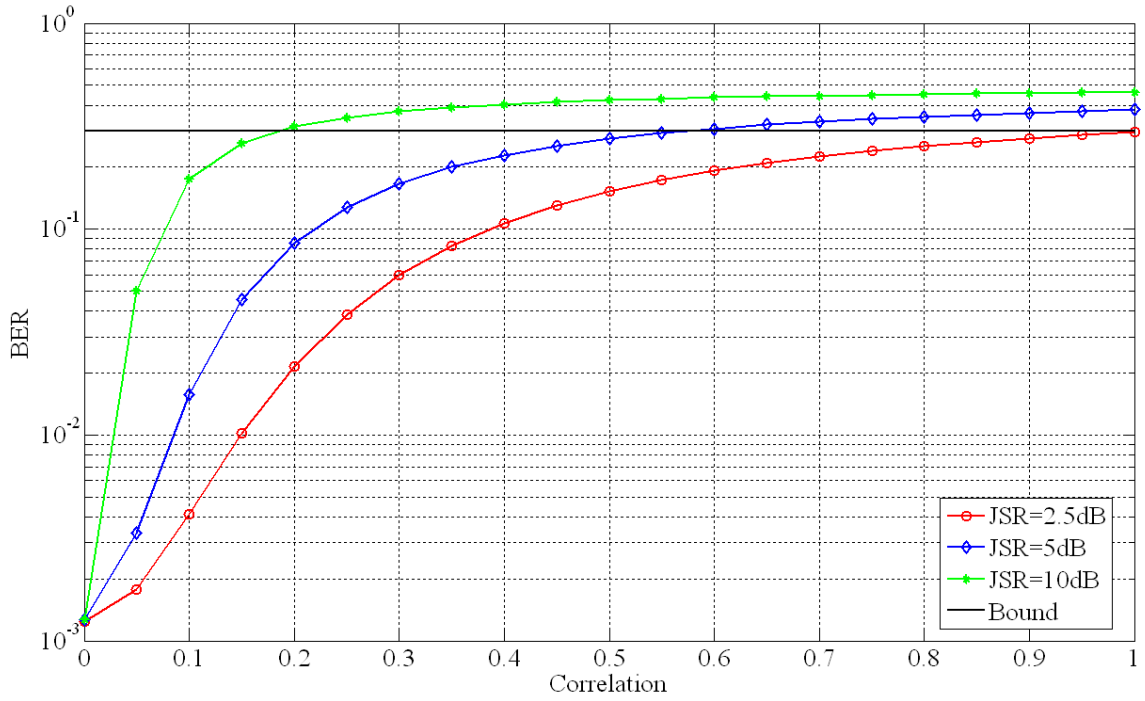


Figure 7.15: Signal Performance under Spread Jamming

Figure 7.16 shows the results of the eavesdropping simulation. This figure illustrates that very high correlation between the estimated and actual sequences is required to achieve reasonable eavesdropping performance, even for high SNRs. The simulation assumes perfect power control; this is unlikely at an intercept receiver, and channel characteristics such as fading were not modelled. Therefore it can be assumed that actual performance would be worse, requiring a higher correlation value. There is also the added complexity of the timing of the signal; synchronous signals may be easier to estimate the spreading sequence conduct eavesdropping, whereas asynchronous signals will be more difficult. The jamming scenario does not require correlation values as high as eavesdropping, as the intention is to introduce errors, and any additional interference will have some detrimental effect on the target signal. For eavesdropping, the objective is to correctly demodulate the target signal without errors; this is highly dependent on the estimated sequence being correct. The requirements for this form of eavesdropping are therefore much higher than for jamming.

As discussed in Sections 7.5.1 and 7.5.2, the ability to jam or eavesdrop on the mobile wireless channels is local; combined with the limitations of effectively jamming or eavesdropping on 3G signals, this method is not efficient unless there is a presence of specialist military electronic warfare assets in the area.

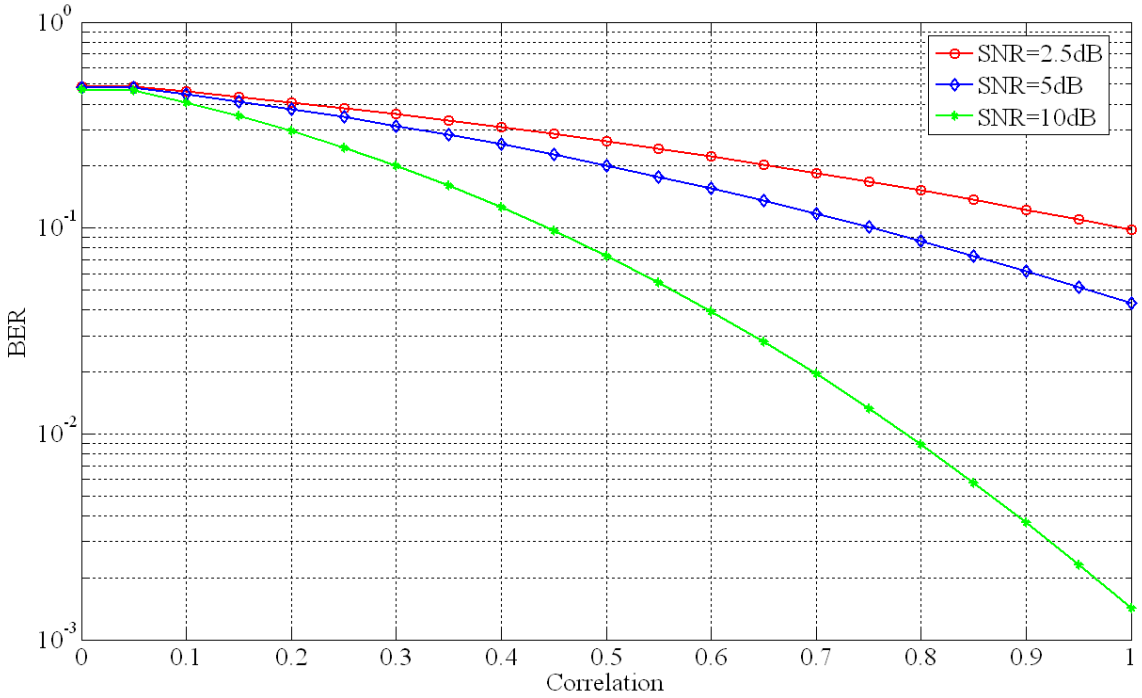


Figure 7.16: Performance of Eavesdropping Using an Estimated Sequence

7.7 Chapter Summary

In Section 7.2, the mobile infrastructure was analysed through the use of graph theory to determine critical nodes. The analysis illustrates that a mobile infrastructure is not scale-free, but appears to have critical nodes according to geographical areas; BSCs control localised areas, and MSCs and HLRs control larger geographical areas. This also may impact on the capacity of the control channels in the densely populated metropolitan areas.

Section 7.3 calculates the capacity of the control channels for South African metropolitan areas, and the feasibility of launching a DoS attack via web-based SMS services. This showed that just over 7000 messages per second were sufficient to deny services to a metropolitan area, and that the Internet traffic required was feasible to compromise the web-based SMS services. Section 7.4 simulates the propagation of mobile malware and the time taken for the infrastructure hardware to become overloaded, assuming no channel limitations. This illustrated that the hardware of a

metropolitan area could become overwhelmed in less than an hour; however given the messages required to achieve this, it is more likely that the control channels will become saturated.

Sections 7.5 and 7.6 assess the feasibility of electronic warfare attacks against the wireless channels; Section 7.5 calculates the maximum effective range for jamming and detecting the uplink and downlink of mobile communications, and wireless networking. The ranges are in the order of kilometres and can only cover localised regions; whereas the eavesdropping attacks experienced in Greece has the capability of intercepting specific phone numbers, and multiple targets from wider geographic regions, without having to track the targets movements. Section 7.6 simulates the performance of jamming and eavesdropping on 3G communications where the attacker attempts to estimate the spreading sequence. While the complexity of eavesdropping is prohibitive without specialist equipment, jamming is feasible, but the range will again be limited. Compared to the possibility of a mobile worm or exploiting web-based SMS services to perform DoS attacks, the electronic warfare attacks are not much of a threat unless there is hostile electronic warfare equipment in the vicinity.

Chapter 8. Vulnerability Assessment

8.1 Introduction

This chapter triangulates the data from Chapters 5 to 7 and uses this to assess the vulnerability of the mobile infrastructure from an IW perspective. This is a primary objective of the study. Section 8.2 discusses the criticality of the mobile infrastructure; and Section 8.3 discusses the threats. The vulnerabilities and the associated impacts are discussed in Section 8.4; the modified TVA worksheet and risk assessment is presented in Section 8.5. Section 8.6 calculates and presents the infrastructure risk and vulnerability ratings and Section 8.7 presents opportunities to improve these ratings. Section 8.8 reviews the proposed assessment and the chapter is summarised in Section 8.9.

8.2 Criticality of the Mobile Infrastructure

An objective of the study was to provide an indication of the criticality of the mobile infrastructure. The information that contributes to this originates from the literature, interviews (Section 6.2), and pilot survey (Section 6.4).

In the literature (Section 2.8.4.3), the high prevalence of mobile communications in South Africa was noted. There is a ratio of 10.75 mobile telecommunication subscriptions for every fixed-line subscription; there are 10.85 mobile broadband subscriptions for every fixed-line broadband subscription. There are 92.67 mobile subscriptions per 100 inhabitants, and 10.52 mobile broadband subscriptions per 100 inhabitants in South Africa (International Telecommunications Union, 2011). A number of health and socio-economic development projects in Africa also utilise the mobile infrastructure. This level of prevalence implies a high reliance on mobile communications in South Africa, which indicates that the mobile infrastructure can be considered as critical to the social and economic wellbeing of South Africa.

From the interviews, ten of the twelve respondents indicated that the mobile infrastructure is part of the critical information infrastructure; the remaining two were unsure. The reasons provided indicates that the mobile infrastructure forms part of the national information and communications infrastructure, which is considered as critical. The reliance on mobile communications was raised, in particular their use by emergency services, government and businesses. A respondent indicated that some organisations in the developed world are solely reliant on mobile communications. These responses indicate that the expert opinion considers mobile communications as critical.

Five of seven respondents indicated that there should be explicit protection policies for the mobile infrastructure due to some of their unique characteristics; two respondents did not believe there should be specific policies, as existing critical information infrastructure policies should cover the mobile infrastructure. These responses indicate that there is some concern over the protection of the mobile infrastructure, and that there are some unique aspects of the mobile infrastructure that should be addressed specifically.

The majority of interview respondents (eleven of twelve) considered mobile phones as important to both small and large businesses; six of these considered them very important. The remaining respondents for each were unsure. It was indicated that for smaller businesses mobile communications may be the only form of telecommunications available. Ten of twelve respondents considered mobile communications important to government and security and intelligence services, with one respondent unsure and one considering other communications methods more important. Ten of twelve respondents considered mobile communications important for the military, and two suggested that due to the dedicated military communications the mobile phones are unimportant. However, the release by Wikileaks suggested that there were concerns that insurgents were able to eavesdrop on mobile conversations of both Coalition diplomats and military in Afghanistan (presented in Section 5.5.1.6); this indicates that modern militaries with sophisticated satellite communications do make use of mobile devices in conflict zones. The reports of Israeli forces penetrating the mobile infrastructure in order to distribute psychological operations messages, presented in Section 5.5.1.6, show an application of IW to the mobile infrastructure. The interview respondents also indicated that additional security measures needed to be taken should government, security, intelligence, or military personnel use public mobile communications. It was also raised that due to possible insecurities, mobile communications may be important to these sectors due to their ability to gather intelligence on malicious actors. All twelve respondents indicated that mobile communications is important to criminal and terrorist actors; seven emphasised their response to very important. The suggested importance to these groups ranges from using mobile to detonate improvised explosive devices, or the fact that they may form "cheap and dispensable communications" (SA5). The use of mobile devices and social networking applications in popular uprisings indicate this technology may be critical for the demonstrators, but also for the authorities in preventing the demonstrations. These responses suggest that the mobile communications are important to all sectors; albeit for slightly different reasons. Therefore the mobile infrastructure can be considered as critical. The use of public mobile communications by the government and military,

especially in conflict zones, indicates that there is a definite relevance of the mobile infrastructure to IW. The hacking and distribution of psychological operations messages through the public mobile infrastructure confirms this.

The pilot survey of informal traders (presented in Section 6.4) indicated that there was a higher use of mobile communications than for business purposes. Whilst the survey is insufficient to draw any firm conclusions, there is an indication that the traders have mixed perceptions regarding the importance of mobile communications for their business. There will be an impact on their business should mobile communications be lost, however it appears to be more of a useful tool than a necessity. All the respondents had access to their own mobile phone, which again indicates the prevalence of mobile phones in South African society. The reports of the instability of the mobile networks (presented in Section 5.7) also indicated severe public frustration over the network outages (Ajam & Bailey, 2009; Mtshali, 2011); therefore there is a general perception that mobile devices are essential. It will therefore be more likely that immediate psychological and social impacts are experienced due to a major mobile network outage caused by a cyber-attack before the economic effects are felt. From the indications from the pilot survey and reports, the mobile infrastructure can be considered an integral part of society and is therefore part of the critical information infrastructure.

The overall indication is that mobile communications, and therefore the devices and infrastructure, are critical. In South Africa, there is a high prevalence of mobile communications compared to that of the equivalent fixed-line communications. Examples have been provided where public mobile networks are used for military and government communications, and military attacks on the infrastructure for psychological operations purposes. This indicates the relevance of the mobile infrastructure to IW. Therefore it can be concluded that the mobile infrastructure is part of the critical information infrastructure, and it is feasible that the vulnerability assessment treats it as such.

8.3 Threats

This section presents the potential IW threats to the mobile infrastructure. It was shown that the broader context is relevant and has an impact when considering IW; therefore the non-technical factors presented in Section 8.3.1 can be considered to be associated with the Context block of the IW Lifecycle model presented in Section 4.2. The technical threats comprise of those methods that may be used to attack or exploit weaknesses in the infrastructure, and form part of the context in

terms of the prevalence of the methods used; this is presented in Section 8.3.2. These technical threats can be related to the weapons block of the IW lifecycle model. Section 5.2.4 summarises the threats and provides the ratings.

8.3.1 Non-Technical Factors

From the examples discussed in Chapter 5, a wide range of threats can be seen; from disgruntled individuals, cyber-crime groups, insurgents, and foreign government organisations, including their militaries; these are a general threat as well as specific to the mobile infrastructure.

From the trend and incident analysis (Sections 5.4 to 5.7), cyber-attacks were seen from hacker groups, disgruntled employees, possibly nations, cyber-criminals, and the military intent to obtain cyber-weapons. Examples were provided from Zimbabwe where the government and their opposition were using cyber-attacks. The most prevalent was breaching confidentiality; however, there have been a number of large-scale DoS attacks since 2007. Attacks on the mobile infrastructure originate from cyber-crime, such as the SMS banking scandal; the military, from the reports of the Israeli penetration of the mobile infrastructure; insurgents, from the concerns that the mobile communications of the US forces in Afghanistan were compromised; a disgruntled employee who penetrated the mobile infrastructure; and possibly intelligence or other state-backed organisations, which may have been involved in the penetration of the Greek mobile infrastructure. Web 2.0 websites, in particular social networks, have also been targeted by cyber-crime. There is also the possible use by intelligence agencies, evident from the reported false-flag operations; the intention of the US military to obtain the Persona software also indicates military use for IW purposes. As many smart mobile devices have integrated Web 2.0 functionality, these threats are also relevant to the mobile devices. What is also apparent from the incident analysis is that many incidents are related in some way to controversial issues or decisions; therefore involvement in a conflict situation or controversial activity may result in the increase in the threats depending on who opposes the action.

From the interviews (Section 6.2), the broad themes for general threats and vulnerabilities include: lack of user awareness and complacency; cyber-crime, hacking and fraud; surveillance; general vulnerabilities; cyber-war and cyber-terrorism; denial of service; illegitimate control; and the image of corruption in South Africa. Cyber-crime, cyber-terrorism, cyber-war attacks were listed as the threat actors, where the focus was on cyber-crime and related issues. There was a strong weighting of the responses towards the lack of awareness, which can be considered as a vulnerability, and

threats that breach confidentiality. The image of corruption is South Africa was an interesting point, in that this perception may result in higher threat activity due to the idea that they are more likely to escape prosecution in South Africa. The broad themes for the mobile threats and vulnerabilities include: general vulnerabilities; espionage and surveillance; reliance; cyber-crime and information theft; malware; lack of user awareness; phishing; SIM cloning; lack of data verification; and cyber-attacks or terrorist-attacks. The threat actors are again listed as cyber-criminals and general cyber-attackers. The responses were weighted strongly towards threats that breach confidentiality.

The workshop discussion (Section 6.3) also indicated that cyber-crime syndicates are a common threat; the discussion largely revolved around cyber-crime and the protection of personally identifiable information; this again indicates a concern over confidentiality. The insider threats were specifically mentioned; in particular employees that are about to leave the organisation, or former employees that have recently left were indicated as the most common. The threat from competitors in terms of corporate espionage was also raised; and it was indicated that this does occur in South Africa. From the mobile related discussion, the devices themselves can be considered as part of a threat to information infrastructure in that they can be used to circumvent the network perimeter controls. Cyber-crime was also mentioned in that there are reports of the legislative controls related to mobile communications being subverted. Web 2.0 can also be seen as a threat in that it facilitates the possibility of information leaks and propagates malicious code. It was indicated that it appears South Africa is being used as a launching point for attacks, and that it is feasible that Africa may have large botnet infections allowing it to be used as a cyber-weapon.

The financial impact of intellectual property theft and espionage outweighs the financial losses due to cyber-crime against individuals. In the Wikileaks incident discussed in Section 4.2.7.4, it was stated the lawyers conducting a case against China for stealing software. This indicates that state-sponsored corporate or industrial espionage is also an economic threat.

Due to the importance of mobile communications to insurgents, general criminal groups, and terrorists, it is unlikely that they will intentionally attempt to disrupt mobile services unless in unique circumstances. Denying mobile communications in conjunction with a physical attack may further hinder emergency services and rescue efforts, and aid in spreading frustration and fear due to the unavailability of communications to check on the health of friends and family. Miller (2005) raises this possibility, and Muir (2005) reports that the mobile phone networks were overloaded after the July 7 London attacks in 2005.

The African-specific trends presented in Section 5.7 provide a political context: there are concerns regarding the political alignment of South Africa; both China and India are taking an economic interest in Africa, and South Africa has been put in a situation where a political decision (whether to allow the Dalai Lama entry into the country or not) will upset one group or another. As China has been blamed for a number of cyber-based attacks, it is possible (assuming the reports are correct) that political actions which oppose Chinese goals may result in such attacks directed at South Africa. A converse opinion is that supporting Chinese wishes may attract attacks from the opposition. The internal political tensions in Zimbabwe exhibited some low-key cyber-attacks; should this expand, South Africa may be affected by some cyber-attacks. The political unrest across Africa in 2011 may also result in a higher threat environment, as this indicates more active potential aggressors. As mobile devices and social networking played a role in this unrest, it is possible that other cyber-attack methods may be used to further the goals of political groups. South Africa has experienced riots regarding the lack of service delivery, and xenophobic attacks; these may be incited through use of mobile communications, or possible instigate an external attack on the nation.

It can be seen that cyber-crime is extremely prevalent; therefore the threat likelihood of cyber-crime is very high. Cyber-crime is also related to cyber-war, as the botnets that are operated by the cyber-crime organisations can be used by groups or nations to perpetrate cyber-attacks. Due to the incidents and factors summarised in this section, it can be seen that politically motivated groups or activists perpetrate a number of acts; therefore the threat from these groups is high. Incidents attributed to nation-state organisations, such as the intelligence agencies or military, are also apparent. The nations may have more resources to assign to developing cyber-attacks; if not, they can use the cyber-crime infrastructure that is for hire. Therefore their capability is greater than or equivalent to the cyber-crime capability, however the likelihood may not be as high, therefore the threat can be considered as medium. The threat of insider access also needs to be accounted for as they have greater access than the external actors; from the workshop and some incidents, it can be seen this is a prevalent threat, and can therefore be rated as high.

8.3.2 Technical Factors

Of the technical threats, malware is one of the most prevalent. The CSIRT data presented in Section 5.4.2 illustrates that the most prevalent incident reported is related to malware or some form of malicious code. There is a shift from the initial virus and worm propagation that result in widespread disruption of network services to cyber-crime based malware. These are usually in the form of a botnet, which has the ability to steal information, send spam, or conduct DoS attacks.

From the workshop it was indicated that the concept of an African botnet is plausible. The documents released indicating the US military were reportedly involved in developing a rootkit codenamed Magenta indicates there is intended military used of malware; as rootkits can remain undetected, this is a serious threat. In addition, the Stuxnet incident indicates that malware can be used to target and affect control systems; when Conficker infected military systems it again illustrated that malware is a threat to military equipment and operations. Malware has also been targeting mobile devices, and this is a rapidly growing threat; Section 5.5.2 presented this in detail. There are emerging trends which suggest mobile malware is also shifting towards cyber-crime, and PC-based malware has been seen to migrate to mobile platforms in order to attack mobile banking applications. Web 2.0 technologies have also been seen as a vector to propagate malware; this may be used in future to propagate mobile malware. Malicious code was used in many espionage attacks based on the Advanced Persistent Threat.

A high proportion of the incidents discussed in Section 5.4 constitute system penetrations to steal information; some of these appear to be acts of state-sponsored espionage. The initial attacks were facilitated through hacking and the later attacks were facilitated through a combination of social engineering and the advanced persistent threat, which behaved like a botnet. This indicates a level of corporate, economic, industrial, and political espionage. Examples were provided of attempted false-flag operations conducted via social networking websites. The workshop confirmed the existence of corporate espionage in South Africa; and the high success rates achieved by social engineering indicate that this is a relevant threat in South Africa. System intrusions and intrusion attempts were listed as the third most prevalent threat by ranking of the CSIRT data (presented in Section 5.4.2); scanning is the fourth most prevalent, which indicates some intent to attempt to target those systems. Hacking was mentioned in the interviews; the concern was the impact on infrastructure services, however this could also be used to access or maliciously alter information. The possibility of espionage through mobile communications due to penetration of the infrastructure or by intercepting the wireless channel is apparent. The penetration of the Greek mobile infrastructure afforded the attackers the ability to monitor high-level individuals; in addition, Wikileaks documents indicated there was a similar concern that insurgents could gain access to the Afghan mobile infrastructure to monitor calls by US forces and diplomats. The research considered indicates that it is possible to intercept and break the encryption of the mobile wireless channel; this was also raised in the interviews. The interception will be discussed in more detail later, as it is relevant to electronic warfare.

Since 2007 there have been a series of large-scale DoS attacks due to botnets; three have targeted national infrastructure, and a series of smaller ones have targeted specific organisations and government websites. The threat of DoS attacks was also raised by an interview respondent; however the indications from the workshop is that South Africa only experiences low-level DoS attacks against specific websites. Given the through-put and capacity of the undersea cables in South Africa, a large-scale DoS equivalent in magnitude to the one that targeted Myanmar in 2010 will result in severe degradation of services in South Africa should the country be targeted; this was presented in more detail in Section 5.7. The CSIRT data also shows some reported DoS attacks in the nations; however this is not a very prevalent threat; and is the sixth ranked threat. There is also the possibility of mobile-based DDoS attacks on the mobile infrastructure; this was raised by a report and in the workshop. Academic research also explores the possibility that exploiting legitimate SMS services and flooding the mobile networks may also result in denial of SMS and voice services. The calculations and simulations in Sections 7.3 and 7.4 further indicate that a DoS attack against the South African mobile infrastructure is feasible; the specific impacts of these will be discussed in Section 8.4.2. Reports also indicate that mobile botnets can be used to flood local towers and infrastructure with messages or requests; due to the prevalence of mobile malware and reports of SMS flooders this is likely to be more prevalent than exploiting the web-based SMS services. It is also possible to deny the services on the devices; an example was provided where a malformed SMS could crash the communications of mobile phones. It may therefore be theoretically be possible to craft an SMS that could crash infrastructure components. This type of attack was discovered through research by security experts, and no reports of this method being used in an actual attack were found.

What should be considered is that if there is a high infection rate of bots in South Africa, then a DoS attack could conceivably come from the systems within the national boundaries. This will be more severe as an attack originating externally could be mitigated by blocking the national gateways, leaving the networks internal to the country unaffected; however, an attack originating from internal systems will be very difficult to protect against.

Section 8.3.1 listed out the broad themes for threats and vulnerabilities that arose from the interviews. The ones that are relevant to technical threats are: hacking and fraud; surveillance; general vulnerabilities; denial of service; and illegitimate control. The relevant broad themes related to the mobile infrastructure are: general vulnerabilities; espionage and surveillance; reliance; cyber-crime and information theft; malware; phishing; SIM cloning; and lack of data verification. The

focus of the threat and vulnerability category was of breaches of confidentiality; however aspects related to denial of service are also raised. What is interesting is that malware was mentioned for mobile devices, yet not for general threats. SIM cloning was raised; this is unique to mobile infrastructure and has been used effectively in a cyber-crime incident in South Africa to intercept the communications between the online banking and the target. Calls could also be made which would be charged to the target's account.

In addition to the malware, intrusion, and DoS threats already mentioned, fraud and website attacks are the second and fifth most prevalent incidents reported to the national CSIRTs. Fraud was also raised in the workshop and interviews. It was indicated in the workshop that many cases of fraud in South Africa are traced back to associated of employees in the victim organisation. The SIM card cloning and the SMS banking scandal incident can both be considered as forms of fraud. These incidents raise concerns over the actual origin of the information; thereby affecting integrity. This concern was also raised in the interviews in relation to threats and vulnerabilities of the mobile devices and infrastructure. Examples include the distribution of SMSes in Kenya advocating violence, the penetration of the mobile infrastructure to distribute psychological messages, and a disgruntled employee sending messages supposedly from an organisation.

Section 5.5.1.4 presents research suggesting that the encryption used in the GSM wireless channels is susceptible to being broken; the research shows how it is possible to eavesdrop on mobile calls. However, there are some technical difficulties with implementing this indicates that it is probable that only organised groups with high intent and capability will attempt this; provided they have a high return on investment. Section 7.5 provides range calculations for electronic warfare jamming and communications intercepts; Section 7.6 simulates the accuracy required to estimate the spreading sequence in order to intercept CDMA communications signals. These indicate that electronic warfare solution to deny or intercept communications are not as efficient due to range limitations, required manpower, and equipment capabilities unless there are already military assets in the area with this capability. Lawful intercept or network warfare methods may be more efficient as they can be done remotely and access more information, or deny services, with limited available human capability. The required capability may initially be higher; however the overall process may be more efficient. This indicates that there will be a higher threat from network warfare attacks than electronic warfare attacks, unless there are operational military electronic warfare assets in the area, such as in a conflict zone.

As discussed in Section 8.3.1, the workshop participants considered both the mobile devices and Web 2.0 technologies as a technical threat in themselves. Mobile devices may be used to subvert network perimeter defences and Web 2.0 technologies may be a vector for attacks and information leaks. They may also be used as a platform for distributing hate speech and psychological operations messages, as discussed above. Mobile devices, combined with social networking applications, have been instrumental in a number of popular anti-government uprisings. The mobile devices may also be compromised through attacks on vulnerabilities in the Bluetooth and WLAN implementation; however these need to be done at a relatively close range to the target. Targeted attacks were raised in the workshop, where high-level individuals are targeted and their laptops are stolen; this may also extend to mobile phones. Phishing was raised in both the interviews and workshop; these attacks have now migrated to mobile phones and are seen in South Africa. The use of voice-over-IP (VOIP) services from mobile devices on open networks may result in interception of the communications.

Due to the antennas on both the towers and mobile devices, there is a level of electromagnetic exposure of the infrastructure and devices. This makes them susceptible to electromagnetic pulses and directed energy devices. It was indicated in reports presented in Section 5.5.1.6 that the mobile infrastructure is more susceptible to these attacks than the fixed-line infrastructure. However, the proliferation of these devices is low and requires a high technical capability. Homemade devices may only have limited power, therefore their effects may be minor, and they would possibly only interfere with a single tower at a time, resulting in multiple attacks on the towers. Protection against lightning and shielding may also be sufficient to mitigate attacks by the low-powered devices.

Aspects not discussed in previous chapters include physical threats. As cable theft in South Africa (Vermeulen, 2011) and Trinidad and Tobago (Cellular-news.com, 2007) have affected mobile services, it should therefore be included here for completeness. Physical attack against information infrastructure components is a valid IW tactic as this will effectively deny services. The most vulnerable points in mobile communications are the mobile devices (targeted theft is discussed previously) and the base station towers. Whilst base stations may be protected by fencing, the base station may be damaged or destroyed by thrown explosive devices and the antenna may be damaged by gunfire. Such an attack may only damage a single tower; therefore a concerted effort to damage multiple towers would be required to disrupt services over a larger geographical area. This method would therefore be prohibitive to the majority of groups. In a conflict zone, there may be the threat

of artillery or air strikes, which could target and destroy more crucial components, such as the switching stations.

The majority of information collected in the workshop, interviews, and incident analysis indicates that threats which breach confidentiality are the most common. Those that result in denial of services or corrupt integrity occurred in similar quantities in interviews; however from the incidents DoS attacks against the information infrastructure are more prevalent in terms of large-scale attacks. Fraud, which affects information integrity, is far more prevalent at an everyday organisational level than denial of service-attacks; however this is more related to cyber-crime than IW attacks. Widespread use of mobile communications affords more opportunities for intercepting information. Web 2.0 technologies may be used to facilitate information leaks; this is also relevant to mobile devices as many smart phones have integrated social networking applications.

8.3.2.1 Rating the Technical Factors for Threats

Assuming an IW attack is a given, the likelihood of the attack vectors or methods should be rated; this will be used to weight the threat ratings. As malware is prevalent, especially in South Africa, it can be rated as having a very high likelihood of being used in an attack as it has been leveraged for both espionage and infrastructure attacks. The malware is used to create botnets, which support cyber-crime and can be used to conduct DoS attacks. Mobile malware is growing in prevalence, and examples have been provided where information can be stolen or possible DDoS attacks on the towers from the mobile devices can be conducted. As mobile malware needs to be generated for various mobile platforms, and requires certain functionality, this threat is not as prevalent as PC-based malware, and can be rated as a medium likelihood. Malware distributed by social media has been seen; whilst this has not targeted mobile devices, it may affect systems connected to the mobile infrastructure. In future it may be possible to infect mobile devices through Web 2.0 technologies, therefore the likelihood of this attack can be considered medium. The use of malformed SMSes or images to crash mobile device or take control of enterprise servers has been identified by research; however no information was found that suggests this has been successfully implemented as an attack; the likelihood can therefore be considered as low. DoS attacks on the mobile infrastructure may be conducted via external SMS entities by flooding the networks with illegitimate SMS messages or requests; this has only been proposed in academic research, and no information on real-world attacks using this method was found. This method is feasible, and allows for a controlled DoS attack against a specific mobile infrastructure; therefore the likelihood can be considered medium.

Penetrating infrastructure appears to occur regularly; and a number of incidents indicate that the mobile infrastructure could also be penetrated to either eavesdrop or leave one's own messages. There are also reports of regular attack attempts against the South African telecommunications networks. In terms of an IW attack, this has a high likelihood. Penetrating the infrastructure may be aided by insiders; this is a prevalent threat in South Africa and has already once been illustrated how the legitimate functioning of mobile communications services were exploited. Therefore the insider threat can be rated as having a high likelihood of occurrence. The subversion of the South African mobile provider was by cloning SIM cards. This may allow illegal calls to me made which are more difficult to trace, and may allow the interception of some mobile communications; in terms of IW, this is more likely to be used by non-state actors rather than national agencies and can therefore be rated as high and low, respectively.

Due to complexities in intercepting the wireless channel, this is unlikely to be conducted during peacetime; in a conflict zone there may be electronic warfare equipment available which will allow for this. However, using intercept facilities in the infrastructure will be more efficient. The likelihood is therefore very low for peace-time conditions, and medium for conflict zones. Jamming the wireless channel is less complex and therefore may be conducted more frequently. In conflict zones one can assume a high prevalence of jamming due to the threat of IEDs detonated by mobile communications and insurgents using them for communications; in peacetime the prevalence will be low. The likelihood of EMP or directed energy devices being employed is very low due to low proliferation of such devices. The likelihood of physical threats during peace-time are low as network warfare-style attacks will be more efficient, however they are still possible; during conflict physical attacks are more likely due to the military assets, and can be rated as medium.

The use of mobile devices also presents threats. Targeted attacks where devices are stolen have a high prevalence in South Africa; targeted attacks may also attempt to exploit vulnerabilities in the WLAN and Bluetooth capabilities of devices, however these are less likely due to the technical capability required and the man-power required to gather the information; therefore these can be rated as low. Mobile communications forms a delivery method for phishing and psychological operations attacks; these are increasing and examples were provided of the use for PSYOPs. Combined with social media, mobile communications have also been used to incite mass demonstrations and delivered hate speech inciting violence. These threats are growing in prevalence, and can therefore be rated as having medium likelihood. Mobile devices can also be used to bypass the perimeter controls of networks, an example of this was provided in the

workshop. Accidental breaches (a user connecting a mobile device in the network and allowing wireless access) cannot be relied upon for IW, and therefore the threat likelihood is low. Intentionally introducing the device to access the networks may result in the eventual loss of the device, however the benefit to the attacker may be worth the loss; this can be rated as a medium likelihood. Information leaks may also occur through mobile devices due to social media applications, the mass storage on the devices, and the use of VOIP services on unsecured networks. The threat of leaks can be considered as having a high likelihood as attackers may copy information onto the devices, which provide an excellent transportation mechanism. This can be rated as a high likelihood as insiders will have access to copy the information. It is also possible to intercept VOIP communications, but this will be somewhat opportunistic unless the network is permanently monitored. In an IW environment, especially where cyber-espionage is prevalent, VOIP interception may exhibit a high likelihood of occurrence.

8.3.3 Threat Summary

Section 8.3.1 discussed the threat context and non-technical factors. For the South African situation, it can be assumed that IW threats will originate from a rogue or vigilante group, or a nation state. These threats can be seen to have the capability or will to implement attacks, or employ the capability of cyber-criminal groups for these attacks. The likelihood of an attack on South Africa is low; however, due to the current political unrest in Africa (Jacobs & Duarte, 2010; Malakata, 2011; Sky News, 2011), this could be elevated to medium if the situations are not dealt with sufficiently at a political level. Table 8.1 provides the matrix to calculate the threat rankings. As the likelihood of threat action is medium, this row is presented with white text on a black background; this row provides the threat rating according to the threat capability.

Table 8.1: Matrix for Threats

Likelihood of Action	**Threat Capability / Prevalence**				
	V. Low	*Low*	*Med*	*High*	*V. High*
V. Low	V. Low	V. Low	Low	Low	Med
Low	V. Low	Low	Low	Med	High
Med	**Low**	**Low**	**Med**	**High**	**High**
High	Low	Med	High	High	V. High
V. High	Med	High	High	V. High	V. High

The prevalence of the individual attack methods provides an indication of the preferred weapon or capability of a potential attacker; for example, a high prevalence in system penetration indicates a

high capability in that area. Table 8.2 provides a list of the threats discussed in Section 8.3.2 and their threat rankings, calculated from the prevalence and likelihood of threat action. Four general threat ratings are provided, prior to rating the specific threats to the mobile infrastructure, and threats due to mobile use. The medium rating of the likelihood of threat action moderates the prevalence of the threat types; therefore the overall ratings range from low to high. For example, whilst there may be a very high threat from malware, the threat of it from an IW application is high. These threat ratings will be associated with vulnerabilities to create potential impacts; this is discussed in Section 8.4.

8.4 Vulnerabilities and Impact

The vulnerabilities, and the potential impact of them being exploited by threats, are derived from the incident and trend analysis (Chapter 4 and Chapter 5), the interviews (Section 6.2), the workshop (Section 6.3), and the simulations and calculations (Chapter 7). Section 8.4.1 discusses the non-technical factors, and the technical factors are covered in Section 8.4.2. Section 8.4.3 summarises the vulnerabilities and provide the vulnerability ratings. In this section, the worst-case scenario for a defender will be considered for the impacts and vulnerabilities. The impact types are breach of confidentiality, corruption (breach of integrity), and denial of services; these were identified in Section 2.3.2.1 and incorporated in the proposed IW Lifecycle Model in Section 4.2.6. For non-technical factors, impacts can be considered as general as they affect a broad range of social, economic, and political areas.

8.4.1 Non-Technical Factors

The political position of South Africa may result in attacks targeted towards the country. Views that South Africa may be targeted due to the apparent political alignment with China or the potential to upset Chinese patriots who have aggressive cyber-tendencies. Any controversial political decisions on an international scale, or the involvement in conflicts, may also attract attention from potential cyber-aggressors. Chapter 5 showed that political context often played a major role in instigation of attacks. Therefore the political context in Africa, which has seen widespread instability and mass anti-government demonstrations across the continent, may spark attacks. Issues of perceived poor service delivery in South Africa may also result in a socio-political environment similar to those in Tunisia and Egypt where there are widespread demonstrations which could eventually be targeted at the national government.

Table 8.2: Summary of Threats

Threat		Threat Prevalence	Overall Threat Rating
General Threats			
Malware		Very High	High
Social engineering		High	High
DoS		Medium	Medium
System penetration		High	High
Threats to the mobile infrastructure			
Jamming	conflict zone	High	High
	peace-time	Low	Low
Wireless intercept	conflict zone	Medium	Medium
	peace-time	Very low	Low
Infrastructure penetration		High	High
Malware		Very high	High
Mobile and social media malware		Medium	Medium
Malformed or malicious messages		Low	Low
SMS flooding from web-based services		Low	Low
SMS flooding from mobile botnet		Medium	Medium
SIM cloning	non-state actors	High	High
	state actors	Low	Low
Insider threats		High	High
Physical threats	conflict zone	Medium	Medium
	peace-time	Low	Low
Directed energy and EMP		Very low	Low
Threats presented by the use of mobile devices and infrastructure			
Phishing		Medium	Medium
PSYOPs and hate speech		Medium	Medium
Uprisings		Medium	Medium
Penetration tool	accidental	Low	Low
	intentional	Medium	Medium
Bluejacking		Low	Low
WLAN attacks		Low	Low
Targeted attacks stealing phone		High	High
Leaks through social media		High	High
Leaks due to mass storage		High	High
Careless use of VOIP on open networks		High	High

The economic interest in Africa by Asian countries may also result in Africa being the object of strong economic and information competition. Aligning politically and becoming involved in international cyber-security efforts will provide South Africa with international political backing to aid in mitigating attacks; the draft cyber-security policy does make provision for the international involvement of South Africa in cyber-security groups; this will provide some assistance in the event of an attack. The control can be rated as medium. The capability required to exploit political vulnerabilities is very low; as can be seen from the Estonian cyber-attacks, seemingly insignificant decisions at a global level may be used as an excuse to attack. There are a number of possible impacts: mass uprisings, economic impacts due to DoS attacks, or loss of international support and investment in a nation. The impact will be rated as high, due to the impacts on Estonia and the uprisings in North Africa.

An aspect that came across strongly in the South African trends due to the number of researchers focussing on this is the lack or end-user awareness regarding security issues in South Africa; this was also raised in the interview and workshop. This creates a general vulnerability in that users are susceptible to scams and malicious links that may result in additional infected systems (possibly creating more bots). The lack of awareness may also indicate that basic security measures, such as updating anti-virus programs, are not done on a regular basis. The high infection rate presented in Section 5.7 indicates that this is definitely the case; and due to the increasing accessibility of broadband and smart mobile devices, this vulnerability will increase. This may result in an economic impact, due to the personal and corporate information that is compromised. There may also be legal and political implications: should a large number of compromised systems participate in a DoS attack it would initially appear that it originated from the country, resulting in political and legal problems. The only possible control mechanism is awareness campaigns; these are not widely implemented in South Africa, therefore the control mechanism can be rated as low. The required capability to overcome the lack of user awareness is minimal and can be rated as very low. The exact impact is difficult to determine, however due to the prevalence of malware in South Africa, it can be rated as medium, escalating to high should there be a rapid increase Internet access.

In addition to user awareness, the incorrect attitude of organisations was raised in both the workshop, and interviews. It was pointed out that some organisations are apathetic and only do the minimum to ensure compliance, whilst smaller businesses may have the perception that information security only applies to the larger organisations. These attitudes indicate that the implemented policies and technical information security controls could be insufficient to protect against cyber-

crime or IW. This will allow for system penetrations and theft of information (in terms of both cyber-crime and espionage), a degree of malware infection, and potential exposure of personal information. This also provides more scope for insider threats. The primary control would be to pass legislation to force organisations into improving their information security; however this takes time to be fully implemented, therefore the control rating can only be considered as medium. The required capability to overcome these vulnerabilities is low. The financial impact in the UK and US due to espionage was significant, and the existence of corporate espionage in South Africa was confirmed in the workshop. This will also create a negative impression from international investors should there be large information security problems. Therefore this impact can be rated as high.

Ineffective policies allow for accidental and intentional breaches from insiders; this may be a result of poor corporate attitude, a lack of capability and understanding, or by accident. The banking SMS scandal illustrated the relevance of the insider threat to the mobile infrastructure. No technical capability is required to overcome this vulnerability; the targeted may be bribed, threatened, or willing due to dissatisfaction. Therefore the required capability rating can be considered low. Contracting experts to assist with generating and testing these policies will aid in significantly reducing the insider threat. One such concept is segregation of duties, which was raised in the workshop; this ensures that no one person has all the access to contribute to a full breach. This control can be rated as medium, as it was also indicates that multiple people are bribed by syndicates to effect the breach.

There is legislation in South Africa related to information security, and some specifically relevant to the mobile infrastructure. Whilst it is stronger than most of Africa, it has not been tested in court, and in some cases is not fully implemented. Examples were given in the workshop (Section 6.3) that RICA is being circumvented, and concerns were raised regarding its ultimate effectiveness. The image of corruption in South Africa, as raised in the interviews, may also contribute to this vulnerability as there appears to be an opportunity for conducting malicious activity in the country. This legislature will probably not be applicable to many countries; therefore if an attacker is international, it will be difficult to prosecute them. There is no effective control, other than political will or public pressure, which does not seem to be prioritised; a draft national information security policy has been released and there is the Protection of Personal Information Bill which is yet to be enacted. It can be seen that some effort is being made; therefore the control can be rated as medium. As RICA already appears to have been circumvented, the required capability to overcome legislative controls can be rated as low. The overall impact of circumventing national legislature

can be classed as low for an IW environment; this applies mostly to criminal groups being able to communicate.

The lack of CSIRTs in Africa was a general problem; due to the political unrest in Tunisia and Egypt, the operations or implementation of two CSIRTs may be hindered. In particular, the lack of a fully operational national CSIRT in South Africa means the nation does not have a central response point to handle incidents, and there is no consolidated information or broad picture of the information security incidents in the country. Compared to other nations with operational CSIRTs, South Africa will be vulnerable to an IW attack as the fragmented information may hinder the detection and response to the attack. As with the legislature, the control is political will and pressure; there are attempts at introducing a CSIRT in South Africa, and the draft national cyber-security policy makes provision for a national and sector CSIRTs. The control can therefore be rated as medium. The required capability to exploit this vulnerability will again low. The impact of this will be medium; a CSIRT will aid in detection of attacks, identify related incidents, and provide incident response. However, this will not necessarily prevent the attacks from occurring in the first place. The CSIRT is a detective and reactive measure, which aids in mitigating the effects and attacks.

Lack of user awareness can be considered the vulnerability that is the most prevalent concern; this appears in both general vulnerabilities and mobile vulnerabilities. The lack of a national CSIRT and legislative issues is also a common concern.

8.4.2 Technical Factors

This section will discuss the technical vulnerabilities of the mobile infrastructure. Prior to this, it is worth assessing the national vulnerability and risk due to the common attack methods exhibited in the trend analysis. Of the significant attacks, system penetration for espionage and DoS attacks are prevalent. Some of the major espionage attacks relied on social engineering and malware; from the gathered data malware and lack of user awareness the two primary concerns in South Africa. This indicates that in general the controls against such an attack in South Africa are low. The required capability can be classed as medium; as the malware and targeted phishing requires more planning and effort than would be expected an opportunistic cyber-criminal group to perform. The impact of such an attack can be rated as high; the trends indicate that the information targeted is not necessarily classified, however it can still be sensitive, especially in the quantities stolen. In many cases, these attacks have been attributed to nation states, and some to vigilante groups.

Very low capability is required to conduct DoS attacks; groups have the option of hiring a botnet. Controls include sinkholes and black holes (presented in Section 2.4.2); these methods appear to be effective at redirecting traffic targeted at specific websites or customers within an ISP. These methods may not be as effective at relieving overloaded international gateways. In the workshop it was indicated that the service providers do not have the capacity to handle DoS attacks; therefore there may not be proper implementation of these countermeasures. The high botnet infection rates in South Africa compared to the global average indicates a susceptibility to these attacks, as the ICT systems within the national boundaries could be used to attack itself. The controls can therefore be rated as low. The impact of the large-scale DoS attacks on Estonia and Georgia can seen to be significant; disrupted communications and financial losses in the order of millions of dollars were seen. The impact can therefore be rated as high. The threat associated with this type of attack appears to be attributed more to rogue groups than nation states, even though Russia as a nation was accused of supporting or conducting the attacks against Estonia and Georgia.

8.4.2.1 Denial of Service and System Breaches

A potential vulnerability of South African mobile infrastructures is the apparent high load that they operate at. A report indicated that network outages have been due to over-subscription (Ajam & Bailey, 2009). Network outages in 2011 also suggest that there may be operating conditions that affect network stability; the report that the networks do not meet the requirements for call processing also indicates high loading. These conditions result in the mobile infrastructure being susceptible to DoS attacks. All that is required is additional requests or SMS messages that flood the network. This can be achieved through the use of malware or exploiting legitimate SMS services. The required traffic to deny services through SMS and malware is discussed in Sections 7.3 and 7.4. From this it can be seen that it is feasible, and the capability exists to conduct such attacks; however the required capability may be more than a conventional computer network-based DoS attack due to the mobile systems or the requirement to exploit the SMS services. The rating for the required capability will therefore be low. Section 2.7.2.1 lists an indirect control for high capacity as a threat warning system; as there is not an operational CSIRT in South Africa, this control can be rated as very low. The resulting impact will be prolonged widespread outages of services; there will also public frustration shown during minor outages and the financial loss to the relevant network providers. There will also be general national network performance degradation should the attack come from web-based SMS entities, due to the traffic following to the websites; the impact from this can be rated as high. The simulations in Section 7.4 showed the potential

effects of a mobile worm on the infrastructure components; this attack will be limited to the mobile infrastructure, and the effects will not be immediately felt; therefore the impact can be rated as medium.

Centralised mobile infrastructure components are also susceptible to DoS attacks, as increased traffic across wide geographical areas may bottle-neck at these components. Examples include the billing infrastructure, home location registers (HLRs), and mobile switching centres (MSCs). These can also be seen as regional singularities. The graph theory analysis presented in Section 7.2 indicates that there are various levels of centralisation according to the geographical area and population centres. The same attacks described for the loading conditions apply for centralisation in terms of DoS attacks by flooding with illegitimate traffic. The required capability will be the same type as above; however additional resources will be required due to the increase in traffic flow. Therefore the required capability will be rated as medium. The controls listed in Section 2.7.2.1 for centralisation and singularities include redundancy, static and dynamic resource allocation, rapid recovery, deception, decentralisation, and self-organisation and collective behaviour. The simulations took a degree of redundancy into account; it terms of DoS attacks, redundancy will just provide the network with extra capacity, and will only slow down a determined attack. As the general structure of the mobile infrastructure is freely available, deception is not possible. The base stations are effectively self-organising and perform dynamic resource allocation in that the users are allocated to the nearest free cell or base station; this will aid in mitigating an overload in specific cells, however the core network may still come under stress. Quick response to an attack will be key; recovery may not be as quick as the mobile devices and external SMS entities are outside the control of the service provider, and this is where the recovery need to take place. The overall rating for the controls can therefore be considered as medium. The impact can be rated the same as for the high operating loads above.

General vulnerabilities may be exploited in order to penetrate the system or infrastructure. These vulnerabilities may come in the form of misconfiguration, unpatched systems, or outdated signatures for anti-virus and other security application. The high levels of software piracy in South Africa indicate that there may be a high prevalence of general threats due to unpatched and vulnerable systems. Many vulnerabilities are widely known, and freely available hacking tools or malware kits exploit these. Therefore the required capability to overcome general vulnerabilities is low. The majority of vulnerabilities can be prevented by ensuring the systems are patched and anti-virus applications have the most recent signature files; these controls can be rated as high, as they

are effective against known vulnerabilities exploited by hacking tools and malware, and can also detect known attacks. Previously unknown vulnerabilities also allow attackers to penetrate systems and are susceptible to malware. The Stuxnet worm exploited multiple known and unknown vulnerabilities. The required capability to overcome these will be rated as high, as the vulnerabilities and relevant exploits need to be researched. As these vulnerabilities are previously unknown, the controls mechanisms for these are non-existent; some control devices, such as anti-virus, firewall, and IDS may be able to identify an attack through unusual activity or code. In many infrastructures, air-gaps are used, where the infrastructure components are physically and electronically separate from the Internet and corporate networks. However, the Stuxnet worm illustrated that air-gaps can be easily circumvented through removable mass storage. The control effectiveness against unknown vulnerabilities can therefore be rated as low. Various impacts are possible through exploiting general vulnerabilities. System penetration may be able to breach confidentiality; this can be rated high due to sensitive information being breached (as in the Athens Affair incident), or the use of personal information by cyber-criminals. System penetration could also affect the integrity of stored information in addition to breaching confidentiality; the recovery from this will be more complex, and can therefore be rated as very high. Penetrations may also allow attackers to deny services; there is potential for wide-spread outages, which will also result in direct financial loss to the relevant organisations. The impact of a DoS attack can therefore be considered high. Malware can also breach confidentiality and system integrity ultimately denying services, as the Stuxnet worm did. The rating for confidentiality breach will be the same as above. Affecting system integrity and denying service can be rated as very high as physical damage may be done to the systems which require replacing.

8.4.2.2 Electro-Magnetic Exposure and Electronic Warfare

Due to the very nature of mobile communications, there is electromagnetic exposure. This indicates that directed energy or EMPs could damage or destroy infrastructure components. The reports indicate that the mobile telecommunications components are more susceptible to this type of attack than fixed-line telecommunications. The required capability to overcome this in terms of widespread infrastructure damage is very high due to the technical requirements. Grounding provides is standard in the telecommunications sector; however this provides little protection. Shielding does provide more protection, however this is not usually done for civilian infrastructure. The controls can therefore be rated as low. The impact of directed energy will be low; towers will need to be attacked individually and they may only be temporarily damaged. The impact of a large

EMP will be worse, and this may result in widespread outages due to destroyed components (including power supplies), and can be rated as high.

The wireless channels may be targeted through electronic warfare attacks. Jamming intends to introduce interference and make the received signal unrecoverable. Devices and equipment is available to jam both GSM and 3G systems; however 3G systems are more resilient to jamming. Section 7.6 presented the accuracy required to target a specific 3G signal without interfering with the other signals; this also maximises the jammer effectiveness. Military technology is also readily available to jam mobile communications, especially due to the threat of IEDs. Even though these devices are available, they are usually only sold to government and military buyers; however it may be possible to produce home-made jamming devices. The required capability to jam mobile communications can therefore be rated as low for GSM and medium for 3G. The controls are built into the communication channel design; this takes the form of power control and the natural anti-jam properties of 3G spread spectrum signals. These can be overcome by increasing the jamming output, or moving the jammer closer to the tower or device. The controls can therefore be rated as low for GSM, and medium for 3G. Homemade and some commercial devices will have a low impact; only a localised area will be affected and multiple devices will be required (as illustrated in Section 7.5). Military jamming equipment have larger ranges as calculated in Section 7.5; the impact from these can be considered medium due to the increased range and efficiency of these devices. Due to these limited ranges, the option of a network warfare attack may be more efficient.

Bluetooth and WLAN communications can also be jammed; this can be considered as part of the mobile infrastructure as they are communication methods which allow for mobility. Due to the power output, close proximity, and antenna height compared to that of the mobile towers (as presented in Section 7.5), jammers may be less effective against these technologies due to the shorter range that the jammer is effective. This indicates a higher required capability, as not only does the attacker need to possess the equipment, but must be able to locate the desired target with greater accuracy. Therefore the required capability can be rated as medium. Whilst these technologies utilise CDMA similar to the 3G channels, the controls against jamming for Bluetooth and WLAN are less effective than that of the 3G mobile due to the lower power output and shorter ranges, and can therefore be rated as low. The impact of such an attack will be very low due to the very localised area of the jamming, unless an organisation is solely reliant on the wireless connections.

Wireless channels are also susceptible to interception. Section 7.5.2 presents the maximum detection ranges for mobile communications. Section 5.5.1.4 presented a method that researches claim will enable eavesdroppers to intercept and break the encryption on GSM calls. 3G communications are more difficult to intercept and detect due to the spread spectrum nature. Section 7.6 illustrates the accuracy required to use correlation with estimated sequences to improve intercept performance. From this, the required capability to intercept GSM communications is medium; for 3G this can be rated as high. Weaknesses in the GSM controls (the encryption) have been illustrated; however this still provides some protection, and can be rated as medium. Due to the spread spectrum nature and improved encryption algorithm for 3G, the controls can be rated as high. The impact of general eavesdropping on individuals will be low; however in a conflict zone, the interception of sensitive information from diplomatic or military personnel can have a high impact.

Bluetooth and WLAN can also be intercepted; Section 7.5.4 presents this information. Due to the lower power and shorter range of the transmissions and the quantity of signals, it will be more difficult to detect and target a specific Bluetooth or WLAN transmission. This indicates that individuals will need to be targeted in a high population environment, and the attacker would need to be within close proximity to be effective. In a conflict zone, the prevalence of these technologies may not be as high, particularly in controlled environments. Statements from the workshop (Section 6.3) indicate that the technology and capability required to intercept wireless communications is readily available; therefore the required capability can be considered as medium, taking into account targeting an individual and coming into proximity. The available controls include the wired-equivalent privacy (WEP) and Wi-Fi protected access (WPA), which can be circumvented; therefore the controls can be rated as medium. General interception of wireless communications poses a medium impact, as financial and account details may be removed. In a conflict zone, sensitive information may be compromised; therefore the impact can be high. There is also the possibility of altering the integrity of the information through modification or fabrication in addition to the eavesdropping; this impact will be very high as the correct information is compromised, and the victim has incorrect information.

8.4.2.3 Physical Exposure and Other Vulnerabilities

Physical exposure leaves some infrastructure components susceptible to physical attack; the base-stations are easily identifiable and could be targeted. The capability to overcome the physical exposure is low for base stations, as even thrown incendiary or explosive devices could damage the

base-station. Improving the physical security will be an effective control against individuals or groups; however the protection against air-strikes or artillery will be less. Therefore the control can be rated as low. The core infrastructure components will have more protection; the required capability to physically attack these would be medium, and the control effectiveness will prevent most attacks, except military strikes. The rating control rating is also high. The impact of attacking a base-station is low as only a localised area will be without services. The impact of attacking the core infrastructure will be high as regional or national services may be affected.

The risk of in-store access to the billing infrastructure was raised in Section 7.2. Account details and payment updates can be made from the stores. Such an attack is unlikely, and no reports have been found of this occurring. The attacker will need to gain access to the store computers and be familiar with the billing systems; therefore a high capability will be required. There are some controls mechanisms, such as security cameras, however these may be circumvented via unattended network points. There are also security guards and attendants in the store and shopping centres. The control strength can be rated as high. Gaining illegitimate access will allow an attacker to breach the confidentiality of subscriber information; this can be rated as medium. In addition, the integrity of the billing system and possibly deny services to users. The impact could potentially be high should an attacker be able to gain access and corrupt all the billing information; this can be rated as high.

Some device communications modules are sensitive to unusual conditions; therefore they are susceptible to malformed messages or images. The report highlighting the possibility of such an attack was presented in Section 5.5. This type of attack can be considered to be similar to a buffer overflow attack. The required capability to overcome this vulnerability can be considered as medium; the device vulnerabilities need to be researched, and the malformed message needs to be generated and transmitted. The only control for this is a possible firmware update on the device. This will have very high effectiveness, however users may not upgrade the device firmware, therefore the control effectiveness can be rated as high. The result of such an attack results in the device communications modules crashing, which is a DoS attack. The impact of such an attack will be limited; only the devices can be targeted, and not all device models may be vulnerable. Therefore the impact rating can be considered low.

It is conceivable that some infrastructure components may have similar vulnerabilities; the required capability to exploit these can be considered high. The vulnerability needs to be researched; however the accessibility to infrastructure components will be lower than devices. As before, the attacker also needs to generate and transmit the malformed message to exploit the vulnerability. The

control will be similar to the device control: a firmware upgrade or patch, which will be very effective. The impact will be greater than that of the devices as the infrastructure components will fail and some local or regional services may be lost; therefore the impact can be rated as medium.

Section 5.5 presented a report of a vulnerability that allowed a mobile enterprise server to be hijacked by transmitting malicious images. Similar vulnerabilities may allow malicious or malformed messages to hijack the system. The enterprise server is a centralised system, and could be used to further propagate malicious code and applications. The report indicated that the vulnerability was patched, and is the only report of such an incident or vulnerability. These servers may also be compromised be malware, mobile malware, social media malware, and system penetration. The required capability to do so appears to be high, as a specific vulnerability needs to be researched and exploited. Patching these vulnerabilities will provide a very high protection against these attacks. Exploiting the servers could lead to denying all organisational mobile communications connected to the server, which will have a high impact. Confidentiality could be breached, and malicious code could be distributed allowing for further breaches of confidentiality; this will have a very high impact.

A similar concept is the centralised kill switch, which enables malicious applications to be removed remotely, or to deactivated lost or stolen devices. Compromising such a system may allow attackers to deny services of all relevant devices remotely. The required capability will be same as that of the enterprise server. The controls could include extra authentication prior to implementing a wipe; this will provide a strong control as each individual device will require different authentication. This can therefore be rated as high. The impact will be low, as only relevant devices will be affected (a specific brand or make of operating system).

In addition to the sensitivity to malformed messages, the operating systems (OS) and modules of the mobile devices may exhibit vulnerabilities that can be exploited by mobile malware; Section 5.5.1.6 illustrated the prevalence of OS vulnerabilities in the malware. These vulnerabilities may allow the malware to propagate, steal information, send illegitimate SMSs or make calls, or corrupt data or the OS. The required capability to overcome these vulnerabilities is low as the development kits to generate applications are available; these can be used to produce malicious applications. Anti-virus and firewall applications, in addition to the device's own security settings, will provide a strong control; messages and files can be scanned for known malicious content, and applications can be blocked from accessing communication technologies. However, many users may not make use of these controls; therefore the rating will be considered as high. The impact of mobile malware will

be limited to vulnerable devices. Those that corrupt files or integrity will have little impact on the infrastructure; only the devices will be affected. Therefore the rating for corruption is low. Others that steal account information or connect to premium rate numbers will have a larger affect as this is financial; more recent version target mobile banking but are still not as prevalent as PC-based malware. The rating for this breach of confidentiality is medium. The impact for devices that conduct DoS attacks will be higher; there is the financial impact of the transmitted messages and the degradation of the mobile network services. The network impact of this was discussed above and in more detail in Section 7.4, and can be rated as high.

There are also vulnerabilities in the implementation of Bluetooth and WLAN on mobile devices and access points. This may allow illegitimate access and system penetration. The required capability and controls are the same for the interception of Bluetooth and WLAN discussed above. The required capability and controls are therefore both rated medium. The impact can be a breach of confidentiality and integrity of the devices; rated medium and high respectively. Should an access point be breached, then the exposure will be greater, and the impact can be rated high and very high, respectively.

The way in which the mobile infrastructure registers SIM cards is vulnerable to allowing SIM cloning. This type of attack was used in the SMS banking scandal (Section 5.5.1.3) and was raised in the interviews (Section 6.2). The technology is seemingly readily available to clone SIM cards. As of yet, there is no evidence of a control other than awareness; therefore this can be rated as low. This vulnerability primarily provides cyber-criminals with a means of communicating anonymously, and may not feature highly in an IW attack. SIM cloning subverts the authenticity of calls; this has a medium impact due to the financial aspects. As in the SMS banking scandal, there is a chance of breaching confidentiality; this can be rated as medium due to the financial impacts due to compromised account details and the potential breach of sensitive messages that are broadcast in the open.

8.4.2.4 Vulnerabilities Introduced by Mobile Devices

Mobile technologies also create vulnerabilities and risks to organisations. As was raised in the workshop, mobile devices can be used to subvert the perimeter defences of networks and provide insider access. Given that it was stated this was used for penetration testing, it implies that the capability is readily available, and therefore can be rated as low. Controls suggested for this include MAC address filtering; this will provide increased security for devices trying to connect to the access points, however it does not prevent the phone being used as a rogue access point, and can

therefore be rated as medium. The impact of such an attack is the same as a system penetration of the organisation's network.

Mobile devices can also be used to instigate violence and social unrest, as seen in the demonstrations in North Africa. Very low capability is required to do this. The only controls are to shut off Internet and mobile access; however the success of this has been inconsistent. Therefore the control will be rated as medium. The impact is high; governments have effectively been overthrown, and it has also led to civil war in one case.

Mobile devices may also be used to propagate PC-malware as illustrated by an example in Section 5.5.2. This appears rare; however the required capability will be medium as new devices need to be infected prior to packaging. Both mobile and PC-based anti-virus applications should provide a strong control, rated high. As a large number of devices need to be infected and connected to PCs for there to be any significant impact; the malware would most likely attempt to breach confidentiality, and can therefore be rated as medium. Mobile devices also provide a mechanism for information leaks; they are capable of mass storage, transmitting information through social media, and the integrated cameras are capable of capturing images and video. Very low capability is required to leak the information. The possible controls for this can be also be rated as low, unless it is a high-security environment where phones are not allowed; this then can be rated as high (there is the possibility that a device could be smuggled in). The devices will be used to breach confidentiality; the impact can be rated as high in normal security, and very high for high security.

8.4.3 Summary

The required capability to exploit a vulnerability, control strength, and impact were discussed in Sections 8.4.1 and 8.4.2. The required capability and control strength are used to provide a vulnerability rating. The matrix used is presented in Table 8.3.

Table 8.3: Matrix for Vulnerabilities

Control Strength	**Required Capability**				
	V. Low	*Low*	*Med*	*High*	*V. High*
V. Low	V. High	V. High	High	High	Med
Low	V. High	High	High	Med	Low
Med	High	High	Med	Low	Low
High	High	Med	Low	Low	V. Low
V. High	Med	Low	Low	V. Low	V. Low

Table 8.4 summarises the vulnerabilities as discussed above, and provides the individual vulnerability ratings.

Table 8.4: Vulnerability Ratings

Vulnerability	Required capability to overcome	Control rating	Vulnerability rating
General/Non-technical			
Awareness	Very low	Low	Very High
Corporate attitude	Low	Medium	High
Ineffective policies	Low	Medium	High
Legislature	Low	Medium	High
CSIRT	Low	Medium	High
Political	Very low	Medium	High
DoS	Very low	Low	Very high
System penetration	Medium	Low	High
Technical			
Operating conditions	Low	Very low	Very high
Centralisation and singularities	Medium	Medium	Medium
Mobile enterprise server	High	Very high	Very low
Centralised kill switch	High	High	Low
General vulnerabilities	Low	High	Medium
Previously unknown vulnerabilities	High	Low	Medium
Electromagnetic exposure	Very High	Low	Low
Jamming GSM	Low	Low	High
Jamming 3G	Medium	Medium	Medium
Jamming WLAN and Bluetooth	Medium	Low	High
Intercept GSM	Medium	Medium	Medium
Intercept 3G	High	High	Low
Intercept WLAN and Bluetooth	Medium	Medium	Medium
Device communications sensitivity	Medium	High	Low
Infrastructure sensitivity	High	Very high	Very low
Device OS vulnerabilities	Low	Medium	High
Bluetooth and WLAN device vulnerabilities	Medium	Medium	Medium
Physical exposure – base stations	Low	Low	High
Physical exposure – core components	Medium	High	Low
SIM authentication weakness	Low	Low	High

Table 8.4: Vulnerability Ratings (Continued)			
Vulnerability	**Required capability to overcome**	**Control rating**	**Vulnerability rating**
Store access	High	High	Low
Vulnerabilities due to mobile devices			
Subvert perimeter	Low	Medium	High
Instigate violence	Very low	Medium	High
Propagate Malware	Medium	High	Low
Information leak – normal security	Very low	Low	Very high
Information leak – high security	Very low	High	High

From the general and non-technical factors, we can see that South Africa is vulnerable to an IW attack. From the technical vulnerabilities of the mobile infrastructure, six of twenty-one listed are rated high or above, seven are rated as medium, and eight are rated as low or less. A concern is the high loads which the mobile infrastructure appears to be operating under; this may leave it susceptible to DoS attacks. It can also be seen that mobile devices in the organisation increase the vulnerability of the organisation's ICT infrastructure to attack, as four of five vulnerabilities are rated as high or above. The vulnerabilities will be prioritised according to the risk they present; these will be calculated in Section 8.5. The vulnerabilities and risks will be discussed further in Section 8.6.

8.5 Modified TVA and Risk

This section presents the modified TVA table and the risk ratings. The threat and vulnerability ratings indicate the likelihood of a successful attack; the matrix for this is presented in Table 8.5. This is then used with the impact to get the risk rating; the matrix is presented in Table 8.6.

Table 8.5: Matrix for the Likelihood of a Successful Attack					
Threat	**Vulnerability**				
	V. Low	*Low*	*Med*	*High*	*V. High*
V. Low	V. Low	V. Low	Low	Low	Med
Low	V. Low	Low	Low	Med	High
Med	Low	Low	Med	High	High
High	Low	Med	High	High	V. High
V. High	Med	High	High	V. High	V. High

Table 8.6: Matrix for Risk

Impact	Likelihood of a Successful Attack				
	V. Low	*Low*	*Med*	*High*	*V. High*
V. Low	V. Low	V. Low	Low	Low	Med
Low	V. Low	Low	Low	Med	High
Med	Low	Low	Med	High	High
High	Low	Med	High	High	V. High
V. High	Med	High	High	V. High	V. High

Table 8.7 summarises the vulnerabilities, their associated threats, and the resultant likelihood of a successful attack. The associated impacts are also listed, and the resultant risk ratings are provided.

Table 8.7: Mobile Infrastructure TVA Worksheet

Vulnerability name and rating	Associated threat names and ratings	Likelihood of Successful Attack	Impact type and rating	Risk rating
Non-technical and General Factors				
Awareness (High)	Malware (High)	High	General (Medium)	High
	Social engineering (High)	High	Confidentiality (Medium)	High
	Mobile phishing (Medium)	High	Confidentiality (Medium)	High
Corporate attitude and ineffective policies (High)	Malware (High)	High	General (High) Confidentiality (High)	High
	System penetration (High)	High		High
	Insider (High)	High		High
	Social media malware (Medium)	High		High
Legislature (High)	Cyber-crime (High)	High	General (Low)	Medium
	Rogue groups (Low)	Medium	General (Low)	Low
CSIRT (High)	Cyber-crime (High)	High	General (Medium)	High
	Rogue groups (Medium)	High	General (Medium)	High
	Nation States (Medium)	High	General (Medium)	High
Political (High)	Rogue groups (Medium)	High	General (High)	High
	Nation States (Medium)	High	General (High)	High

Table 8.7: Mobile Infrastructure TVA Worksheet (Continued)

Vulnerability name and rating	Associated threat names and ratings	Likelihood of Successful Attack	Impact type and rating	Risk rating
DoS (Very high)	Rogue groups (Medium)	High	DoS (High)	High
	Nation states (Low)	High	DoS (High)	High
System penetration (High)	Rogue groups (Low)	Medium	Confidentiality (High)	High
	Nation states (Medium)	High	Confidentiality (High)	High
Technical Factors				
High operating load (Very high)	Mobile DoS (Medium)	High	DoS (Medium)	High
	Exploit SMS functionality (Low)	High	DoS (High)	High
Centralisation of mobile infrastructure components (Medium)	Mobile DoS (Medium)	High	DoS (Medium)	High
	Exploit SMS functionality (Low)	Low	DoS (High)	Medium
Mobile enterprise server vulnerabilities (Very Low)	Malware (High)	Low	Confidentiality (Very high)	High
			DoS (High)	Medium
	Mobile malware (Medium)	Low	Confidentiality (Very high)	High
			DoS (High)	Medium
	Social media malware (Medium)	Low	Confidentiality (Very high)	High
			DoS (High)	Medium
	Malicious messages (Low)	Low	Confidentiality (Very high)	High
			DoS (High)	Medium
	System penetration (High)	Low	Confidentiality (Very high)	High
			DoS (High)	Medium
Centralised kill switch (Low)	System penetration (High)	Medium	DoS (Low)	Low
Device vulnerabilities (High)	Mobile malware (Medium)	High	Corruption (Low)	Medium
			Confidentiality (Medium)	High
			DoS (High)	High
	Malicious messages (Low)	Medium	DoS (Low)	Low

Table 8.7: Mobile Infrastructure TVA Worksheet (Continued)

Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating
General vulnerabilities (Medium)	System penetration (High)	High	Confidentiality (High)	High
			Corruption and Confidentiality (Very high)	Very high
			DoS (High)	High
	Malware (High)	High	Confidentiality (High)	High
			Corruption and DoS (Very high)	Very High
	Social media malware (Medium)	Medium	Confidentiality (High)	High
			Corruption and DoS (Very high)	High
Previously unknown vulnerabilities (Medium)	System penetration (High)	High	Confidentiality (High)	High
			Corruption and Confidentiality (Very high)	Very High
			DoS (High)	High
	Malware (High)	High	Confidentiality (High)	High
			Corruption and DoS (Very high)	Very high
	Social media malware (Medium)	Medium	Confidentiality (High)	High
			Corruption and DoS (Very high)	High
Infrastructure sensitivity (Very low)	Malicious messages (Very low)	Very low	DoS (Medium)	Low
WLAN and Bluetooth device vulnerabilities (Medium)	WLAN attacks (Low)	Low	Confidentiality (Medium)	Low
			Confidentiality and Corruption (High)	Medium
	Bluejacking (Low)	Low	Confidentiality (Medium)	Low
			Confidentiality and Corruption (High)	Medium
Electromagnetic exposure (Low)	Directed energy (Low)	Low	DoS (Low)	Low
	EMP (Low)	Low	DoS (High)	Medium

Table 8.7: Mobile Infrastructure TVA Worksheet (Continued)

Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating
WLAN access point vulnerabilities (Medium)	WLAN attacks (Low)	Low	Confidentiality (High)	Medium
			Confidentiality and Corruption (Very high)	High
Jamming GSM (High)	Jamming – military (High)	High	DoS (Medium)	High
	Jamming – home made (Low)	Medium	DoS (Low)	Low
Jamming 3G (Medium)	Jamming – military (High)	High	DoS (Medium)	High
	Jamming – home made (Low)	Low	DoS (Low)	Low
Jamming WLAN and Bluetooth (High)	Jamming – military (High)	High	DoS (Low)	Medium
	Jamming – home made (Low)	Medium	DoS (Low)	Low
Intercept GSM (Medium)	Eavesdropping – military (Medium)	Medium	Confidentiality (High)	High
	Eavesdropping – individual (Low)	Low	Confidentiality (Low)	Low
Intercept 3G (Low)	Eavesdropping – military (Medium)	Medium	Confidentiality (High)	High
	Eavesdropping – individual (Low)	Low	Confidentiality (Low)	Low
Intercept WLAN and Bluetooth (Medium)	Eavesdropping – military (Medium)	Medium	Confidentiality (High)	High
			Corruption and confidentiality (Very high)	High
	Eavesdropping – individual (Low)	Low	Confidentiality (Medium)	Low
Physical exposure – base stations (High)	Conflict/military (Medium)	High	DoS (Low)	Medium
	Peace/Homemade (Low)	Medium	DoS (Low)	Low
Physical exposure – core components (Low)	Conflict/military (Medium)	Low	DoS (High)	Medium
	Peace/Homemade (Low)	Low	DoS (High)	Medium

Table 8.7: Mobile Infrastructure TVA Worksheet (Continued)

Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating	Vulnerability name and rating
Physical exposure – in-store access (Low)	Illegitimate access (Low)	Low	Confidentiality (Medium)	Low
			CIA (High)	Medium
SIM authenticity weakness (High)	SIM Cloning State (Low)	Medium	Corruption (Medium)	Medium
	SIM Cloning Non-state (High)	High	Confidentiality (Medium)	High
Vulnerabilities due to Mobile Devices				
Subvert perimeter (High)	System penetration (High)	High	Confidentiality (High)	High
			Confidentiality and Corruption (Very high)	Very high
			DoS (High)	High
Instigate violence (High)	Social engineering (High)	High	Uprisings (High)	High
Malware vector (Low)	Malware (High)	Medium	Confidentiality (Medium)	Medium
Information leak normal security (Very high)	Insider Leaks (High)	Very high	Confidentiality (High)	Very high
Information leak high security (High)	Insider Leaks (High)	High	Confidentiality (Very high)	Very high

The general vulnerabilities show that due to the high vulnerability, South Africa is at high risk from an attack. The threats are generally not high, other than malware and cyber-crime. This indicates that the national vulnerabilities need to be addressed in order to reduce risk. The lack of awareness should be addressed. The corporate attitudes could be addressed indirectly by introducing firmer legislation regarding information security; this will also directly address the apparent shortage of cyber-related legislature in South Africa. The introduction of a publicly accessible CSIRT will aid in awareness, assisting organisations with incidents, and provide much needed intelligence regarding the threats and big picture of the incidents in South Africa. Such a facility may also provide crucial support in the event of a major cyber-attack against the national ICT infrastructure.

There are sixty-three technical risk elements listed for the mobile infrastructure; fourteen are low, seventeen are medium, twenty-eight are high, and four are very high. Whilst the worst-case scenario

was taken, which will result in a skewing towards the high ratings of the risk, the majority are due to either high vulnerability, or high impact. This again indicates that vulnerabilities need to be addressed, and the potential high impact also further indicates the criticality of the mobile infrastructure. Of particular concern is the ability of malware and hacking to exploit vulnerabilities of critical systems; this may allow attackers to access potentially sensitive conversations (such as the Athens Affair) and corrupt information to hinder recovery. Infrastructure control systems may also be corrupted, resulting in the ultimate denial of services; due to the corruption (or damage) of systems, the recovery from the initial attack will take longer. The high operating load and centralisation or regional singularities of components also results in susceptibility to DoS attacks.

The vulnerabilities introduced by the use of mobile devices result in high risks. In these instances the threats associated with this use are also rated high, which increases the risks where the vulnerability is low. Of particular note is the very high ratings for information leaks; this vulnerabilities need to be prioritised and addressed. Solutions include stricter device filtering and policy implementation.

The vulnerability and risks are further analysed and discussed in Section 8.6, where the infrastructure vulnerability and risk are calculated. Different aspects of the IW threats and impacts will also be compared and discussed.

8.6 Infrastructure Vulnerability and Risk

In this section, the infrastructure and vulnerability risk ratings are calculated and presented. Section 8.6.1 presents the overall infrastructure vulnerability and risk ratings, whereas Section 8.6.2 will provide comparisons of the IW threat elements and impacts types. Section 8.6.3 will summarise the section.

8.6.1 General

The infrastructure vulnerability and risk ratings are calculated and presented in this section. Section 8.6.1.1 will present the calculation of the infrastructure vulnerability rating, and Section 8.6.1.2 presents the calculation of the infrastructure risk rating.

8.6.1.1 Infrastructure Vulnerability Rating

The infrastructure vulnerability rating is calculated using Equation 4.2 presented in Section 4.3.1:

$$Infrastructure\ vulnerablity = \sqrt[2]{\sum_{i=0}^{N} v_i^2},$$

Table 8.8 summarises the number of elements and individual ratings, and provides the infrastructure vulnerability rating for non-technical or general factors, technical factors, and vulnerabilities introduced by mobile devices into ICT infrastructures.

Table 8.8: Infrastructure Vulnerability Ratings

	General	Technical Mobile	Due to Mobile
No. of elements	8	21	5
No. rated Very Low	0	2	1
No. rated Low	0	6	0
No. rated Medium	0	7	0
No. rated High	6	5	3
No. rated Very High	2	1	1
Infrastructure Rating	12.1	13.93	8.77
Maximum possible rating	14.14	22.91	11.18

As can be seen from Table 8.8, the vulnerability due to general or non-technical factors is high; this is also true for vulnerabilities introduced into ICT infrastructures due to mobile usage. The rating figure for the technical vulnerabilities of the mobile infrastructure is at a point where it can be considered at the juncture of medium and high. This indicates that whilst the vulnerabilities are present, it is not crucially vulnerable to attack the few high priority vulnerabilities can be addressed prior to controls being implemented for others. The high priority vulnerabilities were indicated in Section 8.5. It is important to look at the rating in context of the maximum possible rating; an increase in this gives an indication of a worst-case vulnerability environment. An increase in the maximum possible rating indicates an increase in potential vulnerabilities for an attacker to exploit. These rating figures will allow an assessor to compare the vulnerability with previous (and future) assessments; as threats arise and controls are introduced, the ratings will change, giving an indication of an increase or decrease in vulnerability. The intention is to use this figure to chart the vulnerability ratings over a period of time; ideally the figure should decrease, indicating the number of vulnerabilities or the severity of the vulnerabilities has decreased.

The high vulnerability ratings arising from the assessment for general vulnerabilities is in line with the number of concerns regarding the information security issues; namely the severity of a few key areas which results in a high threat prevalence. The high ratings due to the use of mobile devices

also correspond to concerns regarding the ability to manage new technologies, and the possibility of them being used as an attack vector. This further indicates that mobile devices may be an effective tool in IW and intelligence gathering. The vulnerability rating of the mobile infrastructure indicates that the infrastructure is a potential target for IW attacks due to the number of vulnerabilities present, and their nature and severity.

8.6.1.2 Infrastructure Risk Rating

The infrastructure risk rating is calculated using Equation 4.3 presented in Section 4.3.1:

$$Infrastructure\ risk = \sqrt[2]{\sum_{i=0}^{M} r_i^2},$$

Table 8.9 summarises the number of elements and individual ratings, and provides the infrastructure risk rating for non-technical or general factors, technical factors, and risks introduced by mobile devices into ICT infrastructures.

Table 8.9: Infrastructure Risk Ratings

	General	Technical Factors	Due to Mobile
No. of elements	18	63	7
No. rated Very Low	0	0	0
No. rated Low	1	14	0
No. rated Medium	1	17	1
No. rated High	16	28	3
No. rated Very High	0	4	3
Overall Rating	16.4	27.51	11.49
Maximum possible rating	21.21	39.69	13.23

As can be seen from Table 8.9, the risks are high for all categories. The risk figures are expected to be larger than the vulnerability figures as there are multiple threats and impacts associated with each vulnerability. The risks due to mobile use indicate that there are a few elements, but of high risk.

8.6.2 Comparative

This section presents trends comparisons of the vulnerability and risk ratings related to specific impact types and IW functional areas, namely network warfare and electronic warfare. A comparison of threats is also made. The equations are used as in Section 8.6.1, however each impact type or functional area is considered separately.

8.6.2.1 Impact Types

The vulnerability and risk ratings are compared for different impact types. As above, the impact types are breach of confidentiality, corruption (breach of integrity), denial of services, and general; these were identified in Section 2.3.2.1 and incorporated in the proposed IW Lifecycle Model in Section 4.2.6. The purpose of this comparison is to assess the relative risk of information attributes (confidentiality, integrity, and availability) being breached. This will give an indication of the type of controls required to be implemented to protect the information and relevant systems. Table 8.10 summarises the vulnerability and risk ratings for the various impact types.

Table 8.10: Comparison of Ratings by Impact Type

		Confidentiality	Corruption	Denial	General
Vulnerability	No. of elements	18	9	16	5
	Overall Rating	14.66	9.85	13.4	8.94
	Maximum Possible Rating	21.21	15	20	11.18
Risk	No. of elements	35	14	35	12
	Overall Rating	22.18	15.3	14.66	13.15
	Maximum Possible Rating	29.56	18.71	29.56	17.32

The comparison shows that breaches of confidentiality exhibit the largest risk, followed by corruption, and then DoS attacks. However, vulnerability to DoS attacks is higher than that of integrity and only slightly lower than that of confidentiality. Confidentiality also has a threat of insider attacks and due to penetration by mobile devices; corruption has s higher impact, but it is more difficult to effect and therefore less likely. Consequently, breaches of confidentiality become the higher risk threat.

At a general level, South Africa is vulnerable to attack with a rating of 8.94 out of a maximum of 11.18. This is due to a severe lack of awareness of users with regard to information security issues, a lack of an operational CSIRT, insufficient implemented legislature, perceived political alignments, and some internal dissatisfaction. The risk is not as high, rating 13.15 out of a maximum of 17.32. The current political instability in Africa also heightens the vulnerability and risk of an attack. These ratings indicate a concerted effort needs to be made to improve particularly awareness and the implemented legislature, and commission a CSIRT that is publicly accessible. Political decisions that could possibly be seen as controversial in the international context need to

be very carefully made, as Chapter 4 and Chapter 5 show that this is often the catalyst for IW attacks against a nation or organisation.

Figure 8.1 shows a visual representation of the risk and vulnerability comparison for the various impact types. Those that show high vulnerability and risk (and therefore are located towards the upper right corner of the plot) should be prioritised. From the plot, the priority for technical factors should be, in order: protection of confidentiality, availability, and then integrity. Often controls for confidentiality also provide controls for integrity, for example encryption and digital signatures. General non-technical factors should also be addressed in parallel, however by addressing the technical areas, some mitigation of legal vulnerabilities may be provided.

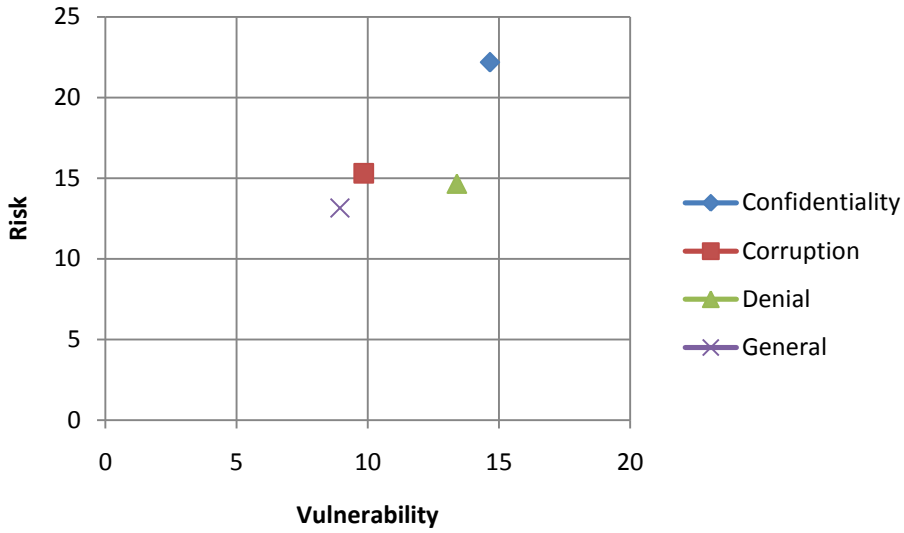


Figure 8.1: Scatter Graph of Impact Types

8.6.2.2 IW Functional Areas

The vulnerability and risk ratings are compared for two IW functional areas, namely electronic warfare and network warfare. The equivalent impacts (jamming and DoS, and interception and breach of confidentiality) will be considered. The purpose of this comparison is to provide an indication the relative effectiveness of the two functional areas against the mobile infrastructure. Table 8.11 summarises the vulnerability and risk of the two IW functional areas. For this comparison the vulnerability of mobile enterprise servers was not considered; only the wireless communication channels and infrastructure components were considered, where the actual communication is the target.

Table 8.11: Comparison of Ratings by IW Functional Area					
		Electronic Warfare		**Network Warfare**	
		Jamming	**Intercept**	**DoS**	**Confidentiality**
Vulnerability	No. of elements	3	3	6	4
	Infrastructure Rating	6.4	4.69	6.24	6
	Maximum Possible Rating	8.66	8.66	12.25	10
Risk	No. of elements	3	Military: 4 Peace: 3	12	9
	Infrastructure Rating	Military: 6.4 Peace: 3.46	Military: 8 Peace: 3.46	13.38	10.63
	Maximum Possible Rating	8.66	Military: 10 Peace: 8.66	17.32	15

In terms of denial, there is a slightly greater vulnerability to jamming than a network warfare DoS attack; however the risk due to network warfare is much higher. In terms of confidentiality, there is a higher vulnerability and risk due to network warfare. This is partly due to the fact that in some cases the communications are not encrypted whilst transiting through the infrastructure components. In this example, the network warfare DoS poses more risk due to the types of attack considered, of which there are more vulnerabilities to a DoS attack than a breach of confidentiality. This indicates that network warfare solutions may be more efficient than electronic warfare. If the range limitations are taken into account, network warfare can be considered as a better strategic option; however should military assets be available in a conflict zone, electronic warfare may prove to be a better tactical option. Network warfare, in general, has more delivery threats, and also has the possibility of insider assistance.

Figure 8.2 presents a visual representation of the comparison. From the plot, the priority should be in securing the availability of mobile services and the confidentiality of the communications from a strategic network warfare attack. In a conflict zone, there should also be focus on protecting the signals from electronic warfare attack. From this it may be required to develop a mobile infrastructure equivalent of a sinkhole or black hole to redirect or filter traffic flooding the network. Introducing end-to-end encryption will reduce the vulnerability and risk due to interception from either electronic warfare or network warfare techniques.

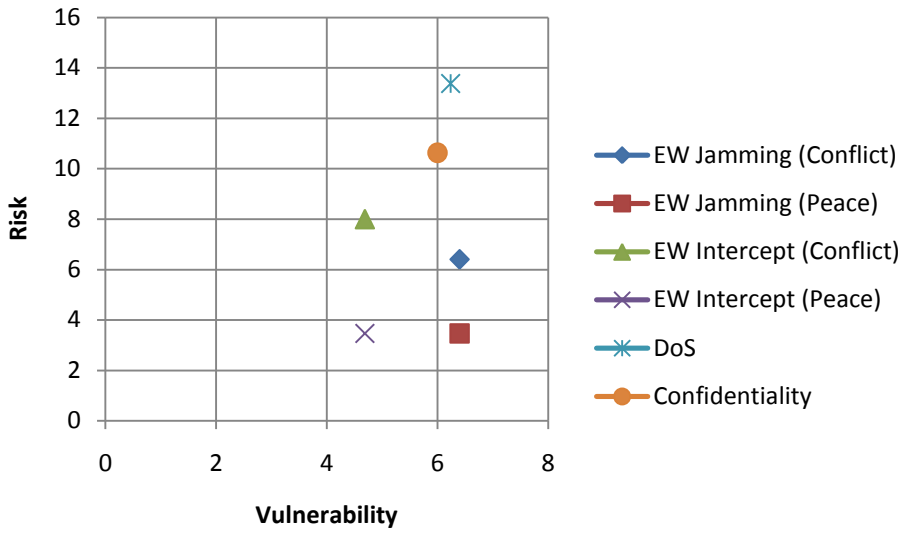


Figure 8.2: Scatter Graph of IW Functional Areas

8.6.2.3 Network Warfare Threats

As network warfare was shown to present a higher risk, various threats associated with network warfare are compared. Table 8.12 summarises the vulnerability and risk ratings for the threats.

Table 8.12: Comparison of Ratings by Network Warfare Threat Type

		Malware	Mobile Malware	Social Media Malware	System Penetration
Vulnerability	No. of elements	6	4	4	7
	Overall Rating	7.42	7.14	5.92	8.43
	Maximum Possible Rating	12.25	10	10	13.23
Risk	No. of elements	9	7	7	14
	Overall Rating	11.79	9.9	10.25	15.23
	Maximum Possible Rating	15	13.23	13.23	18.71

There is a larger vulnerability and risk to system penetration over malware; this is due to the additional vulnerability associated with system penetration. It should be noted that malware might contribute to system penetration, as in the GhostNet and related incidents. Traditional PC-based malware exhibits greater vulnerability and risk ratings over the emerging mobile malware and social media malware. There is a greater vulnerability to mobile malware over social media malware; this is probably due to the fact that mobile equivalents of anti-virus applications are not as

well known or prevalent as the traditional computer anti-virus applications. Social media malware presents a higher risk as it is not limited to specific devices, and targets Internet banking which is still more prevalent than mobile banking.

Figure 8.3 presents the threat comparison visually. The plot indicates that priority should be given to addressing the threat of system penetration, traditional malware, and then the emerging malware versions. Improving anti-virus protection on networks will aid in mitigating traditional malware, social media malware, and therefore system penetration. It was indicated that many breaches could have been easily prevented; therefore the focus should be on ensuring systems are patched, and security mechanisms are up to date and properly configured.

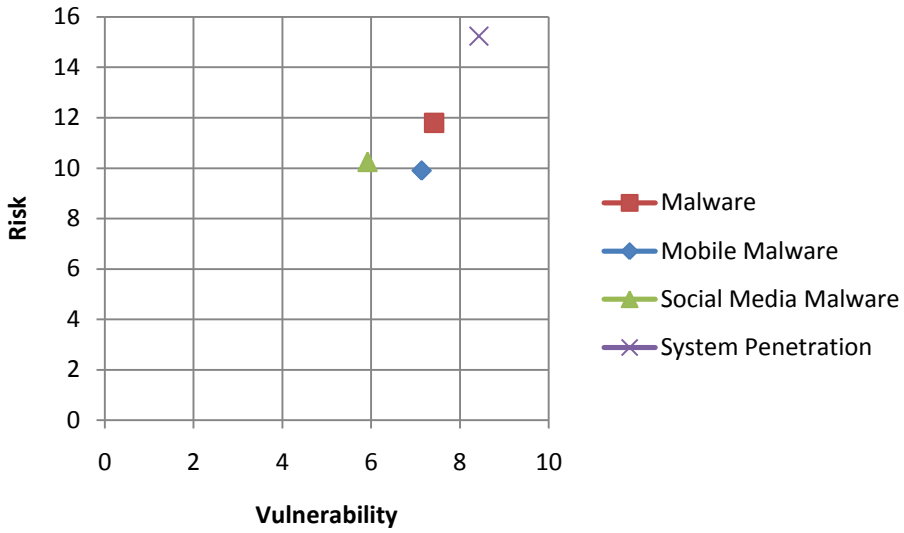


Figure 8.3: Scatter Graph of Network Warfare Threats

8.6.3 Summary and Discussion

The vulnerability of the mobile infrastructure can be considered to be high mid-range given the maximum possible rating. The figure is high though due to the number of vulnerabilities. Whilst a generic mobile infrastructure was considered, this raises concerns over the susceptibility of the South African mobile infrastructure to attack. The related risk is high; this is due to possible high impacts and some high vulnerabilities. Even though the worst-case scenario was used, the high vulnerability and risk values indicate that extra measures need to be taken to improve the security of the mobile infrastructure. The high risk rating corresponds to the discussion in Section 8.2; both indicate that the mobile infrastructure is critical.

Of the technical risks, those related to breaches of confidentiality were the highest, followed by corruption and then denial of service. This is to be expected as a large proportion of attacks discussed in Chapter 4 and Chapter 5 can be considered espionage, and the prevalence of confidentiality issues in the interviews and workshop. The high risk rating indicates that this prevalence has been correctly reflected by the proposed framework. The integrity rating is high due to the fact it is often coupled with breaches of confidentiality or denial of service attacks; for example the Maroochy sewerage incident and the Stuxnet worm both impacted on the integrity of the systems, and the GhostNet types attack had the ability to both makes changes to the targeted systems as well as access information. Large scale DoS attacks on nations are not as prevalent; whilst the immediate impact is greater, it is not always as long lasting as some breaches of confidentiality have been. For instance, the leaked information to Wikileaks is still being gradually released, and some socio-political ramifications are still being felt assuming it is true that the releases contributed to sparking the uprisings in North Africa (presented in Section 4.2.7.6). Therefore denial attacks having the lowest risk rating again correspond to the data, indicating the proposed framework has correctly reflected this. The general impacts indicate that there is a vulnerability to IW attacks, and some risk; however due to low threat the risk is not as high as it could be.

The comparison of the IW functional areas illustrates that network warfare presents a higher risk rating than electronic warfare; this indicates that the proposed framework correctly reflects the discussions of the data. Despite network warfare presenting a higher risk, should military electronic warfare assets be available in a conflict area, these would provide a better tactical option than network warfare. The comparison of the network warfare threats indicates that the framework correctly reflects the high risk presented by malware and system penetration.

There were two aspects that were not covered in the assessment above as they do not relate directly to an IW attack on the mobile infrastructure, or misuse of services for IW purposes, but are in some way relevant and are discussed here for completeness. The first relates to the vulnerability of the mobile infrastructure; in Section 2.7.2.1 dependency on other infrastructures was listed as a vulnerability category. The mobile infrastructure has some dependency on the electric power grid, however backup generators and solar power will be able to provide some functionality should there be widespread power disruption. Therefore an indirect attack on the electric power grid may eventually result in service outages; however there will be additional, more possibly more severe, impacts due to the attack than the lack of mobile services. The second aspect is the use of legitimate

mobile services to detonate IEDs; this was raised in Chapter 5 and Chapter 6. This is one of the reasons that military electronic warfare is used to target mobile phones in conflict zones. Whilst these devices are known for their effectiveness in the Afghanistan and Iraq conflicts, mobile detonate bombs have been used in South Africa, as mentioned in Sections 5.3 and 5.7.

8.7 Opportunities

This section discusses opportunities and possible solutions to the vulnerabilities or to mitigate the impacts. These opportunities are derived from the incident and trend analysis (Chapter 5), the interviews (Section 6.2), and the workshop (Section 6.3). Sections 8.7.1 and 8.7.2 present the non-technical and technical factors, respectively. Section 8.7.3 summarises this section.

8.7.1 Non-Technical

A number of non-technical opportunities and solutions were proposed in the interviews and trend and incident analysis; these range from international assistance to building local capacity. These factors are presented in more detail in this section.

The fields of IW, information security, and critical information infrastructure protection have been researched and effective tools and methods have been developed, particularly in Europe and the United States. There is the opportunity to gain capacity and knowledge through participation and engagement at an international level through conferences and working groups. This can then be used to facilitate local engagement to grow further in these areas. In particular, capacity building in defensive information warfare areas should be prioritised, not only by the military, but by government in general and major service providers.

South Africa has the capacity to introduce a CSIRT; it was indicated in the interviews that international CERTS are willing to aid in the creation of a South African CSIRT. This CSIRT should be developed with the specific aim of interacting with public and private organisations, and some information, such as annual reports, warnings, and advisories, should be accessible by the general population to improve awareness.

Improve general awareness of information security issues is imperative. The lack of awareness was raised repeatedly throughout the study, indicating the prevalence of this problem and the concern it is creating. Awareness training programmes for security online, for mobile devices, and social networks should be conducted. Further reinforcing awareness of information security throughout school and tertiary education should be implemented. In particular, the workshop discussion

suggested that information technology related degrees should increase the level of security considerations in the modules. This could include the concept of integrating security in programming and development from an early stage. It was also suggested in the workshop that the introduction of a professional body to oversee and accredit degrees and professionals could aid in improving the overall quality of professionals and the implementation of systems in South Africa, thereby reducing vulnerabilities.

South Africa has an opportunity to learn from international legislation, standards, and policies; those developed in Europe were specifically cited in the interviews. The advantage of this is that these have already had been implemented and therefore tested more thoroughly, which allows for some hindsight. From the workshop it was clear that the POPI Act will be compliant with all the major corresponding international laws. This provides a unique opportunity to ensure organisational compliance at an international level once the bill has been enacted. The introduction of policies specific to new technologies, or the rapid revising of existing policies to include issues raised by these technologies will aid in addressing specific threat and vulnerabilities at an early stage, prior to bad habits being formed by employees with regards to the use of modern technology.

For the specific case of mobile technology, equivalent security techniques and controls to PC-based networks should be research and developed. This will allow for better prevention, detection, and response should an attack occur.

8.7.2 Technical

A number of technical solutions were suggested in the workshop, interviews, and trend and incident analysis. These factors are presented in this section as opportunities to improve defensive measures against IW attacks.

Stricter filtering mechanisms to prevent unauthorised devices from connecting to the network should be implemented. Internet service providers should also improve filtering and monitoring capabilities, and introduce black holes and sinkholes if this has not already been done.

Data classification was strongly recommended in the workshop as a technique to identify sensitive information, thereby ensuring sufficient protective measures are assigned to the data. Data classification may be mandatory by the POPI Bill; as it is yet to be enacted, organisations have the opportunity to begin implementing this to be compliant by the time the bill is enacted.

Increasing redundancy of critical systems may aid in protecting against attacks; providing for extra capacity and dynamic introduction of these systems will mitigate down-time in the event of physical damage or increase capacity in the event of a DoS attack.

Whilst South Africa is unlikely to be targeted by a large scale EMP, some additional shielding of infrastructure components could aid in survivability and longevity of components; this will also mitigate the impact of other directed energy devices.

All systems should have the most recent anti-virus protection and patches, even if they are behind an air-gap; any flash drives, laptops, or other devices used to perform maintenance and transfer information to the systems behind the air-gap should also be fully protected. This will reduce the chance of malware transiting the air-gap and infecting the control systems and infrastructure components.

A technical control that should be implemented is end-to-end encryption of communications; this will mitigate the threat of information or communications being intercepted in transit, even when the infrastructure or communications medium itself does not provide encryption capability. In particular, mobile communications and VOIP links should employ mandatory end-to-end encryption should any potentially sensitive information be required to be communicated across the channel.

A method that may aid in mitigating legitimate mobile applications being compromised by malware is to provide a method of digitally signing them, and providing the message digest of the file to ensure their integrity before installing.

In Section 5.6 the concept of a social media honey pot was mentioned; this was originally proposed by the candidate in van Niekerk, Ramluckan, and Maharaj (2011). This control could be employed to gain intelligence on social media threats and provide warning to users that have potentially been targeted. Gaining such information could then be used to improve awareness training regarding the threats on social media websites.

8.7.3 Summary

South Africa has the opportunity to become the leading nation in the continent in terms of information warfare and security. The apparent lack of focus on the information security (in particular cyber-security) area may eventually hinder economic development due to direct financial losses from cyber-crime, and loss of confidence of international investors. South Africa may also

lose existing investors should international legislative requirements for information security become stricter and prohibit information interaction with nations that do not have equivalent laws. The POPI Bill provides an opportunity to ensure international compliance.

Generating awareness and additional training dedicated to information security will improve reduce the national vulnerability; improving the capacity will also indirectly aid in improving the technical countermeasures, providing for more secure and stable information environment in South Africa.

8.8 Review of the IW Vulnerability Assessment Framework

This section will review the performance of the proposed vulnerability assessment framework. The objective was to propose a framework that was adaptable, scalable, and progressed logically from high-level concepts to implementation.

The application of the framework to a corporate cloud computing example in Section 4.3.2, and the mobile infrastructure at a national level in the thesis, indicates that scalability has been achieved. The framework is modular in that any section of the assessment can be replaced by another method, allowing for adaptability; the application to the cloud computing scenario in Section 4.3.2 and the mobile infrastructure above also indicates a degree of adaptability. The aim of the framework was to provide a logical progression through high-level concepts to the implementation and assessment and analysis. The implementation in Section 4.3.2 and above illustrated the logical progression of the framework, where the data for the above assessment was presented in Chapter 4 to Chapter 7. Due to security and ethical concerns, not all assessment methodologies could be implemented, such as penetration testing of the actual infrastructure and related systems. From Section 4.3.2, it was indicated that the framework correctly reflected the cloud computing scenario, and Section 8.6.3 indicates that the data from Chapter 4 to Chapter 7 is correctly reflected by the assessment above. In Section 8.6.2 the vulnerability and risk of various aspects were compared; namely the impact type, IW functional areas, and various threats. This indicates that the framework provides the capability for comparative analysis.

From this there is indication that the proposed vulnerability assessment performed its functions adequately. The outcomes of the assessments corresponded to the data and literature, and the framework proved to provide a logical progression through the assessment process. The framework also provided a means of comparing various aspects of the threat, vulnerability, and risk environments related to the scenario being analysed.

8.9 Chapter Summary

The chapter performed the vulnerability and risk assessment of a generic mobile infrastructure from the data presented and framework in Chapter 4 to Chapter 7. It was determined that the mobile infrastructure does form part of the national critical information infrastructure; the prevalence of and dependence on mobile communications in South Africa indicates that it may be more critical than in other nations.

Major threats to South Africa include the high rates of malware infection and software piracy leaving systems vulnerable. The likelihood of threat action is low; however due to the current political in Africa, this can be elevated to medium. The lack of user awareness presents a very high vulnerability to South Africa; there is also a vulnerability to large-scale DoS attacks. The apparent high load of the mobile infrastructure in South Africa presents a high technical vulnerability due to the increased susceptibility to DoS attacks on the infrastructure. The highest risk is the exploitation of vulnerabilities in infrastructure systems to allow breaches of confidentiality, integrity, and possible denial of services. The use of mobiles also presents a high risk of data leaks to organisations. Comparative analysis indicates that breaches to confidentiality form the highest risk, network warfare techniques may prove to be more efficient in strategic attacks, and the threats malware and system penetrations present the highest risk. These correspond to the discussion in Chapter 4 to Chapter 7. Increasing awareness and implementing a CSIRT to aid with both response and improvement of technical security provides major opportunities for South Africa to mitigate the risk. The proposed framework was reviewed, and the objectives of the framework have been met, and the outcomes from the assessments correspond to the gathered data and literature.

Chapter 9. Conclusion

9.1 Introduction

This chapter concludes the thesis, and will discuss the outcome of the study objectives, present recommendations, and propose future research. Section 9.2 discusses the objective of further developing a framework to conduct infrastructure vulnerability assessments; Section 9.3 discusses the information gathered regarding attack on the information infrastructure. Section 9.4 discusses the criticality of the mobile infrastructure, and the framework application to the mobile infrastructure is discussed in Section 9.5, while Section 9.6 discusses the secondary objectives. Section 9.7 presents the recommendations from the study, and Section 9.8 suggests future research.

9.2 Further Develop a Framework for Infrastructure Vulnerability Assessments from and IW Perspective

An objective of the study was to propose a vulnerability assessment framework that could be used to assess information infrastructures from an IW perspective. To do this, a consolidated model for IW incidents was proposed, which could then be related to the risk and vulnerability assessment frameworks. Both the IW Lifecycle model and the vulnerability assessment framework were proposed in Chapter 4.

The IW Lifecycle Model was proposed to form a coherent model by combining aspects of IW models that were presented in the literature review. A two-level model was proposed: the high-level provided the basic concepts of the model, and the second layer provided the detail of the IW concepts. The dual layers were required as some of the detailed concepts overlapped multiple high-level blocks. The model was used to analyse a number of incidents, some of which were used to review the model. The model adequately described the incidents, and from the analysis it could be seen that the role played by the context in shaping the IW incident regarding the methods used was as important as the technical vulnerabilities that were exploited. The model satisfied the objectives of being scalable and applicable to different IW functional areas. The model was also used to relate the IW aspects to the vulnerability assessment framework.

The proposed vulnerability framework was an amalgamation of different frameworks and methods discussed in the literature review. The framework was categorised at a high-level according to a modified SWOT analysis; each of these were divided into factors according to the PESTEL method.

Relevant information sources and methodology types were provided for data gathering; for the specific case of a technical vulnerability analysis, a modified Minimum Essential Information Infrastructure was suggested, which then incorporated technical investigation techniques such as penetration testing and simulations. The information is rated according to a modified FAIR analysis method, where the vulnerability and risk ratings are outputs of process using risk matrices. A mathematical process using vector magnitudes was proposed where the individual risk and vulnerability ratings are used to calculate a single rating for an infrastructure; this can also be used at a national or organisational level.

The vulnerability assessment was applied to the secondary scenario of cloud computing, which was used to perform an initial review of the framework, and the primary focus of the mobile infrastructure. The outcomes of the assessments were consistent with the data and literature. The specific details of the outcomes themselves will be discussed in Sections 9.5 and 9.6.1. The proposed framework satisfied the objectives of being scalable, providing a logical flow through the assessment process from high-level to detailed implementation, and providing the ability to compare vulnerability and risk for different aspects. The structure of the framework was such that it could be adaptable; however this was not implemented in the study.

The proposed model and framework satisfied their objectives, and were successfully implemented in the study for analysis and assessment of various scenarios. This objective of the study was therefore completed.

9.3 Gather Information Relating to Attacks against the Information Infrastructure

An objective of the study was to gather information regarding attacks on the information infrastructure and trends in information warfare and security. Of particular interest are those incidents and trends that relate to South Africa. This information was gathered from documents as presented in Chapter 4 and Chapter 5, and from expert input in the form of interviews and a workshop, presented in Chapter 6. Computer simulations and mathematical calculations were also conducted; these provided a method of feasibility or impact analysis; this was presented in Chapter 7. The gathering of the information was also related to application of the proposed framework, as this data provided the basis for the vulnerability assessment. This also provided the data to establish the criticality of the mobile infrastructure.

At an international level, there is prevalence in attacks that seek to break confidentiality, particularly through system penetration of government or related organisational systems. A number of similar attacks appear to be state sponsored, and target national and international organisations and governments in what appears to be widespread cyber-espionage. The shift of malware to focus on botnets corresponds to the first large-scale DoS attacks that targeted Estonia and Georgia; such attacks have grown in size, where the attacks on Myanmar are reported to have peaked at 14 Gbps. Both espionage and DoS attacks appear to be politically motivated. The prevalence of malware in the CSIRT reports and in the attacks discussed, in addition to reports of a military attempt to develop a rootkit, indicates that the Internet is becoming weaponised. Outcomes from the interviews also highlight concerns over breaches of confidentiality and DoS attacks; however the primary concern was related to lack of user awareness and cyber-crime related activities.

Attacks on mobile devices and the mobile infrastructure follow similar trends; a number of significant attacks, mobile malware, and research in the field of mobile security revolve around the breach of confidentiality. Military use of or attacks on the mobile infrastructure were illustrated; this indicates that the mobile infrastructure is relevant to IW. The threat of mobile malware is growing, and experts are expecting a global pandemic of mobile malware equivalent to the major worms in 2003 and 2004; the concern is that this would deny mobile services as the worms degraded network performance. The outcomes of the interviews also focussed on confidentiality issues. DoS attacks were raised due to the reliance on mobile communications, however no documented record of a DoS attack on the mobile infrastructure was found. General vulnerabilities were a common theme, and malware and awareness were raised. The possibility of a DDoS attack on the mobile infrastructure was raised in the workshop, and the use of mobile devices in penetrating networks. The interview and workshop outcomes therefore corresponded to the documents considered. Social media have also been shown to be a vector for attacks and malware; as before the attacks target confidentiality. The expected availability of social media by employees, and breaches of confidentiality through this medium were raised both in the workshop and the documents considered. The combination of social media and mobile devices played a significant role in many protest actions; and there are reports of intended military use of social media for influence operations, and examples were presented of targeted attacks using social media. This therefore can be considered as a tool that is relevant to IW. The emergence of mobile and social networking technologies has resulted in a convergence of ICTs; this convergence is also seen in the IW sphere, where the overlaps amongst the IW functional areas are increasing. These technologies

and concepts have already begun to impact on IW and information security, and the affects are likely to become more prominent.

Through analysis of the incidents using the IW Lifecycle Model, it can be seen that the context of the IW incident shapes it as much as the technical vulnerabilities and exploits. This supports the models that specifically consider the context, and Armistead's (2010) statement that the broader issues need to be considered. This indicates that high profile, controversial decisions and context may be a good predictor for DoS attacks. Possession of highly valuable information and political alignment in an environment of strong competition could prove a strong predictor for cyber-espionage attacks.

A concern that was prevalent in both the interviews and workshop is the lack of user awareness regarding security issues. This appears particularly relevant to Africa and South Africa; other trends in Africa are high infection rates of malware and high rates of software piracy. The lack of awareness and piracy rates appear to contribute to the high number of infections. The workshop confirmed that these infections are seen, and compromised computers in South Africa have been used as a launching point for attacks. The high infections of botnets could indicate that South Africa is highly vulnerable to DoS attacks from its own information infrastructure. The workshop also confirmed that cyber-based corporate espionage takes place in South Africa, and that social engineering has very high success rates. The political situation in Africa, as well as the internal xenophobic attacks and service delivery riots, may provide motivation for social IW incidents such as those in North Africa. Other political decisions that have attracted international attention, such as denying the Dalai Lama entry (Philp, 2011; South African Press Association, 2009a), and perceived political alignment may also attract attacks from rogue groups and possible other nations. The lack of an operational CSIRT was raised in the documentation considered, the interviews, and the workshop. This contributes to the lack of a big picture regarding the information security incidents in the country, and would make the defence, response, and recovery in the event of a large-scale attack difficult and un-coordinated. South Africa therefore can be seen as being vulnerable to attack, both from within and external aggressors.

9.4 Establish the Criticality of the Mobile Infrastructure

The criticality of the mobile infrastructure needed to be established as it was being treated as part of the national critical information infrastructure. Questions in the interviews provided expert opinion regarding the importance of the mobile infrastructure and its relevance to the critical information

infrastructure. A pilot survey of informal traders in the eThekwini Municipality (Durban and surrounding areas) was conducted to gain an indication of the reliance on the informal businesses on the mobile infrastructure.

From the interviews, the outcomes indicated that the mobile infrastructure should be considered as critical. The majority of responses also indicated there should be specific policies towards protecting the mobile infrastructure; however some considered that existing critical infrastructure protection policies were sufficient. The responses also showed that mobile communications is important to most sectors; however use by government, military, and security or intelligence services should have additional security. The importance and use of mobile communications by criminal groups implies that the infrastructure is critical to security and intelligence services to conduct lawful intercepts. The outcomes of interviews correspond to the reports of incidents, concerns, and roles of mobile security that were discussed in the trend and incident analysis. Of particular note are the military attacks on mobile infrastructure for influence operations, concerns of insurgents accessing military and diplomatic communications by penetrating the infrastructure, and the use of mobile devices in uprisings and the resultant blockage of services indicate that the mobile infrastructure is already relevant to IW, and may play increasingly larger roles in future information conflicts. As many of the demonstrations occurred in Africa, this is of particular relevance to South Africa.

The prevalence and reliance of mobile communications was evident from the literature review, trend analysis, and interviews. The high penetration of mobile phones was seen in a pilot survey was conducted to assess the use of mobile devices by informal traders. However, the results indicated that the traders considered the social use of mobile communications of higher importance than the business use; the indications are that whilst outages of mobile services will have some impact on the traders, they did not view it as critical. The investigation of the reliance of informal traders on mobile communications should be conducted as a future, separate study where all the factors can be assessed in-depth.

The corresponding results from the interviews and documents indicate that the mobile infrastructure is critical, especially in South Africa where there is high reliance on the mobile communications compared to fixed-line telecommunications. The reports relating mobile communications to military activities and mass demonstrations indicates a growing relevance of the mobile infrastructure to IW activities; this corresponds to the effects of modern ICTs on the IW construct discussed in Section 9.3. The reliance of the informal sector on mobile communications should be conducted as future

work where all factors can be assessed in-depth; the results from the pilot indicated that there is some reliance, but mobile communications are perceived as more important for social communications, and not critical for the informal business.

9.5 Application of the Proposed Framework to the Mobile Infrastructure

The proposed vulnerability assessment was applied to a generic national mobile infrastructure. The data gathered was used as the basis of the assessment, which was conducted according to the proposed framework. This assessment is presented in Chapter 8. As discussed in Section 9.2, the outcomes from the assessment corresponded to the data, indicating the results are reliable.

The assessment of the mobile infrastructure rated the threats, vulnerabilities, and risks; from the risks the vulnerabilities were prioritised, and some aspects were compared. The threats were rated according to their prevalence and the overall probability of an attack. In the general context malware, social engineering and system penetrations were rated as high threats and DoS attacks as a medium threat. Threats to the mobile infrastructure that are rated high include: jamming in a conflict zone, infrastructure penetration, malware, and SIM cloning for cyber-crime use. Those rated as medium threat include: mobile and social media malware, SMS DoS from mobile botnets, and both wireless intercept and physical threats in a conflict zone. The use of mobile phones also presents a threat, where those related to leaks and targeted attacks where the device is stolen are rated high; the use of the devices to penetrate networks, for phishing, and distribute hate speech or incite demonstrations are rated as medium.

The vulnerabilities were rated according to the capability required to overcome them, and the effectiveness of the controls that are in place; the most vulnerable areas will be highlighted here. In terms of general, contextual vulnerabilities, two stood out with very high ratings: a lack of user awareness, and vulnerability to DoS attacks. At a national level, the lack of a CSIRT and insufficient legislature are rated as high; poor corporate attitude and general system penetration are also notable vulnerabilities that are rated high. A technical vulnerability of the mobile infrastructure that was rated very high is the apparent high operating load; outages and reports by the regulatory body that the call drop rate is too high and does not meet requirements indicates that the infrastructure may be very susceptible to a DoS attack. Device OS vulnerabilities, susceptibility to jamming, the physical exposure of base stations, and authentication weaknesses allowing SIM

cloning are rated as high. The vulnerability to an information leak in a normal security environment is very high, but is only high in a high security environment. The vulnerability to mobiles subverting network perimeter controls and being used to instigate violence are also rated high. The calculated infrastructure rating for general vulnerabilities is 12.1 out of a possible maximum of 14.14. The rating is 13.93 out of a possible maximum of 22.91 for technical vulnerabilities of the infrastructure, and 8.77 out of 11.18 due to vulnerabilities created by mobile use. From this it can be concluded that there is a significant general vulnerability to attack, and the use of mobile phones do impact on security; the mobile infrastructure vulnerability is high due to the number of vulnerabilities, but they are on average high mid-range vulnerabilities.

The risks rated very high are associated with general vulnerabilities and previously unknown vulnerabilities which are exploited by malware and system penetration and confidentiality is breached and data corrupted. Risks of information leaks or the subversion of perimeter controls by mobile devices are also rated very high. These vulnerabilities should be prioritised to mitigate the vulnerability and risk. Technical vulnerabilities that present a high risk is the interception of wireless network transmissions, vulnerabilities in wireless access points, jamming in a military environment, device vulnerabilities, high operating load, centralisation of infrastructure components, and breaches of confidentiality due to vulnerabilities in mobile enterprise servers. All general vulnerabilities have a high risk associated with them, except for legislative vulnerabilities. The risk ratings are 16.4 out of 21.21 for general vulnerabilities, 27.51 out of 39.69 for technical infrastructure vulnerabilities, and 11.49 out of 13.23 for vulnerabilities due to mobile use. The high risk for the technical vulnerabilities corresponds to the outcome of the study that the mobile infrastructure is critical. The risk ratings for the general vulnerabilities and those due to mobile use indicate that these vulnerabilities can have a significant impact on organisational and national security.

The risk and vulnerability ratings were compared for various aspects. The outcomes of this comparison indicated that breaches of confidentiality posed the greatest risk and had the highest vulnerability rating; mitigating this impact type should therefore be prioritised. Of the technical impacts, corruption of data presented a higher risk than DoS attacks, even though it had the lower vulnerability rating. This is due to the severity of the impacts, which is often coupled with DoS and breaches in confidentiality. The general vulnerabilities were rated lowest for both vulnerability and risk; however these should not be ignored as they may aid in mitigating the technical vulnerabilities and risks. Network warfare presented a higher risk and vulnerability compared to electronic

warfare, and therefore can be considered the more efficient option for a strategic attack on the mobile infrastructure. Should military electronic warfare assets be available in a tactical environment, they will probably be the more efficient. The comparison of threats showed that system penetration presented the highest risk and vulnerability rating, followed by malware. The ratings of social media and mobile malware should be monitored, as they can be expected to increase as these threats grow in prevalence. The comparisons are consistent with the data collected. Suggested solutions and controls to mitigate vulnerabilities are discussed in Section 9.6.2.

The vulnerability and risk assessment indicated that South Africa is vulnerable to attack, and in the current environment, this does present a noticeable risk. In particular, the lack of user awareness poses a large problem, and the negative effects are already being seen. The mobile infrastructure also exhibits a number of vulnerabilities, of which the highest risk is related to the threat of system penetrations of the infrastructure, allowing attackers to monitor communications. The mitigation of general vulnerabilities should be prioritised as this presents a very high risk, and reports presented in the trend analysis indicate that many breaches could have easily been avoided. Network warfare methods can be seen as a high risk to the mobile infrastructure, and confidentiality breach is the highest risk impact; therefore controls mitigating these should be prioritised.

9.6 Secondary Objectives

Secondary objective included the application of the proposed framework to a second infrastructure, and providing possible solutions to mitigate identified vulnerabilities. The application of the framework to a second infrastructure; as part of the initial review of the framework, it was applied to a scenario of cloud computing. The outcomes of the application to the cloud computing scenario is summarised in Section 9.6.1. Potential solutions to vulnerabilities were assessed as part of the data gathering, and are discussed in Section 9.6.2.

9.6.1 Application of the Framework to Cloud Computing

A secondary objective of the study was to apply the proposed framework to another infrastructure in addition to the primary application to the mobile infrastructure. This was provided in Section 4.3.2, where the framework was initially reviewed by applying it to a cloud computing scenario.

The results from the assessment indicated that social engineering and exposure due to mobile devices that can access cloud services posed a very high risk. These vulnerabilities were also rated as high; therefore addressing these issues should be prioritised. Social engineering was also rated

very high as a threat. The vulnerability of different cloud service models was the same; however the risk varied for some impacts types due to their magnitude. Confidentiality presented the highest risk, however it did not have the highest vulnerability rating. Corruption was the second highest risk, but had the lowest vulnerability rating of the three technical impacts. DoS was the lowest risk, but exhibited the highest vulnerability rating. There was a difference between the IaaS and SaaS or PaaS models for the DoS risk rating; the risk was higher for the SaaS and PaaS models due to the increased impact should service be lost. The non-technical factors also presented some risk; this confirmed that the broader context does influence vulnerability and risk.

9.6.2 Possible Solutions to Vulnerabilities

Possible solutions to mitigate vulnerabilities and threats arose from primarily the interviews and workshop. The document analysis also provides some information. The possible solutions were presented as under the opportunities phase of the vulnerability assessment in Section 8.7, and originated from the interviews, workshop, and documents analysed.

Following from the general vulnerabilities, the documents, workshop, and interviews all raised the need for additional legislation, the introduction of a CSIRT, and information security awareness campaigns. The legislation will also aid in forcing organisations into applying information security measures. There was also a suggestion in the workshop that a professional body with oversight of academic degrees and professionals in development and IT security and management to ensure that there is a minimum quality; this will hopefully increase the general quality of information systems and reduce vulnerabilities.

Technical solutions include introducing stricter filtering mechanisms to control mobile device connection to networks and introducing data classification. For the mobile infrastructure specifically, additional shielding could be provided to aid in mitigating the effects of electromagnetic interference (including lightning), increasing redundancy in mobile infrastructure components, and ensuring all servers and components are patched and have the latest anti-virus signatures. Even those systems behind an air-gap need to be patched and protected as the Stuxnet worm managed to transit the air gap. End-to-end encryption of communications should be mandatory in organisations with sensitive or confidential information.

Solutions proposed in this study include the introduction of social media honey pots to investigate attacks through the social networks. This may provide information to aid awareness efforts. Using digital signatures and message digests of mobile applications on the online stores may aid

mitigating legitimate applications being compromised by malware by allowing users to check that they have not been altered. Intrusion detection systems could also be employed on the mobile infrastructure to detect and monitor unusual quantities of requests originating from web-based entities and specific components in the infrastructure. Should there be no real-world reason for the influx of messages, then it could signify a mobile worm outbreak or system penetration.

These solutions originate from the study, and do not provide an exhaustive list. Mitigating the most commonly exploited vulnerabilities will force attackers into finding alternative methods, which at least increase the complexity required for a potential attacker.

9.7 Recommendations

The recommendations from this research follow directly from the opportunities and solutions discussed in Section 8.7 and summarised in Section 9.6.2. Naturally, it is recommended that research in the relevant areas needs to be continued; this is discussed in more detail in Section 9.8. The recommendations presented here focus on those that can be implemented by network providers and organisations to directly mitigate the vulnerabilities and risks.

At a national level, a series of initiatives should be implemented. These include information security awareness campaigns in communities; schools could be targeted to raise awareness of the learners, who could take this back to their communities. There is intent to conduct such projects, as shown by the awareness research conducted by Grobler, Jansen van Vuuren, and Zaaiman (2011). Due to the high penetration of mobile devices and the evolving threats for these devices, there is a need to include these devices in the training in addition to PC-based security. Additional legislature also needs to be implemented; the Protection of Personal Information Bill is yet to be enacted. This legislation will provide excellent support for the existing legislature and standards in South Africa.

A suggestion that arose from the workshop was the further introduction of information security into tertiary computing-related curriculum. The security aspects should be raised for the various topics; however security in the development lifecycle should be stressed. A way of ensuring the introduction of security into the curriculum is, as suggested in the workshop, is to have a professional body oversee and accredit the curriculum; they can also provide for registration of information systems professionals.

The introduction of a CSIRT should be prioritised. Such a facility would provide much needed support to organisations in the country, and provide a central point to co-ordinate responses in the

event of an attack. Such a facility is also crucial to continuing research in the information security and IW areas. Whilst many government CSIRTs keep their information confidential, the high infection rates and low awareness situation in Africa indicates the CSIRTs need to play a more public role. Therefore, should the relevant government CSIRTs or their governing agencies wish to restrict access to the CSIRT services, a second CSIRT should be implemented to respond to general public and organisational issues outside of the government departments.

Infrastructure components need to patched and have the latest security measures. Whilst this should be done for all information-based infrastructures, the focus here will be on the mobile infrastructure. The Stuxnet worm illustrated that even components behind an air gap could be targeted and attacked; and the number of incidents illustrated that the mobile infrastructure can be penetrated. One incident indicated that the communications are only encrypted over the wireless channels. To circumvent this, and end-to-end encryption solution for mobile communications should be introduced for any organisation that requires to transmit or discuss sensitive information over public mobile or network channels. Additional systems should be introduced to monitor unusually high traffic on the mobile networks, with the ability redirect or block the traffic if it is found to be malicious. This can be seen as a mobile equivalent of an intrusion detection system and sinkhole.

Organisations should also introduce measures to mitigate the risk due to the use of mobile devices and related technological concepts, such as cloud computing. Suggestions arising from the workshop are to implement MAC address filtering to mitigate untrusted mobile devices connecting to the wireless networks. Data classification will aid in identifying the protection information requires. Awareness training should also be provided to employees to ensure they have some knowledge of the threats that mobile devices and social networking present to them personally and the organisation. As suggested in Section 5.6, a defence-in-depth approach is often best, where a combination of preventative and detection measures is taken. The preventative measures can be seen as restricting access, installing security applications, and awareness training; detective measures include monitoring of user activity and profiles.

A number of the recommendations are non-technical in nature; this is largely due to the lack of awareness and poor attitude surrounding information security issues. Some technical measures suggested can be easily implemented; others will need to be researched and developed. The following section will propose future research to be conducted.

9.8 Future Research

This section provides suggestions for future research. This follows from the areas identified during the data gathering process of the study and outcomes from the study; some recommendations also require some areas of research covered in this section to be conducted. The primary focus of future research needs to be the continued monitoring and analysis of future IW and security incidents and trends; particularly the impact of evolving technologies on these fields. The evolution of malware, particularly on the mobile and social network platforms, also needs to be monitored and analysed. Whilst the anti-virus and security vendors do this well, some additional academic research is needed to analyse the long-term impacts of malware on society and national economies. For Africa, this research should focus on the possible hindrances malware and the related cyber-crime creates for national economic and social development; if this can be quantified then it may force the relevant governments into taking action to improve their national cyber-security efforts.

As suggested from the pilot survey, the reliance of informal traders on mobile communications should be researched in depth. This can also be expanded to all business sectors, from the micro-enterprise level to the large corporations. This may give an indication of the national economic reliance on mobile communications; similar research for traditional fixed-line telecommunications and web-based communications will allow for the comparison of the economic and social importance of ICTs in the country.

The continued research in the information warfare and security areas to develop new defensive measures to protect infrastructure and information should continue. The research in South Africa should expand on the current IW areas to information operations, which can be seen as an extension to IW. A taxonomy needs to be developed in addition to the frameworks for implementing information operations across the military and government. The difficulties regarding political mandate that has hindered the development of a CSIRT may also hinder the introduction of full spectrum information operations across the military, government departments, and other agencies.

An important area of research will be the development and introduction of dedicated information security degrees and diplomas at tertiary institutions. These need to be researched carefully and catered to the current requirements of industry for them to be viable. The graduates need to gain the relevant experience and knowledge that is required in industry from these degrees to give them a high chance of being employed; industry buy-in for such programmes will also be required. Unique teaching and learning methods and their effectiveness, which may include technological tools, will

also need to be researched to improve the quality of the degree offerings as well as the resultant graduates.

An interesting point to research is the possible roles that the Tunisian and Egyptian CSIRTs played during the unrest in those countries. A concern was raised in the interview that CSIRTs could be used to block access to the internet and other communications technologies. At the time of this study, not enough information was available to assess if the CSIRTs did contribute to the government response to the unrest. This should be research if more information becomes available.

By conducting the suggested research at academic institutes across South Africa, further insight will be gained that will aid in improving the information security landscape in the country. This will in turn improve the economic and social impact of evolving technologies.

9.9 Conclusion

Three modern ICT concepts have been considered to various extents in this thesis: mobile communications, Web 2.0, and cloud computing; where the focus has been on mobile communications. These technologies exhibit their own vulnerabilities, and introduce vulnerabilities and threats into the information infrastructures. These new technologies also appear to impact on the IW constructs; as the technology converges, so do the IW functional areas.

The thesis proposed a descriptive IW model and a vulnerability assessment framework. The proposed IW lifecycle model was used to analyse a number of incidents; this analysis supported the views that context is important in IW, as this provides the reason and motivation for attacks. Therefore non-technical vulnerabilities may be equally as important as the technical vulnerabilities which are exploited during the attack. The proposed vulnerability framework provided the direction for the data gathering in the thesis. The framework was applied to a scenario of cloud computing, but the focus was on the application to the mobile infrastructure.

The results of the assessment indicated that South Africa is vulnerable to cyber-based attacks; these vulnerabilities present a high risk to the nation. It was shown that the mobile infrastructure is critical or important to all sectors; therefore it needs to be afforded protection from potential attack. The assessment results indicated that the mobile infrastructure is also vulnerable to attack, and that malware and system penetration exploiting general vulnerabilities presents the highest risk to the infrastructure. A serious vulnerability is the apparent high operating loads, which result in the infrastructure being susceptible to DoS attacks. Breaches of confidentiality present the highest risk,

and network warfare techniques appear to be the most effective at a strategic level against the mobile infrastructure. The results of the assessment correspond to the gathered data, indicating reliability.

The gathered data indicates that system penetrations to breach the confidentiality of sensitive information appear to be the most prevalent attack. The evolution of malware to the botnet form corresponds to the evolution of large-scale DDoS attacks; these may become more prevalent should the number of infected systems increase. However, the primary focus of malware appears to be accessing account login details for financial cyber-crime purposes. The use of malware in cyber-espionage attacks and in attacks on infrastructure, indicate that the Internet is becoming increasingly weaponised. Attacks on the mobile infrastructure also focussed on confidentiality breaches; however some military attack were aimed at distributing psychological operations messages. The threat of mobile malware is also evolving rapidly, and it may not be long before pandemics are seen that seriously degrade the mobile services. Social media sites have also been seen to be used to distribute malware, amongst other attacks. The combination of social media and mobile devices were instrumental in the initial phases of mass anti-government demonstrations. From a South African perspective, a lack of user awareness and software piracy are contributing to high rates of malware infection and general vulnerabilities in the country and its neighbours. From various aspects, there is a vulnerability to attack, and an increase in cyber-crime activity is expected. A large-scale attack is not expected; however controversial political positions may attract aggressive attention. As a large proportion of the demonstrations took place in Africa, this is of particular relevance to South Africa, where a number of xenophobic attacks and service delivery riots have been experienced. This may be used to the advantage of an attacker, and also heightens the political tension in the region.

It is recommended that measures be taken nationally to improve the context of information insecurity in South Africa: the introduction of awareness campaigns and a CSIRT should be prioritised, and the supporting legislature should also be in place. A stronger presence of security in the computer-based modules at tertiary institutions was also suggested. In the mobile infrastructure all systems should be fully protected, there should be redundancy in the infrastructure, and additional measure should be developed and introduced to detect and protect against attacks. Organisations also need to introduce new, and possibly stricter, security measures to mitigate the threats and vulnerabilities posed by social media and mobile devices. Suggested future research includes the continuation of general research in the information warfare and security areas, and

specifically monitoring incidents and trends. Quantifying the importance of the mobile infrastructure to the national economy and society is also an important area of future research.

The primary and secondary objectives of the study were met; the IW model and vulnerability assessment were proposed and applied. Information was gathered regarding the cyber-environment in terms of attacks and incident trends. The mobile infrastructure was shown to be critical, and possible vulnerabilities in a generic mobile infrastructure were assessed. Broader contextual vulnerabilities were also assessed, and this indicates that South Africa is vulnerable to cyber-attack.

Appendix A. Research Output

A.1 Peer Reviewed Journals

van Niekerk, B., & Maharaj, M. (2009c). The Future Roles of Electronic Warfare in the Information Warfare Spectrum. *Journal of Information Warfare,* 8(3) , pp. 1-13.

van Niekerk, B., Pillay, K., & Maharaj, M. (2011). Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective. *International Journal of Communication*, 5(1), pp. 1406-1416.

van Niekerk, B., & Maharaj, M. (2011c). Relevance of Information Warfare Models to Critical Infrastructure Protection. *Scientia Militaria*, 39(2), pp. 99-122.

van Niekerk, B., & Maharaj, M. (2011d). The IW Life Cycle Model. *The South African Journal of Information Management*, 13(1), available online at: http://www.sajim.co.za/index.php/SAJIM/article/view/476.

A.2 Book Chapter

van Niekerk, B., & Maharaj, M. (c. 2012). A South African Perspective on Information Warfare and Cyber-Warfare. In Ventre, D. (ed.). In press.

A.3 Peer Reviewed Conferences

van Niekerk, B., & Maharaj, M. (2010a). Information as a Strategic Asset in an Asymmetric Unconventional Conflict. *International Conference on Information Management and Evaluation*, pp. 413-421. Cape Town, 25-26 March: Academic Conferences International.

van Niekerk, B., & Maharaj, M. (2010b). Mobile Security from an Information Warfare Perspective. *9th Information Security South Africa Conference.* Sandton, 2-4 August.

van Niekerk, B., & Maharaj, M. (2010c). Weaponisation of the Net. *12th Annual Conference on World Wide Web Applications (ZA-WWW).* Durban, 21-23 September.

Pillay, K., van Niekerk, B., & Maharaj, M. (2010). Web 2.0 and its Implications for the Military. *Workshop on the Uses of ICT in Warfare and the Safeguarding of Peace*, pp. 50-57. Bela-Bela, 11 October: Council for Scientific Research.

van Niekerk, B., & Maharaj, M. (2011a). Infrastructure Vulnerability Analysis from an Information Warfare Perspective. *South African Computer Lecturer's Association (SACLA 2011)*, pp. 76-85. Durban.

van Niekerk, B., & Maharaj, M. (2011b). Mobile Malware Trends. *Business Management Conference*. 28-29 September, Durban.

A.4 Other Conferences

van Niekerk, B., & Maharaj, M. (2009a). The Future Roles of EW in IW. *Big Crow Conference.* Pretoria, 5-26 August: Association of Old Crows Aardvark Roost.

van Niekerk, B., & Maharaj, M. (2009b). Information Operations Education for South Africa. *3rd Annual Teaching and Learning Conference*, pp. 206-224. Durban, 21-23 September: University of KwaZulu-Natal.

van Niekerk, B., Ramluckan, T., & Maharaj, M. (2011). Web 2.0 as an Attack Vector against Strategic Security. 5th *Military Information and Communications Symposium South Africa*. Pretoria, 18-22 July.

A.5 Other Output

van Niekerk, B. (2010a). Vulnerability Assessment of Modern ICT Infrastructure from an Information Warfare Perspective. School of Information Systems and Technology Seminar Series.

van Niekerk, B. (2010b). Safety and Security on the Net. *TEDx UKZN.* Durban, 14 May.

van Niekerk, B. (2010c). Information Warfare. *Durban Whitehat Advisory.* Durban, 17 June.

A.6 Output Related to the Thesis (but not directly from it)

van Niekerk, B. (2009). Interoperability in EW and CNO: Considerations for the African Continent. 4th *Military Information and Communications Symposium of South Africa.* Pretoria, 20-24 July.

Ramluckan, T., & van Niekerk, B. (2009a). The Role of the Media in Joint Operations. 4th *Military Information and Communications Symposium South Africa.* Pretoria, 20-24 July.

Ramluckan, T., & van Niekerk, B. (2009b). The Terrorism/Mass Media Symbiosis. *Journal of Information Warfare* 8(2), pp. 1-12.

Appendix B. Reference Matrix

Table B.1: Reference Matrix for Selected References

References	Information Warfare and Security	Network Warfare	Electronic Warfare	Infrastructure Warfare and Protection	Vulnerability and Risk Assessment	Incident Analysis	Economic and Social Impact	Technical Infrastructure	Application
Adams (1998)	✓					✓			
Adamy (2009)			✓						✓
Anderson *et al*. (1999)				✓	✓				
Armistead (2010)									✓
Arquilla & Ronfeldt (2001)	✓	✓					✓		
Boehm (1991)					✓				
Borden (1999)	✓								
Brazzoli (2007)	✓								
Busuttil & Warren (2002)				✓					
Carr (2010)	✓	✓							
Critical Infrastructure Assurance Office (2000)				✓	✓	✓			
Cronin & Crawford (1999)	✓						✓		
Defense Science Board (1996)		✓		✓					
Denning (1999)	✓	✓			✓	✓			
Department of Homeland Security (2009)				✓					
Dwivedi, Clark & Thiel (2010)						✓		✓	✓
Dudgeon (2008)				✓					
Elky (2006)					✓				
Enck *et al*. (2005)		✓						✓	✓
Erbschloe (2001)	✓						✓		
Gollman (2011)	✓	✓							
Gostev (2006a)						✓			✓
Gostev & Maslennikov (2009)						✓			✓
Habegger (2008)					✓				

References	Information Warfare and Security	Network Warfare	Electronic Warfare	Infrastructure Warfare and Protection	Vulnerability and Risk Assessment	Incident Analysis	Economic and Social Impact	Technical Infrastructure	Application
Hefer & Theron (2009)	✓								
Howard (1997)		✓				✓			
Hutchinson & Warren (2001)	✓	✓		✓	✓	✓			
Hyppönen (2010)						✓			✓
Hyppönen & Sullivan (2010)						✓			✓
Jones (2005)					✓				✓
Jones, Kovacich, & Luzwick (2002)	✓	✓		✓		✓			
Kopp (March 2000)	✓								
Libicki (1995)	✓								
Macaulay (2008)				✓					
Molander *et al.* (1996)	✓			✓	✓		✓		
Molander *et al.* (1998)	✓			✓	✓		✓		
Morales (2009a)						✓			✓
Morales (2009b)						✓			✓
Moteff & Parformack (2004)				✓					
Nicholson (1998)			✓					✓	✓
Nickolov (2005)					✓				
Parker (2002)	✓								
Peltier, Peltier & Blackley (2005)	✓				✓				
Pfleeger & Pfleeger (2003)	✓				✓				
Poisel (2004)			✓						✓
Schwartau (1996)	✓	✓		✓			✓		
US Air Force (1998)	✓	✓	✓						
vanRooyen (2009)						✓	✓		
Veerasamy & Eloff (2008)		✓		✓		✓	✓		
Ventre (2009)	✓	✓		✓		✓			
Waltz (1998)	✓	✓		✓					

References	Information Warfare and Security	Network Warfare	Electronic Warfare	Infrastructure Warfare and Protection	Vulnerability and Risk Assessment	Incident Analysis	Economic and Social Impact	Technical Infrastructure	Application
Ware (1998)		✓	✓	✓			✓		
Wenger, Metzger & Dunn (2002)					✓				✓
Whitman & Mattord (2010)	✓				✓				
Wik (2002)	✓				✓				

Appendix C. Communications Theory

This appendix describes the background to communications theory. The explanations presented are to facilitate understanding of concepts in radio communications to those who do not have experience in the field; therefore the explanations may not be presented in a manner generally accepted as technically correct by the discipline. The explanations are also inclined more towards the estimations used in electronic warfare, as described by Adamy (2009), than pure radio communications. Section C.1 describes the mathematics of decibel calculations, and Section C.2 describes the propagation of radio waves. The measures of performance that are relevant to this dissertation are described in Section C.3.

C.1 Decibel Mathematics

Many terms in communications theory are ratios, such as a signal-to-noise ratio (SNR) or a jamming-to-signal ratio (JSR). These ratios are presented in decibel form, and can be calculated as follows (Taub & Schilling, 1991):

$$K = 10 \log_{10} \frac{S}{N} \quad \textbf{A.1}$$

If S=100 and N=5, then the ratio S/N = 20, and K becomes 13dB. In electronic warfare calculations, when most values are represented in decibel format, output powers also need to be converted. The unit for this is the dBm, which is normalised to one milliwatt (or in a ratio to 1mW); the equation is therefore (Adamy, 2009):

$$K = 10 \log_{10} P \quad \textbf{A.2}$$

If P=100W, then we calculate K for P=100000mW, which gives K=50dBm. Gains are effectively ratios between the input and output, and are also expressed in the decibel format. A loss can be considered as a gain less than one, or a negative gain in decibel form.

C.2 Radio Wave Propagation

As radio waves propagate, they can be reflected off obstructions and the ground. They are also subject to interference, called noise, from the environment, which may result in errors in the reception of digital signals. Shannon's Theorem (Shannon, A Mthematical Theory of Communications, 1948) states that the noise limits the capacity of information that a communications channel can carry; this is presented in Section 2.2. There are multiple models that

describe the propagation of radio waves; these generally calculate the energy loss as the radio wave propagates through the environment (Poisel, 2004). In extremely built-up environments, radio signals may reflect off many objects, in some cases there may not be a direct signal between the transmitter and receiver. These reflections may result in multiple versions of the same transmitted signal being received, not necessarily at the same time, and the path of each reflected version of the transmitted signal may experience different degradation (or enhancement); this is known as multipath fading (Poisel, 2004).

Interference may come from many sources; the local temperatures create noise in the antenna, known as thermal noise. Celestial bodies may also contribute to interference (Poisel, 2004); solar flares sometimes cause outages of both satellite and terrestrial communications. The overall external noise that interferes with a radio signal is usually modelled on statistical probability densities, such as a Gaussian probability density (Taub & Schilling, 1991). As the noise interferes with the radio signal, the quality of the signal can be described by the ratio of the signal strength to the strength of the noise; this is known as the signal-to-noise ratio (SNR); the equation to calculate the SNR in decibels is presented in Section C.1.

Depending on the distance between the transmitter and receiver, the height of the antennas, and the frequency, the communications signal may reflect off the ground resulting in two signals being received. This is known as two-ray propagation, occurs when the distance between the transmitter and receiver is greater than the Fresnel Zone; if the distance is less than the Fresnel Zone, then line of sight propagation occurs (Adamy, 2009; Poisel, 2004). Equation 2.5 in Section 2.5.4.1 determines the Fresnel Zone. Each propagation method experiences different losses, Equations 2.6 and 2.7 determine the signal loss.

Modulation is required to transmit information by radio waves. The radio wave is transmitted at a specific frequency; very often this does not correspond to the frequencies of the human voice or of digital data. The radio signal is then modified to carry the original signal (voice or data) at its frequency. Many modulation schemes are available for both analogue and digital transmissions; the explanation of these schemes does not fall into the scope of this study. In digital communications the noise experienced through transmission may result in errors when the signal is demodulated; this is described in more detail in Section C.3.

C.3 Performance Measures of Communications Systems

The function of a communications system is to transfer information from one location to another; its performance is how well this is achieved. The quality of a digital communications signal is measured by the BER, or probability of error (Adamy, 2009), which is a ratio of the number of bits in error to the total number of bits received. This is related to the SNR or JSR, as the interference is what introduces errors in the signal demodulation. The lower the BER, the better the signal quality; therefore the lower the BER for lower SNRs indicates better performance of the communications system or channel. The point of jamming is to render a signal unreadable by increasing the noise and introducing errors; generally if a third of the bits are in error the signal becomes unreadable (Adamy, 2009). As the intention of jamming is to increase the number of errors, an increase in the BER for a lower JSR indicates better jammer performance.

Usually the performance of a communications channel is represented graphically as the BER versus the SNR; for jamming it is the BER versus the JSR. If one needs to measure the impact of a specific parameter of performance, the graph will be of the BER versus the parameter; the BER (or other measure of performance) is the dependant variable. These graphs usually are semi-log graphs, where the BER (the dependant variable on the y-axis) is represented on the logarithmic scale.

Appendix D. Simulation Flow Diagrams

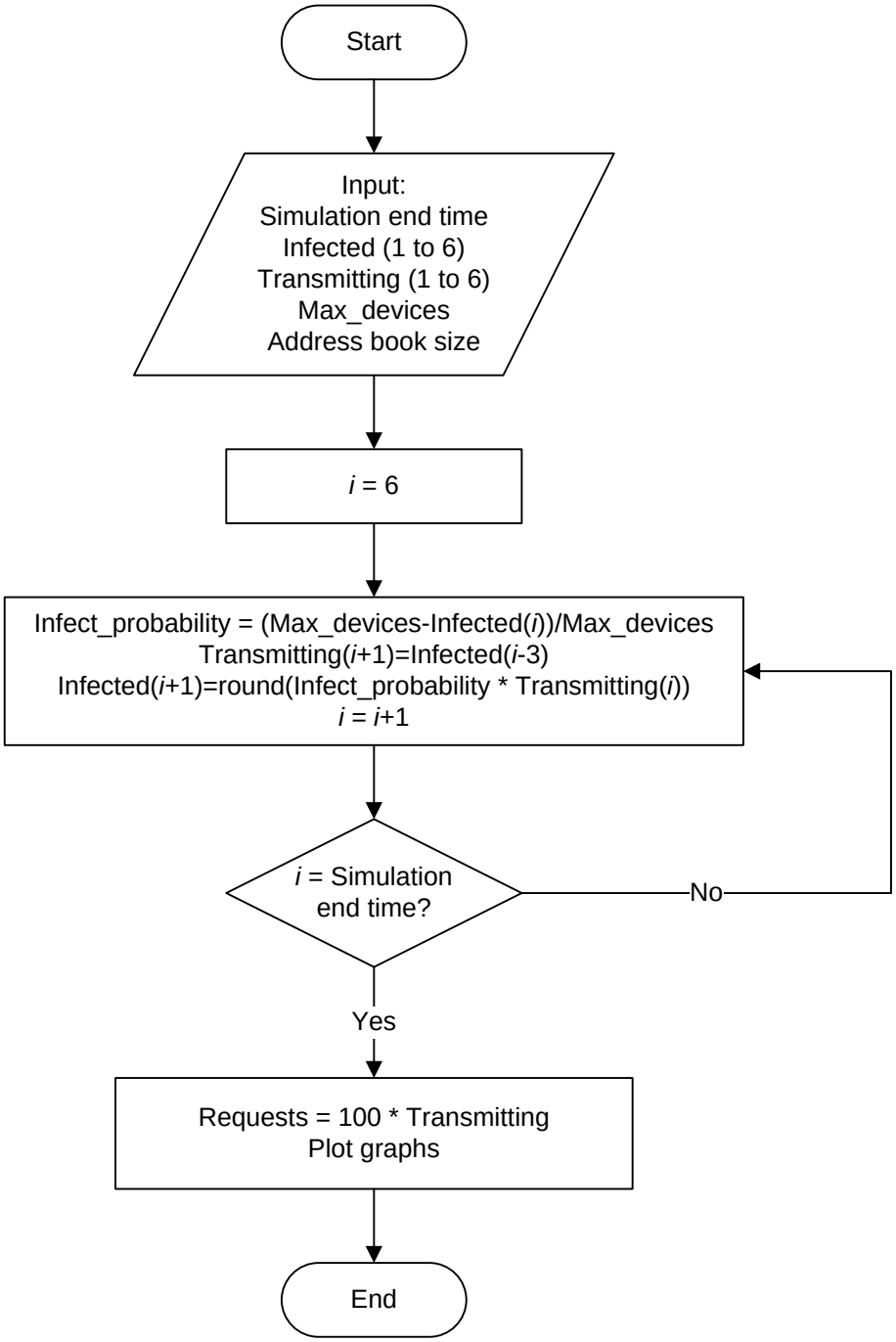


Figure D.1: Beselo Propagation Simulations Flow Diagram

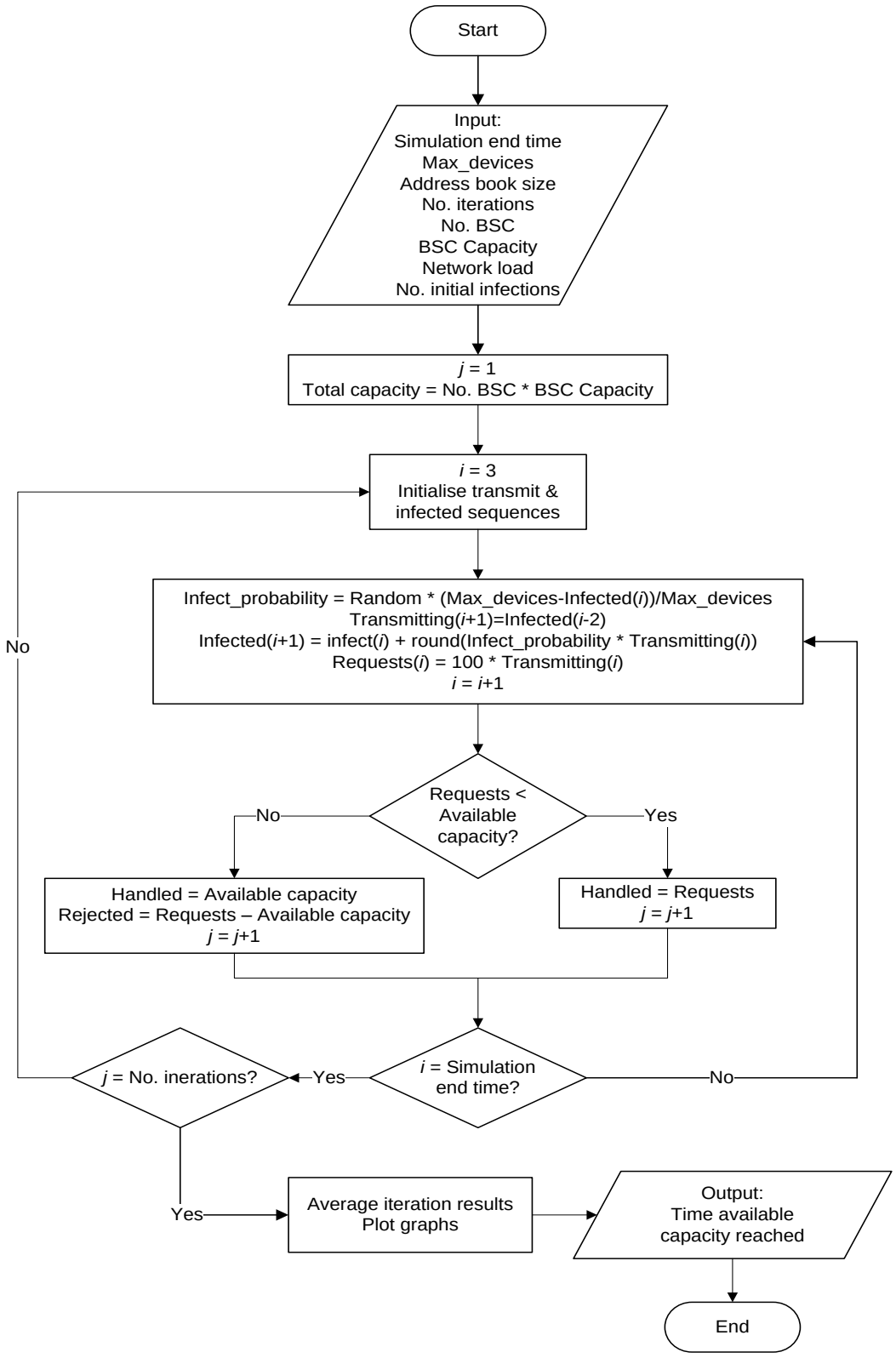


Figure D.2: Hypothetical Worm Propagation Simulations Flow Diagram

Appendix E. Interview Gatekeeper's Letter

To Whom It May Concern:

PERMISSION TO CONDUCT RESEARCH AS PART OF THE PHD RESEARCH DEGREE

Name: Brett van Niekerk

Student No: 991160530

Project Topic: Vulnerability Analysis of Modern ICT Infrastructure from an Information Warfare Perspective

As part of the research, the student is interviewing professionals in the field to gain both South African and international perspectives on issues in critical information infrastructure protection and information warfare. One or more of these professionals that have been identified are members of your organization.

Your assistance in permitting access to your organization for purposes of this research is most appreciated. Please be assured that all information gained from the research will be treated with the utmost circumspection. Confidentiality and anonymity will be strictly adhered to by the student. Interview candidates will not be required to answer questions that may refer to sensitive information, and may withdraw from the process at anytime should they choose, without any consequences to themselves or the organisation.

If permission is granted then UKZN requires this to be in writing on a letterhead and signed by the relevant authority.

Many thanks for your assistance in this regard.

Appendix F. Interview Letter of Informed Consent

Dear Respondent,

PhD Research Project

Researcher: Brett van Niekerk (Tel: 031 260 8521; email: 991160530@ukzn.ac.za)

Supervisor: Prof MS Maharaj (Tel: 031 260 8023; email: maharajms@ukzn.ac.za)

Research Office: Ms P Ximba 031-2603587

I, Brett van Niekerk, am a PhD student at the School of Information Systems and Technology, of the University of KwaZulu-Natal. You are invited to participate in a research project entitled "Vulnerability Analysis of Modern ICT Infrastructure from an Information Warfare Perspective". The aim of this study is to develop a framework for assessing vulnerabilities and associated risks in modern day ICT infrastructures, particularly in a South African context.

Through your participation I hope to gain a perspective of the state of play of critical information infrastructure protection in South Africa in an international context, and the applicability of mobile phones to the concept of a critical information infrastructure. The result of the interview is intended to contribute to placing critical information infrastructure in context, and establishing the criticality of the cell phone infrastructure.

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Information Systems and Technology, UKZN.

If you have any questions or concerns about the interview or about participating in this study, you may contact me or my supervisor at the numbers listed above.

Sincerely

Investigator's signature_____ Date_____

This page is to be retained by participant.

PhD Research Project

Researcher: Brett van Niekerk (Tel: 031 260 8521; email: 991160530@ukzn.ac.za)

Supervisor: Prof MS Maharaj (Tel: 031 260 8023; email: maharajms@ukzn.ac.za)

CONSENT

I_____(full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire.

SIGNATURE OF PARTICIPANT DATE

_____ _____

This page is to be retained by researcher.

Appendix G. Survey Questionnaire

UNIVERSITY OF KWAZULU-NATAL
School of Information Systems and Technology

PhD Research Project
Researcher: Brett van Niekerk031 260 8521
Supervisor: Prof MS Maharaj031 260 8023

Research Office: Ms P Ximba 031-2603587

Use of Communications Technologies

The purpose of this survey is to solicit information regarding the use of cell phones, telephones and email/Internet for business and social activities. The information and ratings you provide us will go a long way in helping us identify the importance of cell phones to the informal economy. The questionnaire should only take 10-15 minutes to complete. In this questionnaire, you are asked to indicate what is true for you, so there are no "right" or "wrong" answers to any question. Work as rapidly as you can. If you wish to make a comment please write it directly on the booklet itself. Make sure not to skip any questions. Please tick the applicable box. Thank you for participating!

Section 1: Demographic and business information

This section is for statistical purposes only, and will not be used to identify or contact you in any way.

1. Age	Under 20	21-40	41-60	Over 60	Prefer not to answer

2. Race	African	Indian	Coloured	White	Other

3. Gender	Male	Female	Prefer not to answer

4. How many employees do you have?	No	No – it is a family business	Yes

5. How many customers do you serve per day?	Less than 20	21-50	51-75	76-100	More than 100

6. What do customers usually spend each visit?	Less than R10	R10-R50	R51-R75	R76-R100	More than R100

7. How much do you spend per day on your cell phone?	Less than R10	R10-R20	R21-R50	R50-R100	More than R100

Section 2: Investigation of accessibility, usage and reliance

This section investigates the access to, usage of and reliance on cell phones, landlines, the Internet and emails. Please tick the most relevant option:

	I do not have access	I have my own	I borrow from someone else	I use a public or community one
8. How do you access a cell phone?				
9. How do you access a landline telephone?				
10. How do you access the Internet?				
11. How do you access emails?				

Please tick the most relevant option:

	I do not have access to this	For my business	For private reasons
12. I mostly use cell phones for:			
13. I mostly use landline telephones for:			
14. I mostly use the Internet for:			
15. I mostly use emails for:			

Please tick the most relevant option:

	It does not require this	No difficulty	Small difficulty	Very difficult
16. How difficult would it be to conduct your business without a cell phone?				
17. How difficult would it be to conduct your business without a landline telephone?				
18. How difficult would it be to conduct your business without Internet access?				
19. How difficult would it be to conduct your business without email access?				

Please tick the most relevant option:

	I do not have access	Never	Less than once a week	A few times a week	Every-day	More than once a day
20. How often do you use a cell phone to make calls for your business?						
21. How often do you use a cell phone to make calls for private reasons?						
22. How often do you use the SMS function for business purposes?						
23. How often do you use the SMS function for private reasons?						
24. How often do you use a cell phone to use mobile money (M-PESA etc)?						
25. How often do you use a landline telephone for your business?						
26. How often do you use a landline telephone for private reasons?						
27. How often do you use email for your business?						
28. How often do you use email for private reasons?						
29. How often do you use the Internet for your business?						

30. How often do you using the Internet for private reasons?						

Please tick the most relevant option:

	I do not use this for my business	No affect	Small affect	Badly affected
31. How badly will your business be affected if the cell phones stopped working?				
32. How badly will your business be affected if the landline telephones stopped working?				
33. How badly will your business be affected if the Internet stopped working?				
34. How badly will your business be affected if the emails stopped working?				

End of the Questionnaire

Thank you for taking the time to complete the questionnaire.

Appendix H. Survey Letter of Informed Consent

Dear Respondent,

PhD Research Project

Researcher: Brett van Niekerk (Tel: 031 260 8521; email: 991160530@ukzn.ac.za)

Supervisor: Prof MS Maharaj (Tel: 031 260 8023; email: maharajms@ukzn.ac.za)

Research Office: Ms P Ximba 031-2603587

I, Brett van Niekerk, am a PhD student at the School of Information Systems and Technology, of the University of KwaZulu-Natal. You are invited to participate in a research project entitled "Vulnerability Analysis of Modern ICT Infrastructure from an Information Warfare Perspective". The aim of this study is to develop a framework for assessing vulnerabilities and associated risks in modern day ICT infrastructures, particularly in a South African context.

Through your participation I hope to gain a perspective of the importance of cell phones in business. The result of the survey is intended to contribute to estimate the economic impact of cell phone service disruptions.

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Information Systems and Technology, UKZN.

If you have any questions or concerns about completing the questionnaire or about participating in this study, you may contact me or my supervisor at the numbers listed above.

Sincerely

Dear Respondent,

Investigator's signature_____ Date_____

This page is to be retained by participant.

PhD Research Project

Researcher: Brett van Niekerk (Tel: 031 260 8521; email: 991160530@ukzn.ac.za)

Supervisor: Prof MS Maharaj (Tel: 031 260 8023; email: maharajms@ukzn.ac.za)

CONSENT

I_____(full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire.

SIGNATURE OF PARTICIPANT DATE

_____ _____

This page is to be retained by researcher.

Appendix I. Proposal Acceptance

Approval of Proposal by the Higher Degrees & Research Committee

5 October 2009

Student Name: B Van Niekerk Student No: 991160530

Qualification: PhD (IS&T) Supervisor: Prof MS Maharaj

Dear B Van Niekerk

This letter confirms that your proposal, titled 'Vulnerability analysis of modern ICT infrastructure from an information warfare perspective.' was approved by the Higher Degrees Panel on the 01 October 2009.
The decision will be placed on the agenda of the next Higher Degrees & Research Committee meeting to be held on 12 October 2009.This will also been recorded at the Faculty Board meeting to be held on 20 October 2009.
Then committee made the following comments:

- Concern that the scope of the research has to be confined.
- Confine and consolidate on the most promising fields

A copy of this letter and the minutes will be placed in your file.

Yours sincerely

Christel Haddon
Post Graduate Administrator
Faculty of Management Studies

Faculty of Management Studies, Westville Campus
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260-1583 Facsimile: +27 (0) 31 260-1312 E-mail: haddonc@ukzn.ac.za
Founding Campuses: Edgewood Howard College Medical School Pietermaritzburg Westville

Appendix J. Ethical Clearance

I.1 Provisional Ethical Clearance

UNIVERSITY OF
KWAZULU-NATAL
University of KwaZulu-Natal
Research Office
Govan Mbeki Centre
Westville Campus
University Road
Chiltern Hills
Westville
3629
South Africa
Tel No: +27 31 260 3587
Fax No: +27 31 260 2384
E-mail : naidoos4@ukzn.ac.za

12 December 2009

Mr B van Niekerk
3 Beaconsfield Road
WESTVILLE
3639

Dear Mr van Niekerk

PROTOCOL: Vulnerability Analysis of Modern ICT Infrastructure from an Information Warfare Perspective
ETHICAL APPROVAL NUMBER: HSS/0967/2009: Faculty of Management Studies

In response to your application dated 20 November 2009, Student Number: **991160530** the Humanities & Social Sciences Ethics Committee has considered the abovementioned application and the protocol has been given **PROVISIONAL APPROVAL.** On receipt of gatekeeper permission your application will be granted full approval.

PLEASE NOTE: Research data should be securely stored in the school/department for a period of 5 years.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

Professor Steve Collings (Chair)
HUMANITIES & SOCIAL SCIENCES ETHICS COMMITTEE

SC/sn

cc: Prof. M Maharaj
cc: Mrs C Haddon

I.2 Final Ethical Clearance

UNIVERSITY OF
KWAZULU-NATAL
University of KwaZulu-Natal
Research Office
Govan Mbeki Centre
Westville Campus
University Road
Chiltern Hills
Westville
3629
South Africa
Tel No: +27 31 260 3587
Fax No: +27 31 260 2384
E-mail : naidoos4@ukzn.ac.za

17 May 2010

Mr B van Niekerk
3 Beaconsfield Road
WESTVILLE
3639

Dear Mr van Niekerk

PROTOCOL: Vulnerability Analysis of Modern ICT Infrastructure from an Information Warfare Perspective
ETHICAL APPROVAL NUMBER: HSS/0967/2009: Faculty of Management Studies

In response to your application dated 20 November 2009, Student Number: **991160530** requiring Gatekeeper's permission which has been received on 13 May 2010, the Humanities & Social Sciences Ethics Committee has considered the abovementioned response and the protocol has been given **FULL APPROVAL.**

PLEASE NOTE: Research data should be securely stored in the school/department for a period of 5 years.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

Professor Steve Collings (Chair)
HUMANITIES & SOCIAL SCIENCES ETHICS COMMITTEE

SC/sn

cc: Prof. M Maharaj
cc: Mrs C Haddon

References

Abrams, M., & Weiss, J. (2008, July 23). *Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia.* Retrieved December 30, 2010, from Computer Security Resource Centre, National Institute of Standards and Technology: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

Ackerman, S. (2010, October 29). *Special Forces Want Android Apps for Warzone 'John Maddens'*. Retrieved October 29, 2010, from Wired.com DangerRoom: http://www.wired.com/dangerroom/2010/10/special-forces-want-android-apps-for-warzone-john-maddens

Ackerman, S. (2011, January 14). *Tweet Away, Troops: Pentagon Won't Ban Social Media*. Retrieved January 17, 2011, from Wired.com DangerRoom Blog: http://www.wired.com/dangerroom/2011/01/tweet-away-troops-pentagon-wont-ban-social-media/

Adams, J. (1998). *The Next World War.* London: Arrow Books.

Adams, J. (2001). Virtual Defence. *Foreign Affairs* 80(3), 98-112.

Adamy, D. L. (2004). *EW102: A Second Course in Electronic Warfare.* Boston & London: Artech House.

Adamy, D. L. (2009). *EW103: Tactical Battlefield Communications Electronic Warfare.* Boston & London: Artech House.

Adamy, D. L. (2011). ES vs. SIGINT. *Journal of Electronic Defense* 34(1), 42-43.

Adhikari, R. (2009, August 13). *Another Day, Another DDoS Blitz for Twitter*. Retrieved September 9, 2009, from E-Commerce Times: http://www.ecommercetimes.com/story/67851.html#

Adkins, B. N. (2001, April). The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcements Role? Maxwell Air Force Base: Air Command and Staff College Air University.

AFP. (2011, September 9). *US Military Plane Forced Down by North Korean Electroni Attack*. Retrieved September 15, 2011, from My Fox NY: http://www.myfoxny.com/dpp/news/us-military-plane-forced-down-by-north-korean-electronic-attack-20110909-ncx

Ajam, K., & Bailey, C. (2009, May 30). Cellphone Chaos Fears. *The Independent on Saturday*, 1.

Ajoku, P. (2009). Information Warfare: Survival of the Fittest. In J. Gupta, & S. Sharma, *Hanbook of Research on Information Security and Assurance* (pp. 18-28). Hershey & New York: Information Science Reference.

Aker, J. C., & Mbiti, I. M. (2010). *Mobile Phones and Economic Development in Africa - Working Paper 211*. Retrieved February 21, 2011, from Center for Global Development: http://www.cgdev.org/files/1424175_file_Aker_Mobile_wp211_FINAL.pdf

Alperovitch, D. (2011). *Revealed: Operation Shady RAT.* Santa Clara, California: McAfee.

Amazon. (2011). *Amazon Elastic Compute Cloud (Amazon EC2)*. Retrieved October 12, 2011, from Amazon Web Services: http://aws.amazon.com/ec2/

Anderson, R. H., Feldman, P. M., Gerwehr, S., Houghton, B., Mesic, R., Pinder, J., et al. (1999). *Securing the US Defense Information Infrastructure: A Proposed Approach.* Santa Monica: RAND Institute.

Armistead, L. (2010). *Information Operations Matters.* Potomac Books: Washington, D.C.

Arquilla, J., & Ronfeldt, D. (1996). *The Advent of Netwar.* Santa Monica: RAND Corporation.

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is Coming! In J. Arquilla, & D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 23-60). Santa Monica: RAND Corporation.

Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica: RAND.

Asquin, H. (2009, October 8). *Somail pirates attack French military flagship.* Retrieved October 12, 2009, from InSing.com: http://www.insing.com/news/international/Somali-pirates-attack-French-military-flagship/id-84870100?nav=60000

Associated Press. (2010, March 4). *Mastermind of World's Worst Computer Virus Still at Large*. Retrieved October 6, 2010, fromFox News: http://www.foxnews.com/scitech/2010/03/04/mastermind-worlds-worst-virus-large/

Barnett, E. (2010, July 5). *YouTube Hacked With Pop Singer Justin Bieber as a Target*. Retrieved July 6, 2010, from The Telegraph: http://www.telegraph.co.uk/technology/google/7872824/YouTube-hacked-with-pop-singer-Justin-Bieber-as-a-target.html

Bay, A. (2011, Januray 18). *Tunisia's Remarkable Revolt*. Retrieved January 19, 2011, from Strategy Page On Point Blog: http://www.strategypage.com/on_point/20110118224752.aspx

BBC. (2005, November 17). *More Pain for Sony over CD Code*. Retrieved October 11, 2011, from BBC News: http://news.bbc.co.uk/2/hi/technology/4445550.stm

BBC. (2008, May 21). *SA Leader Orders Army to Deploy*. Retrieved September 18, 2011, from BBC News: http://news.bbc.co.uk/2/hi/africa/7412128.stm

Black, I., & Chulov, M. (2011, February 18). *Bahrain, Libya and Yemen Try to Crush Protests with Violence.* Retrieved February 21, 2011, from Guardian.co.uk: http://www.guardian.co.uk/world/2011/feb/18/bahrain-libya-yemen-protests-violence

Blahut, R. E. (1990). *Digital Transmission of Information.* New York: Addison-Wesley.

Baocun, W., & Fei, L. (1997). Information Warfare. In M. Pillsbury (Ed.), *Chinese Views of Future Warfare* (pp. 327-342). Washington, D.C.: National Defense University Press.

Boehm, B. W. (1991). Software Risk Management: Principles and Practices. *Software* 8(1), 32-41.

Borden, A. (1999, November 2). *What is Information Warfare?* Retrieved July 02, 2009, from Air & Space Power Journal: http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html

Brazzoli, M. S. (2007). Future Prospects of Information Warfare and Particularly Psychological Operations. In L. (. le Roux, *South African Army Vision 2020* (pp. pp. 217-232). Pretoria: Institute for Security Studies.

Brenton, C. (2006, April 19). *Egress Filtering FAQ.* Retrieved October 12, 2009, from SANS Institute: http://www.sans.org/reading_room/whitepapers/firewalls/egress_filtering_faq_1059?show=1059.php&cat=firewalls

British Educational Research Association. (2006). *Data Collection: Interviews in Research*. Retrieved October 19, 2011, from www.bera.ac.uk: http://www.bera.ac.uk/data-collection-interviews-in-research/

Broadman, H. G. (2008, April). *China and India Go to Africa*. Retrieved August 30, 2011, from Foreign Affiars: http://www.foreignaffairs.com/articles/63224/harry-g-broadman/china-and-india-go-to-africa

Bronstein, P. (2010, April 6). *The Wikileaks Incident: How Social Media has Change Warfare Coverage*. Retrieved April 7, 2010, from The Huffington Post: http://www.huffingtonpost.com/phil-bronstein/the-wikileaks-incident-ho_b_527788.html

Brooks, C. (2009, July 22). *SA Hit by Service-Delivery Protests*. Retrieved September 18, 2011, from Mail and Guardian Online: http://mg.co.za/article/2009-07-22-sa-hit-servicedelivery-protests

Brooks, C. (2011, April 27). *A Crack in the Cloud: Why the Amazon Outage Caught so Many by Surprise*. Retrieved May 4, 2011, from SearchCloudComputing.com: http://searchcloudcomputing.techtarget.com/news/2240035254/A-crack-in-the-cloud-Why-the-Amazon-outage-caught-so-many-by-surprise

Business Monitor International. (2010). *Mozambique: How Rising Wheat Prices Crippled SMS Services*. Retrieved November 5, 2010, from Business Monitor International Risk Watchdog:

http://www.riskwatchdog.com/2010/09/13/mozambique-how-rising-wheat-prices-crippled-sms-services/

Business Software Alliance. (2010). *7th Annual BSA-IDC Global Software Piracy Study 2009.* Washington, D.C.

Busuttil, T. B., & Warren, M. J. (2002). A Conceptual Approach to Information Warfare Security Risk Analysis. *European Conference on Information Warfare and Security* (pp. 35-42). Brunel University, London: Academic Conferences International.

Cable News Network. (2001, May 10). *Epic Cyber Attack Reveals Cracks in U.S. Defense*. Retrieved August 13, 2011, from CNN.com: http://articles.cnn.com/2001-05-10/tech/3.year.cyberattack.idg_1_moonlight-maze-hackers-russian-internet-addresses?_s=PM:TECH

Cable News Network. (2010, February 20). We Were Warned, Cyber Shockwave. Transcript available: http://transcripts.cnn.com/TRANSCRIPTS/1002/20/se.01.html (accessed 1 October 2010).

Carney, S. (2009, July 13). *An Economic Analysis of the Somali Pirate Business Model.* Retrieved August 13, 2009, from Cutthroat Capitalism (Wired.com): http://www.wired.com/politics/security/magazine/17-07/ff_somali_pirates

Carr, J. (2010). *Inside Cyber Warfare.* Sebastopol, USA: O'Reilly Media.

Cellular-news.com. (2007, July 2). *Copper Cable Theft Reaching Epidemic Proportions*. Retrieved November 13, 2011, from: http://www.cellular-news.com/story/24681.php

CERT Brazil. (2011). *CERT.br Stats*. Retrieved August 26, 2011, from CERT.br: http://www.cert.br/stats/incidentes/

CERT Netherlands. (2011). *Knowledge and Publications*. Retrieved August 26, 2011, from Govcert.nl: http://www.govcert.nl/english/organisation/annual+reviews

CERT Poland. (2011). *Reports*. Retrieved August 26, 2011, from CERT Polska: http://www.cert.pl/raporty/langswitch_lang/pl

CERT-Africa. (2010a). *CERT in Africa*. Retrieved May 3, 2010, from: http://www.cert-africa.org/node/3

CERT-Africa. (2010b). *Morocco to establish MA-CERT*. Retrieved May 3, 2010, from: http://www.cert-africa.org/node/135

CERT-Finland. (2011). *CERT-Fi - Reports*. Retrieved August 26, 2011, from CERT-Fi: http://www.cert.fi/en/reports.html

Chabrow, E. (2011, September 22). *The Worst Security Hack Ever*. Retrieved September 23, 2011, from GovInfoSecurity.com: http://blogs.govinfosecurity.com/posts.php?postID=1068&rf=2011-09-22-eg&elq=a399671abe4545449138536f20994b3c&elqCampaignId=406#

Chan-Kyong, P. (2009, July 10). *Cyber Attacks from 16 Countries*. Retrieved April 19, 2010, from News24.com: http://www.news24.com/SciTech/News/Cyber-attacks-from-16-countries-20090710

Charette, R. (2010, March 10). *First Energizer, now Vodaphone: More Malware Found in Store Bought Consumer Electronic Products*. Retrieved May 3, 2010, from IEEE Spectrum Riskfactor Blog: http://spectrum.ieee.org/riskfactor/computing/it/malware-found-in-store-bought-consumer-electronics

Chatterji, S. K. (2008). An Overview of Information Operations in the Indian Army. *IOSphere, Special Edition*, 10-14.

Cisco. (2009). *Cisco 2008 Annual Security Report.* Retrieved January 24, 2011, from Cisco Security Reports: http://www.cisco.com/en/US/prod/collateral/vpndevc/securityreview12-2.pdf

Cisco. (2011). *Cisco 2010 Annual Security Report.* Retrieved January 24, 2011, from Cisco Security Reports: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf

Coleman, K. (2008a). *Cyber Warfare Doctrine (Public Version).* McMurray, USA: Technolytics Institute.

Coleman, K. (2008b, August 13). *Cyberwar 2.0 - Russia vs Georgia*. Retrieved April 14, 2010, from DefenseTech.org: http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/

Compaq, Hewlett-Packard, Intel, Lucent, Microsoft, NEC, et al. (2000, April 27). Universal Serial Bus Specification.

Cordesman, A. H. (2000). *Critical Infrastructure Prtoection and Information Warfare.* Washington, DC: Center for Strategic and International Studies.

Cottrell, R. L., & Kalim, U. (2010, September). *New E. Coast of Africa Fibre*. Retrieved November 30, 2010, from SLAC Confluence: https://confluence.slac.stanford.edu/display/IEPM/New+E.+Coast+of+Africa+Fibre

Cox, L.-V. (1997). *Planning for Psychological Operations: A Proposal.* Air Command and Staff College.

Critical Infrastructure Assurance Office. (2000). *Practices for Securing Critical Information Assets.* Washington D.C.: Critical Infrastructure Assurance Office.

Cronin, B., & Crawford, H. (1999). Information Warfare: Its Application in Military and Civilian Contexts. *The Information Society* 15(4), 257-263.

Daily News. (2010, January 18). SMS Restored. *The Daily News*, p. 4.

Dareini, A. A. (2011, April 25). *Iran Says it Has Uncovered Second Cyber Attack*. Retrieved May 17, 2011, from MSNBC: http://www.msnbc.msn.com/id/42750693/ns/world_news-mideast_n_africa/t/iran-says-it-has-uncovered-second-cyber-attack/

Das, K. (2002). *Protocol Anomaly Detection for Network-based Intrusion Detection*. Retrieved October 11, 2011, from SANS Institute: http://www.sans.org/reading_room/whitepapers/detection/protocol-anomaly-detection-network-based-intrusion-detection_349

Davidson, M. A., & Yoran, E. (2007). Enterprise Security for Web 2.0. *Computer 40(11)*, 117-119.

De Vries, L. (2009, July 20). Expert: SMS fraud a 'world first'. *The Pretoria News*, 4.

Defense Science Board. (1996). *Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D).* Washington, D.C.: Defense Science Board, Office of the Secretary of Defense.

Delibasis, D. (2007). *The Right to National Self-Defence in Information Warfare Operations.* Bury St. Edmunds: Arena Books.

Denning, D. E. (1999). *Information Warfare and Security.* Boston: Addison-Wesley.

Dennis, J. (2010, April 28). *SA Seventh in Global Cyber Crime List*. Retrieved May 3, 2010, from The Times Live: http://www.timeslive.co.za/local/article423649.ece/SA-seventh-in-global-cyber-crime-list

Department of Communications. (2010). *Draft Cybersecurity Policy of South Africa.* Pretoria: Government of South Africa.

Department of Homeland Security. (2009). *The 2009 National Infrastructure Protection Plan.* U.S. Government.

Department of Homeland Security. (2010, April 5). *Critical Infrastructure and Key Resources*. Retrieved May 25, 2010, from: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Department of the Army. (1992, November 23). Field Manual 34-40-7. *Communications Jamming Handbook* . Washington DC, USA.

Department of the Army. (2001, June 14). Field Manual 3-0. *Operations* .

Department of the Army. (2010, October 4). Army Regulation 381-12. *Threat Awareness and Reporting Program* . Washington, D.C., USA.

Dhanjani, N., Rios, B., & Hardin, B. (2009). *Hacking: The Next Generation.* Beijing and Cambridge: O'Reilly.

Dingle, S. (2009, July 15). *Anatomy of an SMS Banking Scam*. Retrieved April 6, 2010, from FIN24.com: http://www.fin24.com/articles/default/display_article.aspx?ArticleId=2638902

Du Toit, B. (2003). The African Battlespace: Challenges for Air Defence. *4th South African Joint Air Defence Symposium.* Pretoria.

Dudgeon, I. (2008). Targeting Information Infrastructures. In G. Waters, D. Ball, & I. Dudgeon, *Australia and Cyber-Warfare* (pp. 59-84). Canberra: The Australian National University.

Dunham, K. (2009). Introduction to Mobile Malware. In K. Dunham (Ed.), *Mobile Malware Attacks and Defense* (pp. 1-16). Burlington: Syngress Publishing.

Dwivedi, H., Clark, C., & Thiel, D. (2010). *Mobile Application Security.* New-York: McGraw-Hill.

ECS. (2002). Electronic Communications Security Pty (Ltd) Act. *Act 68 of 2002* . Pretoria: Government of South Africa.

ECT. (2002). Electronic Communications Act. *Act 25 of 2002* . Pretoria: Government of South Africa.

Elky, S. (2006). *Introduction to Information System Risk Management.* SANS Institute.

EMP Commission. (2008, April). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*. Retrieved September 5, 2011, from EMPCommission.org: http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

Enck, W., Traynor, P., McDaniel, P., & La Porta, T. (2005). Exploiting Open Functionality in SMS-Capable Cellular Networks. *12th ACM Conference on Computer and Communications Security.* Alexandria: Association for Computing Machinery.

Erbschloe, M. (2001). *Information Warfare: How to Survive Cyber Attacks.* New York: Osborne/McGraw-Hill.

Eshel, D. (2007). Defeating IEDs. *Journal of Electronic Defense* 32(12), 28-42.

Espiner, T. (2005, November 23). *Security Experts Lift Lid on Chinese Hack Attacks*. Retrieved August 19, 2009, from ZDNet News: http://news.zdnet.com/2100-1009_22-145763.html

Etsebeth, V. (2006). Information Security Policies - The Legal Risk of Uninformed Personnel. *Information Security South Africa 2006.* Johannesburg, 5-7 July.

Falliere, N., O Murchu, L., & Chien, E. (2010). *W32.Stuxnet Dossier.* Cupertino, California: Symantec Security Response.

Faris, R., & Heacock, R. (2009). *Cracking Diwn on Digital Communication and Political Organizing in Iran*. Retrieved July 9, 2009, from OpenNet Initiative:

http://opennet.net/blog/2009/06/cracking-down-digital-communication-and-political-organizing-iran

Festa, P. (1998, March 5). *Computer Security Problems Growing*. Retrieved November 23, 2010, from CNET News: http://news.cnet.com/2100-1001-208787.html

Fisher, D. (2011a, March 2). *Malware-Infected Apps Yanked from Android Market*. Retrieved March 3, 2011, from ThreatPost: http://threatpost.com/en_us/blogs/malware-infected-apps-yanked-android-market-030211

Fisher, D. (2011b, May 12). *SMS Trojan Found in Several Android Apps*. Retrieved May 16, 2011, from ThreatPost: http://threatpost.com/en_us/blogs/sms-trojan-found-several-android-apps-051211

Fisher, D. (2011c, May 23). *Black Hole Exploit Kit Available for Free*. Retrieved May 24, 2011, from Threapost Blog: http://threatpost.com/en_us/blogs/black-hole-exploit-kit-available-free-052311

Fisher, D. (2011d, July 11). *New SMS Trojan Targeting Android Users*. Retrieved July 12, 2011, from ThreatPost: http://threatpost.com/en_us/blogs/new-sms-trojan-targeting-android-users-071111

Fisher, D. (2011e, July 27). *Wide Range of GSM Modules, SCADA Systems Vulnerable to Remote Control*. Retrieved August 2, 2011, from ThreatPost.com: http://threatpost.com/en_us/blogs/wide-range-gsm-modules-scada-systems-vulnerable-remote-control-072711

Fisher, D., & Roberts, P. (2011, January). *Spotlight Series: Stuxnet*. Retrieved February 17, 2011, from Threatpost: http://usa.kaspersky.com/resources/knowledge-center/threatpost-spotlight-series-stuxnet

Fiterman, E. M. (2010, December 20). *Cyberwar: Enemy Needn't Be a Nation-State*. Retrieved December 23, 2010, from GovInfoSecurity.com Blog: http://blogs.govinfosecurity.com/posts.php?postID=828&rf=2010-12-22-eg

Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G. M., & Mehes, A. (2007). Can You Infect Me Now? Malware Propagation in Mobile Phone Networks. *Proceedings of the 2007 ACM Workshop on Recurring Malcode (WORM '07)* (pp. 61-68). Alexandria, Virginia: ACM.

Francis, L. (2009, July 23). *Phishing Scams Migrate to Mobile*. Retrieved April 8, 2010, from ITWeb: http://www.itweb.co.za/index.php?option=com_content&view=article&id=24706:phishing-scams-migrate-to-mobile

Fryer, B., Merrit, K., & Trias, E. (2010). Security in the Emerging African Broadband Environment. *Proceedings of the 5th International Conference on Information Warfare and Security*, (pp. 98-105). Wright-Patterson Air Force Base, Ohio, USA.

F-Secure Corporation. (2005, November 9). *Virus Descriptions: Skulls.A*. Retrieved April 7, 2010, from F-Secure: http://www.f-secure.com/v-descs/skulls.shtml

F-Secure Corporation. (c. 2007). *Virus Descriptions: Worm:SymbianOS/Commwarrior*. Retrieved April 7, 2010, from F-Secure: http://www.f-secure.com/v-descs/commwarrior.shtml

Germain, J. M. (2008, Aoril 29). *The Art of Cyber Warfare, Part 1: The Digital Battlefiels*. Retrieved September 1, 2009, from TechNewsWorld: http://www.technewsworld.com/story/The-Art-of-Cyber-Warfare-Part-1-The-Digital-Battlefield-62779.html

Gilligan, A. (2010, December 12). *Now Wikileaks Suffers its own Leaks*. Retrieved December 13, 2010, from The Telegraph: http://www.telegraph.co.uk/news/worldnews/wikileaks/8196946/Now-Wikileaks-suffers-its-own-leaks.html

Gleditsch, J. M., Wallensteen, P., Eriksson, M., Sollenberg, M., & Strand, H. (2002). Armed Conflict 1946-2001: A New Dataset. *Journal of Peace Research* 39(5), 615-637.

Glenn, M. (2003, August 1). *A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment.* Retrieved September 14, 2011, from SANS Institute: http://www.sans.org/reading_room/whitepapers/intrusion/summary-dos-ddos-prevention-monitoring-mitigation-techniques-service-provider-enviro_1212

Global Mobile Suppliers Association. (2010). *Evolution of Mobile Systems to 3G*. Retrieved April 8, 2010, from GSAcom GSM/3G Stats: http://www.gsacom.com//downloads/charts/Evolution_of_mobile_systems_to_3G.php4

Global Mobile Suppliers Association. (2011a, January 28). *Mobile Subscritpions Market Share Worldwide*. Retrieved May 30, 2011, from GSAcom GSM/3G Stats: http://www.gsacom.com//downloads/charts/GSM_market_share_global.php4

Global Mobile Suppliers Association. (2011b, January 28). *Mobile Subscriber Growth - Africa*. Retrieved January 28, 2011, from GSAcom GSM/3G Stats: http://www.gsacom.com//downloads/charts/mobile_subscriber_growth_africa.php4

GlobalSecurity.org. (2011, July 5). *Solar Sunrise*. Retrieved August 13, 2011, from GlobalSecurity.org: http://www.globalsecurity.org/military/ops/solar-sunrise.htm

Gollmann, D. (2011). *Computer Security*, 3rd ed. Chichester, United Kingdom: John Wiley & Sons.

Goodin, D. (2011a, January 31). *Network Attacks (Allegedly) Ravage London Stock Exchange*. Retrieved August 12, 2011, from The Register: http://www.theregister.co.uk/2011/01/31/london_stock_exchange_attack/

Goodin, D. (2011b, August 11). *Smartphone Images can Hijack BlackBerry Servers*. Retrieved August 12, 2011, from The Register: http://www.theregister.co.uk/2011/08/11/blackberry_high_severity_bug/

Goodman, S., & Harris, A. (2010). The Coming African Tsunami of Information Insecurity. *Communications of the ACM* 53(12), 24-27.

Goodwins, R. (2010, November 28). *Wikileaks Shows US Cyber Intelligence at Work, Gets DDoS Attack*. Retrieved November 29, 2010, from ZDNET: http://www.zdnet.co.uk/blogs/mixed-signals-10000051/wikileaks-shows-us-cyber-intelligence-at-work-gets-ddos-attack-10021175/

Gostev, A. (2006a, September 29). *Mobile Malware Evolution: An Overview, Part1*. Retrieved December 7, 2010, from SecureList: http://www.securelist.com/en/analysis/200119916/Mobile_Malware_Evolution_An_Overview_Part_1

Gostev, A. (2006b, October 26). *Mobile Malware Evolution: An Overview, Part 2*. Retrieved Decemer 7, 2010, from SecureList: http://www.securelist.com/en/analysis/201225789/Mobile_Malware_Evolution_An_Overview_Part_2

Gostev, A., & Maslennikov, D. (2009, September 29). *Mobile Malware Evolution: An Overview, Part 3*. Retrieved December 07, 2010, from SecureList: http://www.securelist.com/en/analysis?pubid=204792080

Grobler, M. (2010). Strategic Information Security: Facing the Cyber Impact. *Workshop on the ICT Uses in Warfare and the Safeguarding of Peace* (pp. 12-21). Bela Bela, South Africa: Council for Scientific and Industrial Research.

Grobler, M., & Bryk, H. (2010). Common Challenges Faced During the Establishment of a CSIRT. *2010 Information Security for South Africa (ISSA 2010).* Sandton: IEEE.

Grobler, M., Jansen van Vuuren, J., & Zaaiman, J. (2011). Evaluating Cyber Security Awareness in South Africa. *Proceedings of the 10th European Conference in Information Warfare and Security* (pp. 113-121). Tallinn, Estonia: Academic Publishing.

Guest, G., Bunce, A., & Johnson, L. (2005, December 23). *How Many Interviews are Enough? An Experiment with Data Saturation and Variability*. Retrieved October 19, 2011, from Sage Publishing: http://fmx.sagepub.com/content/18/1/59.full.pdf

Gühring, P. (2006, September 12). *Concepts against Man-in-the-Browser Attacks.* Retrieved November 9, 2010, from www.cacert.at/svn/sourcerer/CAcert/SecureClient.pdf

Habegger, B. (Ed.). (2008). *The International Handbook on Risk Analysis and Management.* Zurich: Center for Security Studies, Swiss Federal Institute of Technology.

Habib, T. (2011, May 10). *Stuxnet, Wikileaks, and the Militarisation of the Internet*. Retrieved May 12, 2011, from ITWeb: http://www.itweb.co.za/index.php?option=com_content&view=article&id=43443:stuxnet-wikileaks-and-the-militarisation-of-the-internet

HackingStats.com. (2010, December 20). *Hacking Statistics*. Retrieved December 20, 2010, from http://www.hackingstats.com/hacking-statistics.php

Harding, J. (2011). *Warning: IO Professionals are Being Targeted in a False-Flag Operation*. Retrieved March 14, 2011, from LinkedIn: http://www.linkedin.com/groupItem?view=&gid=2195454&type=member&item=39479605&qid=b3d6de4e-1421-4b62-8b8b-ceb65ef75243&goback=%2Egmp_2195454

Hart, K. (2008, August 14). Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar. *The Washington Post*, p. D01.

Hartman, J. (2005, June 1). *The Impact of SPAM on Email Tested*. Retrieved December 2, 2009, from MarketingExperiments.com: http://www.marketingexperiments.com/email-marketing-strategy/impact-spam-email.html

Hayden, M. V. (2010, July 21-29). *Cyber War... Are We at War? And if We are, how Should We Fight it?* Retrieved August 17, 2010, from Blackhat USA 2010: http://media.blackhat.com/bh-us-10/video/Keynote2/BlackHat-USA-2010-Keynote-Hayden.m4v

Hefer, J., & Theron, J. (2009). IW into Africa. *Military Information and Communications Sumposium of South Africa 2009.* Pretoria.

Hendawi, H. (2011, January 27). *Egypt Protests Pose Threat for Regime*. Retrieved January 27, 2011, from Yahoo! News: http://news.yahoo.com/s/ap/20110127/ap_on_re_mi_ea/ml_egypt_protest_66

Hodge, N. (2008, December 30). *YouTube, Twitter: Weapons in Israel's Info War*. Retrieved June 2, 2010, from Wired.com DangerRoom Blog: http://www.wired.com/dangerroom/2008/12/israels-info-wa

Hodge, N. (2009a, April 8). *Inside Moldova's Twitter Revolution*. Retrieved August 20, 2009, from Wired.com DangerRoom: http://www.wired.com/dangerroom/2009/04/inside-moldovas/

Hodge, N. (2009b, April 24). *JailhouseTech Sniffs Out 'Cell' Phones*. Retrieved August 13, 2009, from Wired.com DangerRoom: http://www.wired.com/dangerroom/2009/04/jailhouse-tech-sniffs-out-cell-phones/

Hodge, N. (2010, March 3). *Israelis Nix Op After Facebook Fiasco*. Retrieved May 25, 2010, from Wired.com DangerRoom Blog: http://www.wired.com/dangerroom/2010/03/israeli-military-cancels-raid-after-facebook-fiasco/

Holt, O. (2009a). Technology Survey: Sampling of COMINT and DF Receivers. *Journal of Electronic Defense* 32(7), 33-44.

Holt, O. (2009b). Technology Survey: Sampling of SIGINT Antennas. *Journal of Electronic Defense* 32(8), 45-50.

Holt, O. (2010). Technology Survey:RF Power Sources for IED/Communications Jammers. *Journal of Electronic Defense,* 33(9), 47-52.

Honk Kong CERT. (2011). *Statistics*. Retrieved August 26, 2011, from HKCERT: https://www.hkcert.org/statistics

Hutchinson, W. (2002). Concepts in Information Warfare. *Logistics Information Management* 15(5/6), 410-413.

Hutchinson, W., & Warren, M. (2001). *Information Warfare: Corporate Attack and Defense in a Digital World.* Oxford & Auckland: Butterworth Heinemann.

Hutchinson, W., Huhtinen, A., & Rantapelkonen, J. (2007). The Impact of Perspective on the Effects and Outcomes of Conflict. *Journal of Information Warfare* 6(1), 1-6.

Hyppönen, M. (2010, October 11). *F-Secure Mobile Security Review September 2010.* Retrieved December 13, 2010, from FSecure News You Tube Channel: http://www.youtube.com/watch?v=fJMLr8BDQq8

Hyppönen, M., & Sullivan, S. (2010, May 12). *Security Review May 2010: Mobile Phone Security*. Retrieved December 13, 2010, from FSecureNews YouTube Channel: http://www.youtube.com/watch?v=4xi9SdSXIl8

IBM. (c. 2011). *Cloud Computing*. Retrieved October 12, 2011, from IBM.com: http://www-935.ibm.com/services/za/gts/cloud/systems.html

Ignatieff, M. (2001). *Virtual War: Kosovo and Beyond.* London: Vintage.

Indian CERT. (2011). *Annual Report*. Retrieved August 26, 2011, from CERT-In: http://www.cert-in.org.in/

INet Bridge and AFP. (2011, July 14). *Murdoch Pulls BSkyB Bid Amid British Scandal*. Retrieved July 14, 2011, from Microsoft Network South Africa (MSN ZA) News: http://news.za.msn.com/murdoch-pulls-bskyb-bid-amid-british-scandal

Information Systems Audit and Control Association. (2009). *Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives*. Retrieved April 5, 2011, from ISACA Knowledge Center: http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf

Information Warfare Monitor and Shadowserver Foundation. (2010, April 6). *Shadows in the Cloud: Investigating Cyber Espionage 2.0.* Retrieved August 12, 2011, from Scribd.com: http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0

Information Warfare Monitor. (2009, March 29). *Tracking GhostNet: Investigating a Cyber Espionage Network.* Retrieved September 1, 2009, from: http://128.100.171.10/modules.php?op=modload&name=News&file=article&sid=2386

International Telecommunications Union. (2011, May 23). *ICT Data and Statistics*. Retrieved May 31, 2011, from:www.ITU.int: http://www.itu.int/ITU-D/ict/statistics/index.html

Internet Crime Complaint Center. (2010). *2009 Internet Crime Report*. Retrieved May 3, 2010, from IC3 Annual Reports: http://www.ic3.gov/media/annualreports.aspx

Internet Crime Complaint Center. (2011). *2010 Internet Crime Report*. Retrieved August 24, 2011, from IC3 Annual Reports: http://www.ic3.gov/media/annualreports.aspx

Isachenkov, V. (2011, April 9). *Kremlin Rejects FSB Proposal to Ban Skype, Gmail*. Retrieved April 9, 2011, from Yahoo! News: http://news.yahoo.com/s/ap/20110409/ap_on_hi_te/eu_russia_internet_ban

Jacobs, S., & Duarte, D. (2010, September 16). *Protest in Mozambique: The Power of SMS*. Retrieved November 5, 2010, from AfrOnline: http://www.afronline.org/?p=8680

Janczewski, L. J., & Colarik, A. M. (2008). *Cyber Warfare and Cyber Terrorism.* Hershey and New York: Information Science Reference.

Jansen van Vuuren, J., Phahlamohlaka, J., & Brazzoli, M. (2010). The Impact of the Increase of Broadband Access on South Africa. *Proceedings of the 5th International Conference of Information Warfare and Security*, (pp. 171-181). Wright-Patterson Air Force Base, Ohio, USA.

Jeong, H. C. (2007, August 10). *Botnet C&C Handling with DNS Sinkhole.* Retrieved November 25, 2010, from www.cert.org: http://www.cert.org/archive/pdf/BotSinkhole_KrCERTCC.pdf

Joint Chiefs of Staff. (1996a). Instruction 3210.01. *Joint Information Warfare Policy* . Washington D.C.: U.S. Department of Defense.

Joint Chiefs of Staff. (1996b). Joint Pulication 3-31.1. *Joint Doctrine for Command and Control Warfare* . Washington DC: US Department of Defense.

Joint Chiefs of Staff. (1998, October 9). Joint Publication 3-13. *Joint Doctrince for Information Operations* . Washington DC, USA: US Department of Defense.

Joint Chiefs of Staff. (2007, January 25). Joint Publication 3-13.1. *Electronic Warfare* . Washington DC, USA: US Department of Defense.

Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002). *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages.* Boca Raton, London & New York: Auerbach Publications.

Jones, C. (2009, May 29). *SA Could Face Cyber War*. Retrieved November 29, 2010, from ITWeb: http://www.itweb.co.za/index.php?option=com_content&view=article&id=23157:sa-could-face-cyber-war&catid=296:security-summit-2009&tmpl=component&print=1

Jones, J. A. (2005). *An Introduction to Factor Analysis of Information Risk (FAIR).* Retrieved November 25, 2010, from Risk Management Insight: http://www.riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf

Kabweza, L. S. (2011, August 11). *Details of the ZSE Hacking. It Happened Twice and it was Through Joomla*. Retrieved August 12, 2011, from TechZim: http://www.techzim.co.zw/2011/08/details-of-the-zse-hacking/

Kaplan, J. A. (2011, June 1). *Exclusive: Northrop Grumman May Have Been Hit by Cyberattack, Source Says*. Retrieved June 10, 2011, from Fox News: http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/

Karrim, Q. (2009, March 11). *Local Leaders 'Behind Xenophobic Attacks'*. Retrieved September 18, 2011, from Mail Guardian Online: http://mg.co.za/article/2009-03-11-local-leaders-behind-xenophobic-attacks

Katelhut, B. (2011, August 7). *Warning: Fake LinkedIn Profiles and Tehran Hackers*. Retrieved August 8, 2011, from LinkedIn: http://www.linkedin.com/groupItem?view=&gid=47520&type=member&item=65346842&qid=6c81d6fb-1eaf-4ff7-92a5-c7f64713242e&trk=group_most_popular-0-b-ttl&goback=%2Egmp_47520

Keizer, G. (2010, September 16). *Is Stuxnet the 'Best' Malware Ever?* Retrieved October 4, 2010, from ComputerWorld: http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_

Keizer, G. (2011, March 7). *Google Throws 'Kill Switch' on Android Phones*. Retrieved August 10, 2011, from ComputerWorld: http://www.computerworld.com/s/article/9213641/Google_throws_kill_switch_on_Android_phones

Kennedy, H. (2010, January 18). *Twitter Used to Help Land Plane with Aid for Haiti Earthquake Victims*. Retrieved January 20, 2010, from NY Daily News: http://www.nydailynews.com/news/world/2010/01/18/2010-01-18_twitter_used_to_help_land_plane_with_aid_for_haiti_earthquake_victims.html

Kerrigan, S. (2011, February 18). *US Gov. Software Creates 'Fake People' on Social Networks*. Retrieved March 22, 2011, from examiner.com: http://www.examiner.com/social-media-in-national/us-gov-software-creates-fake-people-on-social-networks-to-promote-propoganda

Kessler, S. (2011, January 25). *Twitter Blocked in Egypt as Protests Turn Violent.* Retrieved January 26, 2011, from Yahoo! News: http://news.yahoo.com/s/mashable/20110125/tc_mashable/twitter_blocked_in_egypt_as_protests_turn_violent

Kiley, S. (2010, Novemner 25). *Super Virus a Target for Cyber Terrorists*. Retrieved November 25, 2010, from Sky News: http://news.sky.com/skynews/Home/World-News/Stuxnet-Worm-Virus-

Targeted-At-Irans-Nuclear-Plant-Is-In-Hands-Of-Bad-Guys-Sky-News-Sources-Say/Article/201011415827544

King Committee on Goverance. (2009). *King Report on Governance for South Africa - 2009 (King III)*. Retrieved October 21, 2011, from University of Pretoria Library: http://www.library.up.ac.za/law/docs/king111report.pdf

Kirk, J. (2009, January 19). *Virus Attacks Ministry of Defence*. Retrieved October 19, 2010, from CIO.co.uk: http://www.cio.co.uk/news/3460/virus-attacks-ministry-of-defence/

Kirkpatrick, D. D. (2011, January 14). *Tunisia Leader Flees and Prime Minister Claims Power*. Retrieved January 17, 2011, from The New York Times: http://www.nytimes.com/2011/01/15/world/africa/15tunis.html?pagewanted=1&_r=2&nl=todaysheadlines&emc=tha2

Kitten, T. (2010, October 13). *Zeus Strikes Mobile Banking*. Retrieved October 18, 2010, from BankInfoSecurity.com: http://www.bankinfosecurity.com/articles.php?art_id=3005&rf=2010-10-16-eb

Kitten, T. (2011, June 13). *IMF Attack: 1 of Dozens of Breaches*. Retrieved June 15, 2011, from Bank InfoSecurity: http://www.bankinfosecurity.com/articles.php?art_id=3736&opg=1

Knowler, W. (2010, January 18). Be Careful About What You're Replying 'Yes' To. *The Daily News*, 10.

Kopp, C. (2000). A Fundamental Paradigm of Infowar. *Systems: Enterprise Computing Monthly*, Sydney:Auscom Publishing, 46-55.

Kravets, D. (2011, January 27). *Internet Down, Tens of Thousands Protest in 'Friday of Wrath'*. Retrieved February 1, 2011, from Wired.com Threatpost: http://www.wired.com/threatlevel/2011/01/egypt-internet-down/#

Krebs, B. (2010, October 24). *Zeus v SpyEye Rivalry Ends in Quiet Merger*. Retrieved October 25, 2010, from KrebsOnSecurity Blog: http://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/

Kretkowski, P. D. (2007, November 12). *The 10 Worst Virus Attacks of All Time*. Retrieved October 6, 2010, from ITSecurity.com: http://www.itsecurity.com/features/10-worst-virus-attacks-111207/

Kunkel, M. (2008a). EA/SIGINT Payloads for UAVs. *Journal of Electronic Defense* 31(6), 32-40.

Kurtz, G. (2010, January 14). *Operation Aurora Hit Google, Others*. Retrieved April 12, 2010, from McAfee Labs Blog: http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/

Labovitz, C. (2010, November). *Attack Severs Burma Internet*. Retrieved November 11, 2010, from Arbor Networks: http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet/

Landler, M., & Markoff, J. (2007, May 29). *Digital Fears Emerge After Data Siege in Estonia*. Retrieved April 14, 2010, from The New York Times Online: http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1

Lardner, R. (2009, August 10). *Air Force Used Twitter to Track NY Flyover Fallout*. Retrieved May 28, 2010, from ABC News: http://abcnews.go.com/Technology/Politics/wireStory?id=8290402

Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H., et al. (2009). *Effective Influence Operations: A Framework for Enhancing Army Capabilities.* Santa Monica: RAND Corporation.

Laudon, K., & LaudonJ.P. (2004). *Management Information Systems: Managing the Digital Firm*, 8th ed. New Jersey: Prentice Hall.

laurelai. (2011, February 14). *HBGary Inc, Working on Secret Rootkit Project Codename: "Magenta"*. Retrieved May 13, 2011, from Crowdleaks: http://crowdleaks.org/hbgary-inc-working-on-secret-rootkit-project-codename-magenta/

Lawton, G. (2007). Web 2.0 Creates Security Challenges. *Computer* 40 (10), 13-16.

Lee, M. (2011, February 1). *Obama Urges Mubarak to Step Down.* Retrieved February 28, 2011, from Missourian: http://www.columbiamissourian.com/stories/2011/02/01/obama-urges-mubarak-step-down-now/

Lehmann, H., & Quilling, R. (2009). Why are there not More Grounded Theories of Information Systems. *Business and Management Conference.* Durban.

Lekic, S. (2011, February 11). *Denmark Prime Minister Lars Loekke Rasmussen Calls on Egypt's Mubarak to Resign.* Retrieved March 1, 2011, from The Huffington Post: http://www.huffingtonpost.com/2011/02/11/denmark-lars-loekke-rasmussen-mubarak-egypt_n_821804.html

Lewis, T. G. (2004). Vulnerability Analysis in Critical Infrastructure Protection. *Journal of Information Warfare* 3(2), 1-13.

Leyden, J. (2011, February 7). *NASDAQ Admits Hackers Planted Malware on Web Portal*. Retrieved August 12, 2011, from The Register: http://www.theregister.co.uk/2011/02/07/nasdaq_malware_breach/

Libicki, M. (1995). What is Information Warfare? Center for Advanced Concepts and Technology, National Defense University.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica: RAND Corporation.

Lindqvist, P., & Nordanger, U. K. (2007). (Mis-?) Using the E-Delphi Method: An Attempt to Articulate the Practical Knowledge of Teaching. *Journal of Research Methods and Methodological Issues*. Retrieved August 28, 2009 from: http://www.scientificjournals.org/journals2007/articles/1222.pdf

Macaulay, T. (2008). *Critical Infrastructure.* Boca Raton, London & New York: CRC Press.

Madrigal, A. (2011, January 24). *The Inside Story of How Facebook Responded to Tunisian Hacks.* Retrieved January 25, 2011, from The Atlantic: http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/#

Malakata, M. (2011, April 28). *Uganda Moves to Block Social Networks*. Retrieved May 7, 2011, from ComputerWorld Kenya: http://www.computerworld.co.ke/articles/2011/04/28/uganda-moves-block-social-networks

Malaysian CERT. (2011). *MyCERT Incident Statistics*. Retrieved August 26, 2011, from MyCERT: http://www.mycert.org.my/en/services/statistic/mycert/2011/main/detail/795/index.html

Marquit, M. (2010, August 3). *The 12 Costliest Computer Viruses Ever*. Retrieved October 6, 2010, from Insecure Blog: http://blog.insure.com/2010/08/03/the-12-costliest-computer-viruses-ever/

Maslennikov, D. (2011, February 4). *The Dark Side of the New Android Market*. Retrieved February 7, 2011, from ThreatPost: http://threatpost.com/en_us/blogs/dark-side-new-android-market-020411

Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). *Stuxnet Under the Microscope.* ESET.

Mavhunga, C. (2008). *The Glass Fortress: Zimbabwe's Cyber-Guerrilla Warfare*. Retrieved November 26, 2010, from Concerned African Scholars, no. 80: http://concernedafricascholars.org/docs/acasbulletin80.pdf

McDermott, R. N. (2009). Russia's Conventional Armed Forces and the Georgian War. *Parameters*, 65-80.

McKenna, E. (2007, July 1). *Counter MANPADS: Live-fire Finale?* Retrieved September 2, 2009, from Avionics Magazine: http://www.aviationtoday.com/av/categories/commercial/Counter-MANPADS-Live-fire-finale_13519.htm

McMillan, R. (2010, January 13). *China: Google Attack Part of a Widespread Spying Effort*. Retrieved January 20, 2010, from MacWorld UK: http://www.macworld.co.uk/digitallifestyle/news/index.cfm?newsid=28293.

Meeks, D. (2011, August 7). *Warning! Suspicious Contacts on LinkedIn*. Retrieved August 8, 2011, from LinkedIn: http://www.linkedin.com/groups/WARNING-Suspicious-Contacts-on-LinkedIn-1705277.S.65284431

Menn, J., & Gelles, D. (2009, August 6). *Concerted cyber-attack takes down twitter.* Retrieved August 7, 2009, from FT.com: www.ft.com/cms/s/.../038b9b54-82a6-11de-ab4a-00144feabdc0.html

Microsoft Corporation. (2009). *Microsoft Security Intelligence Report,* vol. 7. Retrieved November 26, 2010, from:http://www.microsoft.com/security/sir/archive/default.aspx

Microsoft Corporation. (2010a). *Microsoft Security Intelligence Report,* vol. 8. Retrieved November 26, 2010, from:http://www.microsoft.com/security/sir/archive/default.aspx

Microsoft Corporation. (2010b). *Microsoft Security Intelligence Report,* vol. 9. Retrieved November 26, 2010, from:http://www.microsoft.com/security/sir/archive/default.aspx

Microsoft Corporation. (2010c). *Microsoft Security Intelligence Report - Global Botnet Infection Rates, vol. 9*. Retrieved November 26, 2010, from: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=%20b5f9eddc-70dc-4b11-996b-1bc6987c44b9

Microsoft Corporation. (2011a). *Microsoft Security Intelligence Report,* vol. 10. Retrieved May 4, 2011, from: http://www.microsoft.com/security/sir/archive/default.aspx

Microsoft Corporation. (2011b). *Microsoft Security Intelligence Report - Global Threat Assessments, vol. 10*. Retrieved May 4, 2011, from: http://www.microsoft.com/security/sir/default.aspx

Microsoft Corporation. (2011c). *Cloud Solutions*. Retrieved October 12, 2011, from Microsoft.com: http://www.microsoft.com/en-us/cloud/cloudpowersolutions/development-and-hosting.aspx?fbid=mcr-2nuK0-R#tab1-tabs

Miguel, R. (2009, August 7). *Russian Hackers Besiege Social Sites to Silence Pro-Georgian Blogger*. Retrieved August 13, 2009, from E-Commerce Times: http://www.ecommercetimes.com/story/67809.html

Miller, C. R. (2005). Electromagnetic Pulse Threats in 2010. In M. J. Kwolek (Ed.). Maxwell Air Force Base: Air War College, Air University.

Mills, E. (2011, April 18). *Cyber Attakcs Rise at Critical Infrastructure Firms*. Retrieved May 13, 2011, from CNet News: http://news.cnet.com/8301-27080_3-20055091-245.html?tag=mncol;mlt_related

Mitchell, S. (2010, August 17). *Spy Tool Highlights Android App Store Security Issues*. Retrieved August 19, 2010, from PC Pro: http://www.pcpro.co.uk/news/security/360370/spy-tool-highlights-android-app-store-security-issues#ixzz0x20ZTgJK

Molander, R. C., Riddile, A. S., & Wilson, P. A. (1996). *Strategic Information Warfare: A New Face of War.* Santa Monica: RAND Institute.

Molander, R. C., Wilson, P. A., Mussington, D. A., & Mesic, R. F. (1998). *Strategic Information Warfare Rising.* Santa Monica: RAND Institute.

Morales, J. A. (2009a). Timeline of Mobile Malicious Code, Hoaxes, and Threats. In K. Dunham (Ed.), *Mobile Malware Attacks and Defense* (pp. 35-70). Burlington: Syngress Publishing.

Morales, J. A. (2009b). Taxonomy of Moibile Malware. In K. Dunham (Ed.), *Mobile Malware Attacks and Defense* (pp. 93-124). Burlington: Syngress Publishing.

Moteff, J., & Parfomack, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification.* Washington D.C.: Congressional Research Service.

Motorola. (2010). *Can Wireless LAN Denial of Service Attacks be Prevented*. Retrieved October 5, 2011, from BearCom Wireless Worldwide: http://www.bearcom.com/resource-library/ems/wlandenial.pdf

Moyer, E. (2010, September 26). *Stuxnet Worm Hits Iranian Nuclear Plant*. Retrieved October 4, 2010, from CNet News: http://news.cnet.com/8301-1009_3-20017651-83.html

Mtshali, N. (2011, July 1). *Vodacom's Clients See Red Over Cut-off*. Retrieved July 3, 2011, from The Daily News: http://www.dailynews.co.za/vodacom-s-clients-see-red-over-cut-off-1.1091740

Muir, H. (2005, December 2). *Muddle over Mobile Phone Calls Blocked on July 7.* Retrieved September 2011, 2011, from The Guardian: http://www.guardian.co.uk/uk/2005/dec/02/july7.mobilephones

Mulliner, C., & Miller, C. (2009, June 25). *Fuzzing the Phone in Your Phone*. Retrieved June 26, 2010, from Black Hat USA 2009: http://www.blackhat.com/html/bh-usa-09/bh-usa-09-archives.html

Mulvenon, J. C. (1998). The PLA and Information Warfare. *The People's Liberation Army in the Information Age* (pp. 175-186). San Diego: RAND Corporation.

Munger, F. (2011, April 18). *Cyber Attack Forces ORNL to Shut Down Internet Access; Experts Probing Advanced Persistent Threat*. Retrieved May 17, 2011, from Know News: http://blogs.knoxnews.com/munger/2011/04/cyber-attack-forces-ornl-to-sh.html

Nair, Y. (2011, November 8). RICA Phone Racket Bust. *The Daily News*, 1.

Nakamoto, S. (1996, July 6). *Diet Coca-Cola Now Available in Japan.* Retrieved October 13, 2009, from Colawp: http://www.colawp.com/topics/1999/0700-en.html

Nakashima, E. (2011, August 3). *Report on 'Operation Shady RAT' Identifies Widespread Cyber-spying*. Retrieved August 4, 2011, from Washington Post: http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html

Naraine, R. (2009, May). *When Web 2.0 Becomes Security Risk 2.0.* Retrieved April 18, 2011, from Kaspersky Lab: http://usa.kaspersky.com/resources/knowledge-center/when-web-20-becomes-security-risk-20-0

News24.com. (2011, February 1). *Google Launches Twitter Workaround.* Retrieved February 1, 2011, from News24.com: http://www.news24.com/SciTech/News/Google-launches-Twitter-workaround-for-Egypt-20110201

Nichols, R., & Lekkas, P. (2002). *Wireless Security: Models, Threats and Solutions.* New York: McGraw-Hill.

Nicholson, D. L. (1998). *Spread Spectrum Signal Design: LPE and A.J. Systems.* Rockville: Computer Science Press Inc.

Nickolov, E. (2005). Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations. *Information and Security*, vol. 17, 105-119.

Nohl, K., & Paget, C. (2009, December 27-30). *GSM: srsly?* Retrieved March 19, 2010, from 26th Chaos Communications Congress: http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf

O'Brien, J. A., & Marakas, G. (2008). *Introduction to Information Systems 14th ed.* New York: McGraw-Hill.

Ojanpera, T., & Prasad, R. (1998). *Wideband CDMA for Third Generation Mobile Communications.* Boston and London: Artech House.

Okeowo, A. (2008, February 19). *SMSs 'tool of hate in Kenya'.* Retrieved March 04, 2009, from Mail and Guardian Online: http://www.mg.co.za/article/2008-02-19-smss-used-as-a-tool-of-hate-in-kenya

Open Net Initiative. (2005, April 25). *Special Report: Kyrgyzstan - Election Monitoring*. Retrieved April 19, 2010, from Open Net Initiative: http://www.opennetinitiative.net/special/kg/

Open Net Initiative. (2006, April). *The Internet and Elections: The 2006 Presidential Elections in Belarus (and its Implications)*. Retrieved April 19, 2010, from Open Net Initiative: http://opennet.net/sites/opennet.net/files/ONI_Belarus_Country_Study.pdf

Open Security Foundation. (2011). *Data Loss Database*. Retrieved November 12, 2011, from http://datalossdb.org

O'Reilly, T. (2005, September 30). *What is Web 2.0?* Retrieved May 28, 2010, from O'Reilly Media: http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1

Parial, J. (2005, May 11). *An Analysis of the Cabir Mobile Phone Virus.* Retrieved November 25, 2009, from CERT-In: http://www.cert-in.org.in/

Parker, D. B. (2002). Toward a New Famework for Information Security. In S. Bosworth, & M. E. Kabay (Eds.), *Computer Security Handbook, 4th Edition* (pp. 5·1-5·19). New York: John Wiley and Sons.

Paul, I. (2011, June 12). *IMF HAcked: No End in Sight to Security Horror Shows*. Retrieved June 13, 2011, from PC World: http://www.pcworld.com/article/230157/imf_hacked_no_end_in_sight_to_security_horror_shows.html

PBS.org. (2003a, April 24). *Cyberwar Warnings*. Retrieved August 13, 2011, from Frontline: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

PBS.org. (2003b, April 24). *The Spread of the Slammer Worm.* Retrieved August 15, 2011, from Frontline: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/slammermap.html

Peltier, T. R. (2005). *Information Security Risk Analysis.* Boca Raton: CRC Press.

Peltier, T. R., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals.* Boca Raton, London and New York: Auerbach Publications.

Perelson, S., Ophoff, J., & Botha, R. (2006). A Model for Secure Value-Added Service Subscriptions in Cellular Networks. *Information Security South Africa*. Johannesburg: 5-7 July.

Perenson, M. J. (2010, January 11). *USB 3.0 Finally Arrives*. Retrieved October 11, 2011, from PC World: http://www.pcworld.com/article/186566/usb_30_finally_arrives.html

Pfeffer, A. (2010, January 20). *IDF Sets up 'Facebook' Unit to Plug Media Leaks*. Retrieved January 21, 2010, from Haaretz.com: http://www.haaretz.com/hasen/spages/1143897.html

Pfeffer, A., & Izikovich, G. (2009, December 1). *New IDF Web 2.0 Unit to Fight Enemies on Facebook, Twitter*. Retrieved December 1, 2009, from Haaretz.com: http://www.haaretz.com/hasen/spages/1131918.html

Pfleeger, P., & Pfleeger, S. (2003). *Security in Computing, 3rd Edition.* Upper Saddle River, New Jersey: Prentice Hall.

Philp, R. (2011, October 2). *SA Dithers over Dalai Lama Visa*. Retrieved October 26, 2011, from Times Live: http://www.timeslive.co.za/politics/2011/10/02/sa-dithers-over-dalai-lama-visa

Pickworth, E. (2009, July 21). *Phishing scams persist.* Retrieved August 4, 2009, from News24.com: http://www.news24.com/Content/SciTech/News/1132/85d65418408c4cc1920b78b8aaa930de/21-07-2009-10-32/Phishing_scams_persist

Pillay, K., van Niekerk, B., & Maharaj, M. (2010). Web 2.0 and its Implications for the Military. *Workshop on the Uses of ICT in Warfare and the Safeguarding of Peace* (pp. 50-57). Bela-Bela: Council for Scientific Research.

Poisel, R. A. (2004). *Modern Communications Jamming Principles and Techniques.* Boston & London: Artech House.

Ponemon Institute. (2008). *2007 Annual Study: U.K. Cost of a Data Breach.* PGP Corporation.

Ponemon Institute. (2009). *Fourth Annual US Cost of a Data Breach Study.* PGP Corporation.

Ponemon Institute. (2010a). *2009 Annual Study: Cost of a Data Breach (US).* PGP Corporation.

Ponemon Institute. (2010b). *2009 Annual Study: Cost of a Data Breach (UK).* PGP Corporation.

Ponemon Institute. (2010c). *2009 Annual Report: German Cost of a Data Breach.* PGP Corporation.

Ponemon Institute. (2011a). *2010 Annual Study: Global Cost of a Data Breach.* Symamtec.

Ponemon Institute. (2011b). *2010 Annual Study: U.K. Cost of a Data Breach.* Symantec.

Ponemon Institute. (2011c). *2010 Annual Study: Australian Cost of a Data Breach.* Symantec.

POPI. (2009). Protection of Personal Information Bill. *Bill 9 of 2009* . Pretoria: Government of South Africa.

Porras, P., Saidi, H., & Yegneswaran, V. (2009, December 21). *An Analysis of the iKee.B (Duh) iPhone Botnet.* Retrieved November 15, 2010, from SRI International: http://mtc.sri.com/iPhone/

Poulsen, K. (2003, March 7). *Windows Root Kits a Stealthy Threat*. Retrieved October 28, 2010, from The Register: http://www.theregister.co.uk/2003/03/07/windows_root_kits_a_stealthy/

Poulsen, K. (2010, July 25). *Wikileaks Releases Stunning Afghan War Logs - Is Iraq Next?* Retrieved July 26, 2010, from Wired.com Threatlevel: http://www.wired.com/threatlevel/2010/07/wikileaks-afghan/

Poulsen, K. (2011, May 31). *Second Defense Contractor L-3 'Actively Targeted' with RSA SecurID Hacks*. Retrieved June 6, 2011, from Wired.com Threatlevel: http://www.wired.com/threatlevel/2011/05/l-3/

Poulsen, K., & Zetter, K. (2010, June 6). *U.S. Intelligence Analyst Arrested in Wikileaks Video Probe*. Retrieved June 7, 2010, from Wired.com Threatlevel: http://www.wired.com/threatlevel/2010/06/leak/

Press Association. (2011, October 12). *BlackBerry Users Vent Frustrations on Third Day of Service Disruption*. Retrieved October 13, 2011, from The Guardian: http://www.guardian.co.uk/technology/2011/oct/12/blackberry-service-disruption-third-day

Prevelakis, V., & Spinellis, D. (2007, July). *The Athens Affair.* Retrieved March 12, 2010, from IEEE Spectrum: http://spectrum.ieee.org/telecom/security/the-athens-affair/1

PriceWaterhouseCoopers. (2010). *King's Counsel.* Retrieved August 26, 2011, from Corporate Governance - King III report - Introduction and Overview: http://www.pwc.com/za/en/king3

Proakis, J. G. (2001). *Digital Communications.* New York: McGraw Hill.

Prusak, L. (2001). Where did Knowledge Management Come From? *IBM Systems Journal* 40(4), 1002-1007.

PuFeng, W. (1997). The Challenge of Information Warfare. In M. Pillsbury (Ed.), *Chinese Views of Future Warfare* (pp. 317-326). Washington, D.C.: National Defense University Press.

Ragan, S. (2009, August 28). *GSM Alliance Downplays Seriousness of GSM Project*. Retrieved April 6, 2010, from The Tech Herald: http://www.thetechherald.com/article.php/200935/4332/GSM-Alliance-downplays-seriousness-of-GSM-project

Ragan, S. (2010, November 4). *DDoS: Myanmar Attacks Larger Than Those Against Estonia and Georgia*. Retrieved November 11, 2010, from The Tech Herald: http://www.thetechherald.com/article.php/201044/6381/DDoS-Myanmar-attacks-larger-than-those-against-Estonia-and-Georgia

Ramluckan, T., & van Niekerk, B. (2009a). The Role of the Media in Joint Operations. *Military Information and Communications Symposium South Africa 2009.* Pretoria, 20-24 July.

Ramluckan, T., & van Niekerk, B. (2009b). The Terrorism/Mass Media Symbiosis. *Journal of Information Warfare* 8(2), 1-12.

Rawnsley, G. D. (2005, October). Old Wine in New Bottles: China-Taiwan Computer-Based 'Information Warfare' and Propaganda. *International Affairs* 81(5), 1061-1078.

Red Hat. (2010). *Private IaaS Clouds*. Retrieved April 5, 2011, from Red Hat Reference Architecture Series: http://www.redhat.com/f/pdf/ciab-howto.pdf

RICA. (2002). Regulation of Interception of Communications and Provision of Communication-Related Information Act. *Act 70 of 2002* . Pretoria: Government of South Africa.

Rigby, B. (2008). *Mobilising Generation 2.0: Technologies to Recruit, Organise and Engage Youth.* San Francisco: Jossey-Bass.

Roberts, P. (2010, December 20). *New Intel Chips Support SMS Kill Switch*. Retrieved December 23, 2010, from ThreatPost: http://threatpost.com/en_us/blogs/new-intel-chips-support-sms-kill-switch-122010

Roberts, P. (2011a, March 7). *Report: French Ministry of Finance Confirms Hack*. Retrieved March 8, 2011, from Threatpost.com: http://threatpost.com/en_us/blogs/report-french-ministry-finance-confirms-hack-030711

Roberts, P. (2011b, May 20). *Malware in Mass Breac Observed Stealing 200 MB a Day During Infection*. Retrieved May 23, 2011, from ThreatPost: http://threatpost.com/en_us/blogs/malware-mass-breach-observed-stealing-200-mb-day-during-infection-052011

Roberts, P. (2011c, June 13). *Google: Spyware Found, Removed from Android Market*. Retrieved June 21, 2011, from ThreatPost: http://threatpost.com/en_us/blogs/google-spyware-found-removed-android-market-061311

Roberts, P. (2011d, October 12). *Air Force Struggled for Weeks with Malware in Drone Fighter Systems*. Retrieved October 13, 2011, from ThreatPost: http://threatpost.com/en_us/blogs/report-air-force-struggled-weeks-malware-drone-fighter-systems-101211

Robinson, J. J. (2011, February 2). *Maldavian President Joins Calls for Mubarak to Step Down.* Retrieved March 01, 2011, from Minivan News: http://minivannews.com/politics/maldivian-president-joins-calls-for-mubarak-to-step-down-15715

Rolski, T. (2007, May 17). *Estonia: Ground Zero for World's First Cyber War.* Retrieved September 23, 2009, from ABC News: http://abcnews.go.com/print?id=3184122

Roman, J. (2011, July 5). *Mobile Devices Intensify IT Security Jitters*. Retrieved July 11, 2011, from Gov InfoSecurity: http://www.govinfosecurity.com/articles.php?art_id=3815&opg=1

Rondganger, L. (2007, May 9). Credit card scam costs SAA R14m. *The Star*, p. 1.

RSA FraudAction Research Labs. (2009, September 16). *"Chat-in-the-Middle" Phishing Attack Attempts to Steal Consumers' Data via Bogus Live-Chat Support*. Retrieved November 9, 2010, from RSA Blogs: http://blogs.rsa.com/rsafarl/chat-in-the-middle-phishing-attack-attempts-to-steal-consumers-data-via-bogus-live-chat-support/

Sabasteanski, A. (2005). *Patterns of Global Terrorism 1985-2005: U.S. Department of State Reports with Supplementary Documents and Statistics.* Great Barrington: Berkshire Publishing.

SANS Institute. (2010). *SANS Institute Glossary of Security Terms – R*. Retrieved 10 28, 2010, from http://www.sans.org/security-resources/glossary-of-terms/r

Savitz, E. (2011, September 19). *Military Contractor Mitsubishi Heavy Hit by Hack Attack.* Retrieved September 21, 2011, from Forbes: http://www.forbes.com/sites/ericsavitz/2011/09/19/military-contractor-mitsubishi-heavy-hit-by-hack-attack/

Scheepers, W. (2009). Information (Cyber) Warfare: Fact or Fiction. *4th Military Information and Communications Symposium of South Africa 2009.* Pretoria.

Schneier, B. (2010, November 16). *Bruce Schneier on Cyber War and Cyber Crime*. (The Institute for International and European Affiars) Retrieved December 23, 2010, from YouTube: http://www.youtube.com/watch?v=Tkcxi-D5_C0

Schwartau, W. (1996). *Information Warfare: Chaos on the Information Superhighway 2nd Ed.* New York: Thunder's Mouth Press.

Seriot, N. (2010). *iPhone Privacy.* Retrieved June 26, 2010, from Black Hat DC 2010, Arlington: http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html

Shachtman, N. (2008, March 4). *Isreali Drones Jamming Phones in Gaza?* Retrieved August 12, 2009, from Wired.com DangerRoom: http://www.wired.com/dangerroom/2008/03/israel-drones-j/

Shachtman, N. (2009a, July 6). *UK Spy Chief's Facebook Fail: Big Deal, or Big Whoop?* Retrieved May 25, 2010, from Wired.com DangerRoom Blog: http://www.wired.com/dangerroom/2009/07/uk-spy-chiefs-facebook-fail-big-deal-or-big-whoop/

Shachtman, N. (2009b, July 28). *Exclusive Interview: Pirate on When to Negotiate, Kill Hostages*. Retrieved August 13, 2009, from Wired.com Dangerroom: http://www.wired.com/dangerroom/2009/07/exclusive-interview-pirate-on-when-to-negotiate-kill-hostages/#more-15332

Shachtman, N. (2009c, July 30). *Military May Ban Twitter, Facebook as Security 'Headaches'*. Retrieved May 25, 2010, from Wired.com DangerRoom Blog: http://www.wired.com/dangerroom/2009/07/military-may-ban-twitter-facebook-as-security-headaches/

Shachtman, N. (2010, June 1). *Israel Turns to YouTube, Twitter After Flotilla Fiasco*. Retrieved June 2, 2010, from Wired.com DangerRoom Blog: http://www.wired.com/dangerroom/2010/06/israel-turns-to-youtube-twitter-to-rescue-info-war/

Shachtman, N. (2011, October 8). *Computer Virus Hits US Predator and Reaper Drone Fleet*. Retrieved October 13, 2011, from ARS Technica: http://arstechnica.com/business/news/2011/10/exclusive-computer-virus-hits-drone-fleet.ars

Shafiee, S., & Ulukus, S. (2009). Correlated Jamming in Multiple Access Channels. *IEEE Transactions on Information Theory* 55(10), 4598-4607.

Shake, T. H., Hazzard, B., & Marquis, D. (1999). Assessing Network Infrastructure Vulnerabilities to Physical Layer Attacks. *National Information Systems Security Conference.* Crystal City, Virginia: National Institute of Standards and Technology.

Shannon, C. E. (1948). A Mathematical Theory of Communications. *Bell Systems Technical Journal* 3(27), 379-423.

Sherr, I. (2011, July 4). *Computer-Hacking Group Targets Apple in Latest Attack*. Retrieved July 11, 2011, from Wall Street Journal Online: http://online.wsj.com/article/SB10001424052702304803104576424573989176378.html

Sikwane, B. (2010). *The Art of Hide and Seek in Warfare*. Retrieved December 29, 2010, from Aardvark AOC: http://aardvarkaoc.co.za/index_files/Page316.htm

Singel, R. (2009, August 5). *Prison Cell Jamming Bill Close to Senate Passage*. Retrieved August 13, 2011, from Wired.com Epicenter: http://www.wired.com/epicenter/2009/08/prison-cell-jamming-bill-close-to-senate-passage/

Sky News. (2011). *Middle East: See Facts About all the Countries in the Region.* Retrieved March 1, 2011, from news.sky.com: http://news.sky.com/skynews/Interactive-Graphics/middleeast

Smith, D. (2009, July 22). *Anger at ANC Record Boils Over in South African Townships*. Retrieved 18 September, 2011, from The Guardian: http://www.guardian.co.uk/world/2009/jul/22/south-africa-protests

Smith, R., & Knight, S. (2005). Applying Electronic Warfare Solutions to Network Security. *Canadian Militry Journal,* Autumn 2005.

Smyth, N., McLoone, M., & McCanny, J. V. (2006). WLAN Security Processing Architectures. In N. Sklavos, & X. Zhang (Eds.), *Wireless Security and Cryptography.* Boca Raton: CRC Press.

Software Engineering Institute. (2003, June 9). *OCTAVE Method Implementation Guide Version 2.0.* Retrieved September 16, 2009, from OCTAVE Information Security Risk Evaluation: http://www.cert.org/octave/

Song, S. (2011). *African Undersea Cables*. Retrieved August 24, 2011, from Many Possibilities: http://manypossibilities.net/african-undersea-cables/

South African Cities Network. (2011a). Retrieved May 20, 2011, from: http://www.sacities.net/

South African Cities Network. (2011b). *State of the Cities Report*. Retrieved May 30, 2011, from http://www.sacities.net/what/strategy/report/607-towards-resilient-citie

South African Press Association. (2009a, March 22). *'Best Not to Invite Dalai Lama'*. Retrieved April 19, 2010, from News24.com: http://www.news24.com/SouthAfrica/Politics/Best-not-to-invite-Dalai-Lama-20090322

South African Press Association. (2009b, July 10). *Third Wave of Cyber Attacks*. Retrieved April 19, 2010, from News24.com: http://www.news24.com/World/News/Third-wave-of-cyber-attacks-20090710

South African Press Association. (2010, January 2010). *Cyberattack on Lawyers in Software Piracy Case*. Retrieved January 17, 2010, from Independent Online: http://www.ioltechnology.co.za/article_page.php?iSectionId=2885&iArticleId=5312752

South African Press Association. (2011, July 1). *ICASA: Cell Operators Don't Meet Requirements*. Retrieved July 3, 2011, from Daily News: http://www.dailynews.co.za/icasa-cell-operators-don-t-meet-requirements-1.1092245

Spirovski, B. (2010, July 27). *Geo Location Based DDoS Targets Mobile Operators*. Retrieved July 4, 2011, from InfoSec Island: https://www.infosecisland.com/blogview/5600-Geo-Location-Based-DDOS-Targets-Mobile-Operators-.html

SpyOps, Technolytics Institute, and Intelomics. (c. 2008). *Cyber Weapons Threat Matrix.*

Stannard, C. (2008). *Beyond the Edge of the Sky.* Valhalla: Crowbar Enterprises.

Stein, J. (2011, March 2). *Spy Bloggers not 'Friending' U.S. Targets, Centcom Says*. Retrieved March 22, 2011, from Washington Post: http://voices.washingtonpost.com/spy-talk/2011/03/spy_bloggers_not_friending_us.html

Stevens, K., & Jackson, D. (2010, March 11). *Zeus Banking Trojan Report*. Retrieved October 6, 2010, from SecureWorks: http://www.secureworks.com/research/threats/zeus

Stewart, P. (2010, October 25). *Pentagon Braces for Huge Wikileaks dump on Iraq War*. Retrieved October 18, 2010, from Yahoo News: http://news.yahoo.com/s/nm/us_usa_iraq_leaks

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *NIST Special Publication 800-30: Risk Management Guide fo Information Technology Systems.* National Institute of Standards and Technology.

StrategyPage.com. (2008, December 3). *Israeli Telephone Commandos Strike Again*. Retrieved April 7, 2010, from StrategyPage.com: http://www.strategypage.com/htmw/htiw/20081203.aspx

StrategyPage.com. (2009a, January 2). *Gaza Cell Phones Targeted*. Retrieved July 27, 2009, from StrategyPage.com: http://www.strategypage.com/htmw/htiw/articles/20090102.aspx

StrategyPage.com. (2009b, September 23). *Why Pirates Hate Mercury.* Retrieved September 23, 2009, from StrategyPage.com: http://www.strategypage.com/htmw/htterr/articles/20090923.aspx

StrategyPage.com. (2010a, April 1). *Marines Return to Facebook*. Retrieved April 1, 2010, from StrategyPage.com: http://www.strategypage.com/htmw/htiw/articles/20100401.aspx

StrategyPage.com. (2010b, April 11). *What was not Said*. Retrieved April 12, 2010, from StrategyPage.com: http://www.strategypage.com/htmw/htiw/articles/20100411.aspx

StrategyPage.com. (2010c, May 1). *The NATO Cyber War Agreement*. Retrieved May 3, 2010, from StrategyPage.com: http://www.strategypage.com/htmw/htiw/articles/20100501.aspx

StrategyPage.com. (2010d, May 2). *India Bans Chinese Cell Phones*. Retrieved May 3, 2010, from StrategyPage.com: http://www.strategypage.com/htmw/htiw/articles/20100502.aspx

Strickland, J. (2008, August 26). *10 Worst Computer Viruses of All Time*. Retrieved October 6, 2010, from How Stuff Works: http://computer.howstuffworks.com/worst-computer-viruses.htm

Subhedar, V., & Leung, A. (2011, August 10). *Hong Kong Exchange Trading Disrupted as Hackers Target Website*. Retrieved August 12, 2011, from Yahoo! News Canada: http://ca.news.yahoo.com/hk-exchange-trading-disrupted-hackers-target-website-112104764.html

Sudworth, J. (2009, July 9). *New 'Cyber Attacks' Hit S Korea*. Retrieved September 01, 2009, from BBC News: http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm

Swartz, J. (2005, April 28). *Cell Phones now Richer Targets for Viruses, Spam, Scams*. Retrieved April 8, 2010, from USA Today: http://www.usatoday.com/money/industries/technology/2005-04-27-cell-phones-usat_x.htm

Symantec Corporation. (2011a). *Symantec Internet Security Threat Report, Vol. 16: Trends for 2010.* Mountain View, California. Retrieved November 14, 2011, from: http://www.symantec.com/business/threatreport/

Symantec Corporation. (2011b). *Norton Cybercrime Report 2011*. Retrieved September 21, 2011, from Norton South Africa: http://za.norton.com/content/en/za/home_homeoffice/html/cybercrimereport/#nav

Symantec Security Response. (2009, April 3). *Backdoor.GhostNet*. Retrieved May 3, 2010, from YouTube.com: http://www.youtube.com/results?search_query=ghostnet+backdoor&aq=f

Symantec Security Response. (2011, October 20). *W.32 Duqu: The Precursor to the Next Stuxnet*. Retrieved October 26, 2011, from Symantec.com: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf

TamilNet.com. (2009, February 9). *TamilNet.com.* Retrieved February 16, 2009, from SLBC jamming FM broadcast prompts BBC to suspend partnership: http://www.tamilnet.com/art.html?catid=13&artid=28358

Tate, R. (2010, June 9). *Apple's Worst Security Breach: 114,000 iPad Owners Exposed*. Retrieved June 10, 2010, from Gawker.com: http://gawker.com/5559725/att-fights-spreading-ipad-fear

Taub, H., & Schilling, D. L. (1991). *Principles of Communication Systems.* New Delhi: Tata McGraw-Hill Publishing.

Taylor, P. M. (2002). Perception Management and the 'War' Against Terrorism. *Journal of Information Warfare* 1(3), 16-29.

Teraco. (2011). *The Cloud - Cloud Server Hosting Providers (SaaS/PaaS)*. Retrieved October 12, 2011, from Teraco Data Environments: http://www.teraco.co.za/data-centre-colocation-clients/data-centre-service-directory/hosting-services/cloud-computing/

Theron, J. (2008). Operational Battle Space: An Information Warfare Perspective. *IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace* (pp. 41-47). Pretoria: CSIR.

Thion, R. (2008). Network-Based Passive Information Gethering. In L. J. Janczewski, & A. M. Colarik, *Cyber Warfare and Cyber Terrorism* (pp. 120-128). Hershey, Pennsylvania, and London, UK: Information Science Reference.

Thornburgh, N. (2005a, August 25). *Inside the Chinese Hack Attack*. Retrieved April 14, 2010, from Time: http://www.time.com/time/nation/article/0,8599,1098371,00.html

Thornburgh, N. (2005b, August 29). *The Invasion of the Chinese Cyberspies (and the Man who tried to Stop Them)*. Retrieved April 14, 2010, from Time Magazine Online: http://www.time.com/time/magazine/article/0,9171,1098961,00.html

Tisdall, S. (2010, July 25). *Afghanistan War Logs: NATO Feared Taliban Coul Tap its Mobile Phones*. Retrieved August 16, 2011, from The Guardian: http://www.guardian.co.uk/world/2010/jul/25/taliban-tapped-mobile-phones-afghanistan

Torchia, C. (2009, July 8). *Pirate attacks go unreported.* Retrieved October 12, 2009, from News24.com: http://www.news24.com/Content/World/News/1073/a770b67c2166425f8e2945057160e3ff/08-07-2009-11-51/Pirate_attacks_go_unreported

Traynor, P., Lin, M., Ontang, M., Rao, V., Jaeger, T., McDaniel, P., et al. (2009). On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. *Proceedings of the 16th ACM Conference on Computer and Communications Security (CSS '09)* (pp. 223-234). Chicago: ACM.

Trustwave. (2011, January 19). *Global Security Report 2011.* Retrieved February 3, 2011, from Trustwave Global Security Report: https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2011.pdf

Tubbs, B. (2011, October 10). *Seacom Experiences Another Outage*. Retrieved October 26, 2011, from ITWeb: http://www.itweb.co.za/index.php?option=com_content&view=article&id=48017:seacom-experiences-another-outage&catid=198

Twitter. (2010, September 21). *All About the "onMouseOver" Incident*. Retrieved October 18, 2010, from Twitter Blog: http://blog.twitter.com/2010/09/all-about-onmouseover-incident.html

United Nations Foundation. (2009). *New technologies in Emergencies and Conflict - The Role of Information and Social Networks.* Retrieved February 2010, 2010, from Global Problems, Global Solutions: http://www.globalproblems-globalsolutions-files.org/pdf/UNF_tech/emergency_tech_report2009/Tech_EmergencyTechReport_full.pdf

United States Air Force. (1998, August 5). Air Force Doctrine Document 2-5. *Information Operations* . Washington DC, USA: United States Air Force.

University of California Berkeley Library. (2009). *Recommended Search Strategy: Analyze Your Topic & Search with Peripheral Vision*. Retrieved May 31, 2011, from UC Berkeley Teaching Library Internet Workshops: http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Strategies.html

Uppsala Conflict Data Program, International Peace Research Institute. (2007). Human Security Report Project. *UCDP/HSC Dataset*. Retrieved October 12, 2009, from: http://www.hrsgroup.org/index?option=content&task=view&id=112

Uppsala Conflict Data Program, International Peace Research Centre. (2009). UCDP/PRIO Armed Conflict Dataset version 4-2009. Retrieved September 1, 2009, from: http://www.prio.no/CSCW/Datasets/Armed-Conflict/

US Army Signal Center of Excellence. (2011, August 16). *Army Cellular Capability Development Strategy*. Retrieved September 8, 2011, from: http://www.ecrow.org/pdf/Army_Cellular_Capability_Development_Strategy_16_August_2011.pdf

US-CERT. (2009). *Vulnerability Note VU#261869: Clientless SSL VPN products break web browser domain-based security models*. Retrieved October 11, 2011, from http://www.kb.cert.org/vuls/id/261869

van Creveld, M. (2000). *The Art of War: War and Military Thought.* London: Cassel & Co.

van Niekerk, B. (2009). Interoperability in EW and CNO: Considerations for the African Continent. *Military Information and Communications Symposium of South Africa.* Pretoria, 20-24 July.

van Niekerk, B. (2010a, February 11). Vulnerability Assessment of Modern ICT Infrastructure from an Information Warfare Perspective. School of Information Systems and Technology Seminar Series.

van Niekerk, B. (2010b). Safety and Security on the Net. *TEDx UKZN.* Durban, 14 May.

van Niekerk, B. (2010c). Information Warfare. *Durban Whitehat Advisory.* Durban, 17 June.

van Niekerk, B., & Maharaj, M. (2009a). The Future Roles of EW in IW. *Big Crow Conference*. Pretoria, 5-26 August: Association of Old Crows Aardvark Roost.

van Niekerk, B., & Maharaj, M. (2009b). Information Operations Education for South Africa. *3rd Annual Teaching and Learning Conference* (pp. 206-224). Durban, 21-23 September: University of KwaZulu-Natal.

van Niekerk, B., & Maharaj, M. (2009c). The Future Roles of Electronic Warfare in the Information Warfare Spectrum. *Journal of Information Warfare* 8(3), 1-13.

van Niekerk, B., & Maharaj, M. (2010a). Information as a Strategic Asset in an Asymmetric Unconventional Conflict. *International Conference on Information Management and Evaluation* (pp. 413-421). Cape Town: Academic Conferences International.

van Niekerk, B., & Maharaj, M. (2010b). Mobile Security from an Information Warfare Perspective. *9th Information Security South Africa Conference.* Sandton, 2-4 August.

van Niekerk, B., & Maharaj, M. (2010c). Weponisation of the Net. *12th Annual Conference on World Wide Web Applications (ZA-WWW).* Durban.

van Niekerk, B., & Maharaj, M. (2011a). Infrastructure Vulnerability Analysis from an Information Warfare Perspective. *South African Computer Lecturer's Association (SACLA 2011)* (pp. 76-85). Durban: SACLA and University of KwaZulu-Natal.

van Niekerk, B., & Maharaj, M. (2011b). Mobile Malware Trends. *Business Management Conference (BMC) 2011*. Durban: University of KwaZulu-Natal.

van Niekerk, B., & Maharaj, M. (2011c). Relevance of Information Warfare Models to Critical Infrastructure Protection. *Scientia Militaria* 39(2), 99-122.

van Niekerk, B., & Maharaj, M. (2011d). The IW Life Cycle Model. *South African Journal of Information Management* 13(1), http://www.sajim.co.za/index.php/SAJIM/article/view/476.

van Niekerk, B., & Maharaj, M. (c. 2012). National Perspective: South Africa. In D. Ventre. ISTE.

van Niekerk, B., Pillay, K., & Maharaj, M. (2011). Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective. *Internation Journal of Communications,* vol. 5, 1406-1416.

van Niekerk, B., Ramluckan, T., & Maharaj, M. (2011). Web 2.0 as an Attack Vector Against Strategic Security. *5th Military Information and Commnuications Symposium of South Africa (MICSSA 2011).* Pretoria.

van Rooyen, K. (2009, July 18). Hidden price of a banking scam. *The Times*, URL: http://www.thetimes.co.za/News/Article.aspx?id=1036132 [Accessed: 30 July 2009].

Veerasamy, N. (2009a). Towards a Conceptual Framework for Cyber-terrorism. *4th International Conference on Information Warfare and Security*, (pp. 10-19). Cape Town.

Veerasamy, N. (2009b). A High-Level Conceptual Framework of Cyber-Terrorism. *Journal of Information Warfare* 8(1), 42-54.

Veerasamy, N., & Eloff, J. H. (2008). Towards a Framework for a Network Warfare Capability. *Information Security South Africa 2008*, (pp. 405-422). Pretoria.

Veerasamy, N., & Eloff, J. (2009). Understanding the Elementary Considerations in a Network Warfare Environment: An Introductory Framework. *IFIP TC9 Proceedings in ICT uses in Warfare and the Safegarding of Peace* (pp. 95-108). Pretoria: CSIR.

Ventre, D. (2009). *Information Warfare.* London: ISTE.

Verdu, S. (1998). *Multiuser Detection.* Cambridge: Cambridge University Press.

Verizon. (2011). *2011 Data Breach Investigations Report*. Retrieved April 4, 2011, from Verizon Business: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Vermeulen, J. (2011, May 24). *Fibre Cable Theft in SA.* Retrieved November 13, 2011, from MyBroadband.co.za: http://mybroadband.co.za/news/telecoms/20457-fibre-cable-theft-in-sa.html

Villeneuve, N. (2010, November 12). *Koobface: Inside a Crimeware Nework.* Retrieved November 15, 2010, from Munk School of Global Affairs, InfoWar Monitor, and The SecDev Group: http://www.infowar-monitor.net/koobface

Walker, R. (2010, December 9). *A Brief History of Operation Payback*. Retrieved December 21, 2010, from Salon.com: http://mobile.salon.com/news/feature/2010/12/09/0

Waltz, E. (1998). *Information Warfare: Principles and Operations.* Boston & London: Artech House.

Ward, J. (2003). *Strategic Influence Operations - The Information Connection.* Pennsylvania: U.S. Army War College.

Ware, W. H. (1998). *The Cyber Posture of the National Information Infrastructure.* Santa Monica: RAND Institute.

Waterman, S. (2008, August 18). *Analysis: Russia-Georgia Cyber-war Doubted*. Retrieved August 19, 2008, from The Middle East Times: http://www.metimes.com/Security/2008/08/18/analysis_russia-georgia_cyberwar_doubted/1a29/

Weaver, M. (1999, August 16). *Computer Genius Took His Revenge*. Retrieved August 16, 2011, from RT Mark: http://www.rtmark.com/more/articles/naughtynews.htm#revenge

Webb, J. (2009, May 11). *Somali pirates using London contacts - Spain radio.* Retrieved September 4, 2009, from Reuters: http://www.reuters.com/articlePrint?articleId=USLB570114

Weinberger, S. (2009, September 4). *And Spooks Heart Software for Rooting out Terrorists.* Retrieved September 7, 2009, from Wired.com DangerRoom: http://wired.com/dangerroom/2009/09/can-paypal-help-find-terrorists/

Wenger, A., Metzger, J., & Dunn, M. (Eds.). (2002). *CIIP Handbook 2002: An Inventory of Policies in Eight Countries.* Swiss Federal Institute of Technology.

Westervelt, R. (2009, October 27). *Pushdo Botnet uses Facebook to Spread Malicious Email Attachment*. Retrieved January 21, 2011, from SearchSecurity.com: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1372558_mem1,00.html

Westervelt, R. (2011a, January 20). *Bredolab Trojan attack uses job applications, nets hackers $150K*. Retrieved January 21, 2011, from SearchSecurity.com: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1526342,00.html

Westervelt, R. (2011b, July 12). *New Android Phone Malware Indicates Transition to Mobile Platform Attacks*. Retrieved July 14, 2011, from SearchSecurity.com: http://searchsecurity.techtarget.com/news/2240037695/New-Android-phone-malware-indicates-transition-to-mobile-platform-attacks

Weston, G. (2011, February 17). *Foreign Hackers Attack Canadian Government*. Retrieved February 18, 2011, from CBC News: http://www.cbc.ca/technology/story/2011/02/16/pol-weston-hacking.html

Whitman, M. E., & Mattord, H. J. (2010). *Management of Information Security, 3rd Ed.* Boston: Cengage Learning Course Technology.

Wik, M. W. (2002). Revolution in Information Affairs: Tactical and Strategic Implications of Information Warfare and Information Operations. In A. Jones, G. L. Kovacich, & P. G. Luzwick, *Global Information Warfare* (pp. 579-628). Boca Raton, London, and New York: Auerbach Publications.

Williams, F., Rice, R. E., & Rogers, E. M. (1988). *Research Methods and the New Media.* The Free Press.

Willsher, K. (2009, February 7). *French Fighter Planes Grounded by Computer Virus*. Retrieved October 19, 2010, from The Telegraph: http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html

World Movement for Democracy. (c. 2009). *Twitter Case Study*. Retrieved June 17, 2010, from: http://www.wmd.org/resources/whats-being-done/information-and-communication-technologies/case-study-twitter

Wyld, B. (2004, July 17). *The Fear Factor*. Retrieved July 31, 2009, from The Age: http://www.theage.com.au/articles/2004/07/16/1089694549469.html

Wylder, J. (2004). *Strategic Information Security.* Boca Raton and London: Auerbach Publications.

Xenakis, C., & Merakos, L. (2006). Vulnerabilities and Possible Attacks Against the GPRS Backbone Network. *Critical Information Infrastructures Security* (pp. 262-272). Samos, Greece: Springer.

Yao, Y., & Poor, H. V. (2001). Eavesdropping in the Synchronous CDMA Channel: an EM-Based Approach. *IEEE Transaction on Signal Processing* 49(8), 1748-1756.

Yin, J. K. (2009). The Electronic Intifada: The Palestinian Online Resistances in the 2nd Intifada. *Journal of Information Warfare* 8(1) , 1-19.