CLC- Cyberterrorism Life Cycle Model

Thesis

by

NAMOSHA VEERASAMY

MSc (Computer Science)

201185569

Submitted in fulfilment of the requirements

for the degree

PHILOSOPHIAE DOCTOR

in

COMPUTER SCIENCE

in the

Faculty of Science

at

UNIVERSITY of JOHANNESBURG

Promoter: Prof MM Grobler

Co-promoter: Prof SH von Solms

Johannesburg

September 2014

Abstract

The rise of technology has brought with it many benefits but also the potential for great dangers. In particular, Information Communication Technology (ICT) is involved in many facets of life-influencing systems, which range from power plants to airports. Terrorists are now realising the great possibilities of interfering with critical infrastructure. Remote access, reduced costs, automation, replication, speed, direct effect, varied targets and anonymity are all benefits that make attacking computers and networks in cyberspace an attractive solution. ICT could thus serve as a powerful instrument to advance political and ideological viewpoints.

The ICT landscape now faces an emerging threat in the form of cyberterrorists. However, it is important not to incorrectly perceive ordinary cyber attacks as cyberterrorism. Cyberterrorism is different from cybercrime in that is has differing motives, attack goals, techniques and intended effects. The motivation for cyberterrorism largely stems from political and ideological views (religious, social activism, retributional). Cyber attacks are mainly driven by financial theft, fraud or espionage, whereas cyberterrorism aims to create publicity for a cause and leave a high impact.

In this study, a Cyberterrorism Life Cycle (CLC) Model is developed in order to demonstrate the various factors that lead to the establishment and growth of cyberterrorism. The model depicts the various strategic and technical issues that are relevant to the field. Overall, this model aims to structure the dynamic interaction of the behavioural and technological factors that influence the development of cyberterrorism.

Throughout the research, various factors that are influential to cyberterrorism are investigated. The research follows a systematic approach of revealing various underlying issues and thereafter compiling the holistic CLC model to depict these critical issues. Part 1 introduces cyberterrorism and provides the background to the field by discussing incidents and example groups. Initially, the concept of cyberterrorism is explored and the proposed definition tested. Part 2 looks at investigating cyberterrorism more deeply. A conceptual framework is presented that introduces the most pertinent factors in the field of cyberterrorism. Next, the traditional and innovative use of the Internet to carry out and support terrorism is explored. Then, the study addresses the determination of additional social factors using Partial Least Squares Path Modelling. In Part 3, the field of cyberterrorism is more intensely studied. Cyberterrorism is mapped to the Observe-Orient-Decide-Act (OODA) loop, which will form the basis of the CLC model. Thereafter, the most influential concepts essential to the field of cyberterrorism are applied in order to classify attacks as cyberterrorism using ontologies. Furthermore, in Part 3, countermeasures are discussed to look at ways to combat cyberterrorism. Part 4 forms the crux of the research. The CLC model is presented as a structured representation of the various influential factors relevant to cyberterrorism. Thereafter, the CLC model is simulated to show the field more dynamically. Overall, the CLC model presented in this study aims to show the interaction of the various strategic, behavioural and technical issues. The CLC model can help elucidate the reasons for attraction into extremist groups and how attacks are carried out.

Acknowledgements

A big thank you to…

To the **Almighty God**, for the strength in completing this work.

My supervisor **Prof MM Grobler**, for your strong leadership, guidance and knowledge in aiding me with my post-graduate studies. Working with you is a great pleasure.

My co-supervisor **Prof SH von Solms** for his technical expertise and direction throughout the development of this work.

My **parents** and **sisters** for their continued support in my pursuit for academic excellence.

The **National Research Foundation (NRF**) and the **University of Johannesburg** for their financial assistance.

Prof Tom Holt for your technical assistance in understanding statistics.

Most importantly to my husband **Aubrey**, for your undying love, constant support, endless energy and inner strength. You have not only been my inspiration but also given me so much of technical support, ideas and input into this research.

Contents

Figures

Tables

Abbreviations

Abbreviation	Full Description
ALF	Animal Liberation Front
C2	Command and Control
CFR	Cyber First Responder
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CLC	Cyberterrorism Life Cycle
CNA	Computer Network Attack
CRT	Cyber Response Team
CSIR	Council for Scientific and Industrial Research
CSIRT	Computer Security Incident Response Team
CyberSec	Cyber Security
DOD	Department of Defence
DOI	Digital Object Identifier
DOS	Denial-of-Service
ECIW	European Conference on Information Warfare and Security
ECT	Electronic Communications and Transaction
FBI	Federal Bureau of Investigations
FTP	File Transfer Protocol
GoF	Goodness of Factor
GPS	Global Positioning System

Abbreviation	**Full Description**
HSCB	Human Social and Cultural Board
ICIW	International Conference on Information Warfare and Security
ICT	Information Communication Technology
IDART	Information Design Assurance Red Team
IGC	Institute for Global Communications
IP	Internet Protocol
ISP	Internet Service Provider
IS CERT	Industrial Control Systems Cyber Emergency Response Team
ISSA	Information Security South Africa
JIW	Journal of Information Warfare
LTTE	Liberation Tamil Tigers of Eelam
MICSSA	Military Information and Communications Symposium of South Africa
NATO	North Atlantic Treaty Organisation
NIPALS	Nonlinear Iterative Partial Least Squares
NIST	National Institute of Standards and Technology
NPS	Navy Post-graduate School
NRF	National Research Foundation
OODA	Observe-Orient-Decide-Act
PIRA	Provisional Irish Republican Army
PLS PM	Partial Least Squares Path Modelling
PSYOPS	Psychological Operations

Abbreviation	**Full Description**
RBN	Russian Business Network
SCADA	Supervisory Control and Data Acquisition Systems
SEM	Structured Equations Modelling
SITE	Search for International Terrorist Entities
SMS	Small Message Service
SQL	Standard Query Language
UK	United Kingdom
UNSC	United Nations Security Council
USA	United States of America

Terminology

Cyberattack: An attack, via cyberspace that targets a company's networks, computers or systems with the goal of disrupting, disabling, destroying or maliciously controlling the computing environment/infrastructure. Data can also be destroyed, stolen or its integrity changed (National Institute of Standards and Technology 2013).

Cybercrime: According to the Electronic and Communications Transactions (ECT) Act, cybercrime is (The Government Gazette 2002):

- intentionally accessing intercepting or interfering with data without the appropriate authorisation.
- intentional modification, destruction or rendering of data ineffective without the authority to do so.
- unlawful removal of security measures established to protect data access.interference with the accessibility to an information system with the aim of causing a denial or partial Denial-of Service.
- committing of computer-related extortion, fraud and forgery.

Cyberespionage: This is an exercise of finding secrets without obtaining the permission of the holder of the information. The information could be of a personal, proprietary or classified nature and could be used to gain personal, economic, or military advantage (RSA 2011).

Cyberspace: Cyberspace is a global domain that exists within the information environment and consists of an interdependent network of information technology infrastructures and data residing within it. This may include the Internet, computer systems, telecommunications networks, and embedded processors and controllers" (US DoD 2008). Furthermore, the Canadian Cyber Strategy defines cyberspace as the electronic world created by interconnected networks of information technology and the information on those networks (Public Safety Canada 2012).

Cybersecurity: Cybersecurity refers to actions undertaken by key stakeholders in order to establish and maintain security in cyberspace (International Standards Organisation (ISO) 2012). Furthermore, ISO/IEC 27032:2012(E) Information technology - Security techniques - Guidelines for cybersecurity states that cybersecurity is dependent on information security, application security, network security and Internet security serving as fundamental building blocks in the establishment of cybersecurity. Cybersecurity is one of the activities necessary for Critical Information Infrastructure Protection (CIIP). The protection of critical infrastructure services helps meet basic security needs by ensuring security reliability and availability of critical infrastructure. CIIP can help provide assurance that the goals of cybersecurity are being adequately addressed.

Cyberwarfare: The government security expert Richard A. Clark in his book “Cyber war” (together with Knake) (Clarke, Knake 2011) provides the following definition: Cyberwar are actions carried out by a nation-state in order to penetrate another nation's computers or networks with the purpose of causing damage or disruption. Ventre (2009) states that computer network attacks (CNA) can also be described as cyberwarfare. Furthermore, Ventre proposes that cyberwarfare is a computer attack including trying to access systems, controlling systems, destruction, distortion of data (through viruses, worms and Trojan horses) and data interception. Cyberwarfare can be described as cyber battles. Cyberwarfare group techniques are used to destroy, deteriorate, exploit, or compromise enemy computer systems. Cyberwarfare includes hacking type attacks against enemy computers. Computer hacking can authorise the deterioration of the enemy command and control (C2) structure. It is also known as hacking warfare.

Cyberterrorism: Cyberterrorism is defined as a purposeful act, motivated by personal or political reasons that aim to disrupt or destroy stable organisational or national interests by aiming electronic devices at information systems like computer programs and other electronic methods of communication, transfer and storage (Desouza, Hensgen 2003). Terrorists use coercion to generate support for their cause and can commit violent attacks to force governments to meet their demands. Thus, intimidation and publicity are key objectives for terrorists. Cyberterrorism incorporates the ideas of using cyberspace to carry out acts of terror. Cyberterrorism thus brings together the use of information communication technologies to encourage extremist or aggressive motives, mainly stemming from political, religious or social reasons often in order to create brutal impact.

Terrorism: This consists of criminal acts that are targeted at civilians with the aim of causing death or serious bodily harm. It may include the taking of hostages, which can create a state of terror within the general public or the targeted group. Terrorism tries to intimidate a nation, its government or an international group into performing or abstaining from an act. Such forceful behaviour is forced upon governments, countries or groups based on political, philosophical, ethnic, ideological, racial, religious and other similar causes (United Nations Security Council (UNSC) 2004).

1 CLC- Cyberterrorism Life Cycle Model

> *"Cyberterrorism could also become attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet."*
>
> *– Dorothy Denning*

Information Communication Technology (ICT) provides for huge benefits in terms of convenience and performance but it also brings with it opportunities for malicious onslaught. ICT infrastructure in the hands of terrorists could be a powerful instrument to promote extremist ideologies and propaganda. Terrorism invokes strong emotional responses due to the often-horrific consequences. With the use of technology to facilitate and carry out attacks, comes a rising discipline that holds technical complications, as well as emotional effects. Cyberterrorism has been coined as a concept that combines malicious weapons and technology in order to affect society. This study proposes a model to describe the life cycle development of a cyberterrorist. The model is wide-ranging in that it covers aspects that are relevant to the field of terrorism support, as well as the use of ICT infrastructure to carry out cyberterrorist attacks.

The study provides insight into an emerging and dynamic area. The development of a life cycle model in the area of cyberterrorism instigates discussion and understanding of how terrorism develops and what behavioural and technical countermeasures should be developed. The use of ICT by cyberterrorists relies on rapidly changing technology that makes the task of controlling cyberterrorism challenging. However, defensive security measures do exist that aim at preventing, detecting and reacting to cyber attacks. In addition, various legal, religious, political, social and economic measures can also be executed in an effort to curb the rise of cyberterrorism.

This study considers the use of the Internet in the support of terrorism, driving forces, cybercrime, countermeasures and ontologies together with other modelling techniques. It looks at how the recruitment process of a potential terrorist can be carried out, the planning of an attack and the actual execution of an attack all using ICT. ICT infrastructure can also play a supporting role to terrorism in general. Recruitment, planning and finance are all activities that can utilise modern technologies. Blogs, social networking sites and email are a few examples of ICT that can be used to support terrorism in general. By constructing a life cycle model, understanding can be gained about actual cyberterrorist threats, terrorism support and ordinary cybercrime.

Since cyberterrorism encompasses so many aspects ranging from the influential techniques used to recruit members to the various technical means that can be deployed to carry out an attack, this model is by no means a complete depiction of the field. The complex relationships between the behavioural factors and the technical activities make the representation of a dynamic field rather challenging. Rather, the model aims to show a snapshot of the interactions with the various factors.

The model is by no means a flawless representation. Rather it shows a number of technical and non-technical concepts that are relevant within the security and terrorism fields. The model is not a prescript that dictates that cyberterrorism only develops systematically but rather a representation of the field with the goal of encouraging exploration of the topic, and clarifying associated concepts and links. The model therefore aims to assist in the analysis of the field and not serve as a predictive instrument.

Cyberterrorism is a developing discipline and therefore scientific publications in this emerging area are limited. This resulted in the use of many Internet-based references. The concept of cyberterrorism is still being established in the security field and therefore printed resources are not in abundance. Opinions, views and data emerged at a more frequent rate in newspaper and web articles and were therefore used in this research. The concept of cyberterrorism has been adopted at an international level but in the South African context does not feature prominently.

At the time of the research, the author is employed at the Council for Scientific and Industrial Research (CSIR) as a senior researcher in the field of cyber security. As part of her responsibilities, a research project pertaining to cyberterrorism was carried out. This sparked an interest into a dynamic and emerging field. The research entailed carrying out a preliminary literature study on the current concept of cyberterrorism. This led to continued research into the field using various analysis techniques in order to establish the Cyberterrorism Life Cycle Model, which is presented in this thesis.

This study resulted in the publication and presentation of various conference papers, a journal paper, book chapter, science talk, seminar lecture and a number of citations, which are listed at the end of the document (see Section 14). Six of these publications featured at international conferences:

- “*Towards a Conceptual Framework for Cyberterrorism”* was presented at the 4th International Conference on Information Warfare and Security (ICIW) 2009
- *“An Introduction to Emerging Threats and Vulnerabilities”,* was presented at Information Security South Africa (ISSA) 2009
- “*A High-level mapping of Cyberterrorism to the OODA loop”* was presented at the 2010 ICIW Conference in Ohio, USA
- “*Motivation for Cyberterror”* was presented at ISSA 2010
- *“Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure”* was presented at ICIW 2011 in Washington DC, USA
- “*Building an Ontology for Cyberterrorism”* was presented at the 2012 European Conference on Information Warfare and Security (ECIW) in Greece

Other publications include the conceptual framework of cyberterrorism appearing in the *2009 International Journal of Information Warfare (JIW)*, as well as a book chapter contribution in the 2011 edition *of Leading Issues in Information Warfare and Research.* Furthermore, two more peer-reviewed publications were presented at *the Workshop on ICT Uses in Warfare and the Safeguarding of Peace* in 2010 and 2012. The author also provided a lecture at the Ekwinox Information Warfare and Cyberterrorism Seminar in 2009, as well as a science talk at the CSIR, which was featured on the CSIR’s news intraweb.

Additionally, four of the published papers (listed in Section 14) resulted in **nine** citations. This indicates that the research carried out can be applied practically and used by the research community. They are as follows:

- "*Countermeasures to consider in the combat of cyberterrorism*" was cited in
    - "*A dynamic cyberterrorism framework*", which appeared in the International Journal of Computer Science and Information Security vol 10, no 2
    - "*Collaborative and protective measures against cyber warfare in South Africa*", which can be found in the African Security Review Journal vol 21, issue2.
- The paper "*Motivation for cyberterrorism*" is cited in
    - "*A dynamic cyberterrorism framework*" appearing in the International Journal of Computer Science and Information Security vol 10, no 2.
    - "*Understanding cyberterrorism: The grounded theory method applied*" at the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensics (CyberSec).
    - A dissertation entitled "*Culture and Computer Network Attack Behaviour*".
- The third paper "*Introduction to emerging threats and trends to create user awareness*" is cited in
    - "*Broadband broadens scope for cybercrime in Africa*" at the Information Security South Africa (ISSA) Conference 2010.
    - "*Fostering content relevant to information security awareness through extensions*" which appears in the journal Information Assurance and Security Education and Training IFIP Advances in Information and Communication Technology Volume 406.
    - The dissertation "*Comprehensive legal approach to cyber security*".
- The forth paper to receive a citation is "*High-level mapping of cyberterrorism to the OODA loop*".
    - The citation appears in the paper "*Comparing models of offensive operations*" at the 2012 International Conference on Information Warfare and Security.

The accompanying CD contains these publications and presentations. In addition, videos of the logic tester, ontology and simulation can be found on the accompanying CD.

The reporting of the research in this thesis is made up of four parts- all of which contribute to the development of the Cyberterrorism Life Cycle (CLC) Model. Figure 1 shows the four parts in chronological order from left to right. This shows the process of developing the CLC Model.

- Part 1: Setting the Scene
- Part 2: Cyberterrorism Field
- Part 3: Development of Cyberterrorism
- Part 4: Life Cycle Model

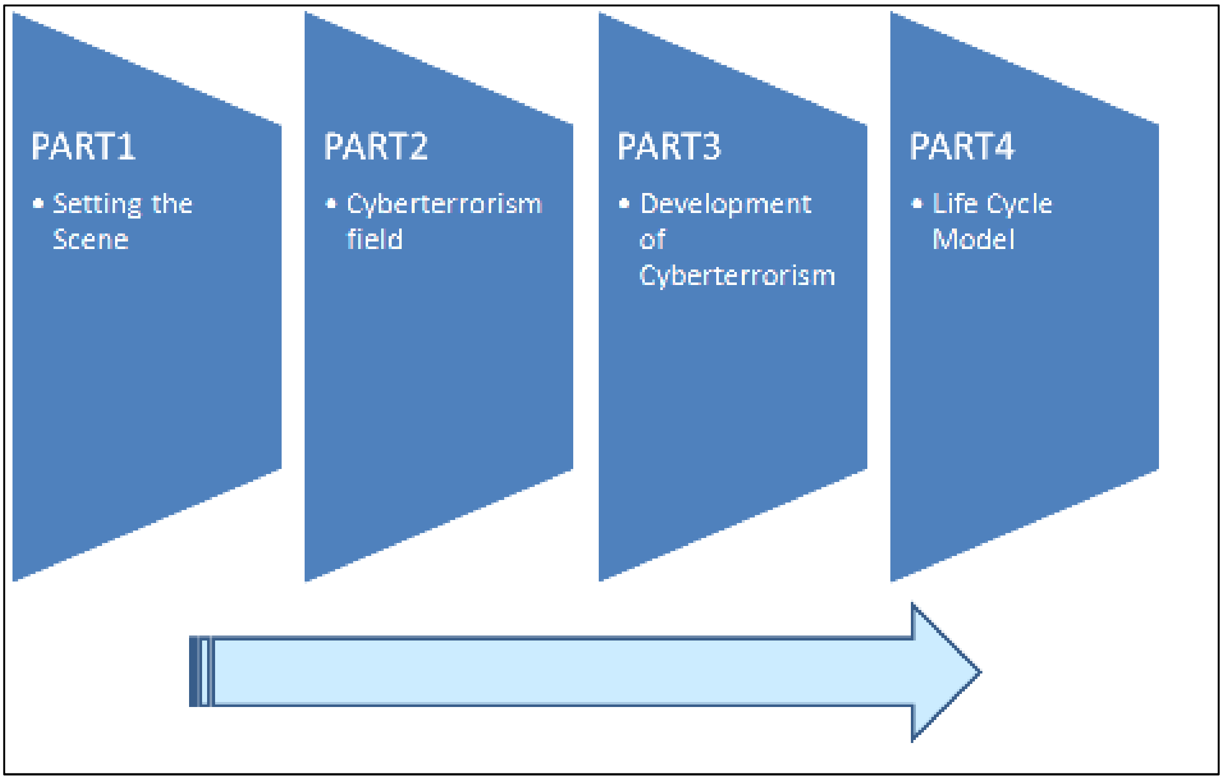


Figure 1: Parts of the Cyber Life Cycle Model Development Study (Own Compilation)

Parts 1 to 3 discuss the various drivers that contribute to the development of the CLC Model. At the end of every chapter, a summary is given of the identified drivers before the next chapter commences. In Part 4, these various factors are brought together to form the CLC Model which is explained in more detail. The final model, presented in Part 4 has five dimensions: Prepare, Acquaint, Choose, Execute and Deter.

At the time of writing, the CLC Model aims to provide an analytic tool for the field of cyberterrorism by representing the various factors relevant to the field. It serves as a foundation to build other models that helps clarify the field. The study addresses both technical and strategic aspects at a high-level and overall presents the interpretation of the author. The study considers various issues related to religious, political and social reasoning together with the various technical means of implementation. The study leaves the room open for further exploration in that the various factors are dynamic and growing. Part 1, Setting the Scene commences the study.

Part 1 Setting the Scene

This study, Cyberterrorism Life Cycle Model is divided into four parts. Figure 2 shows the development of the four parts, and how each part moves from the one part to the next (left to right).

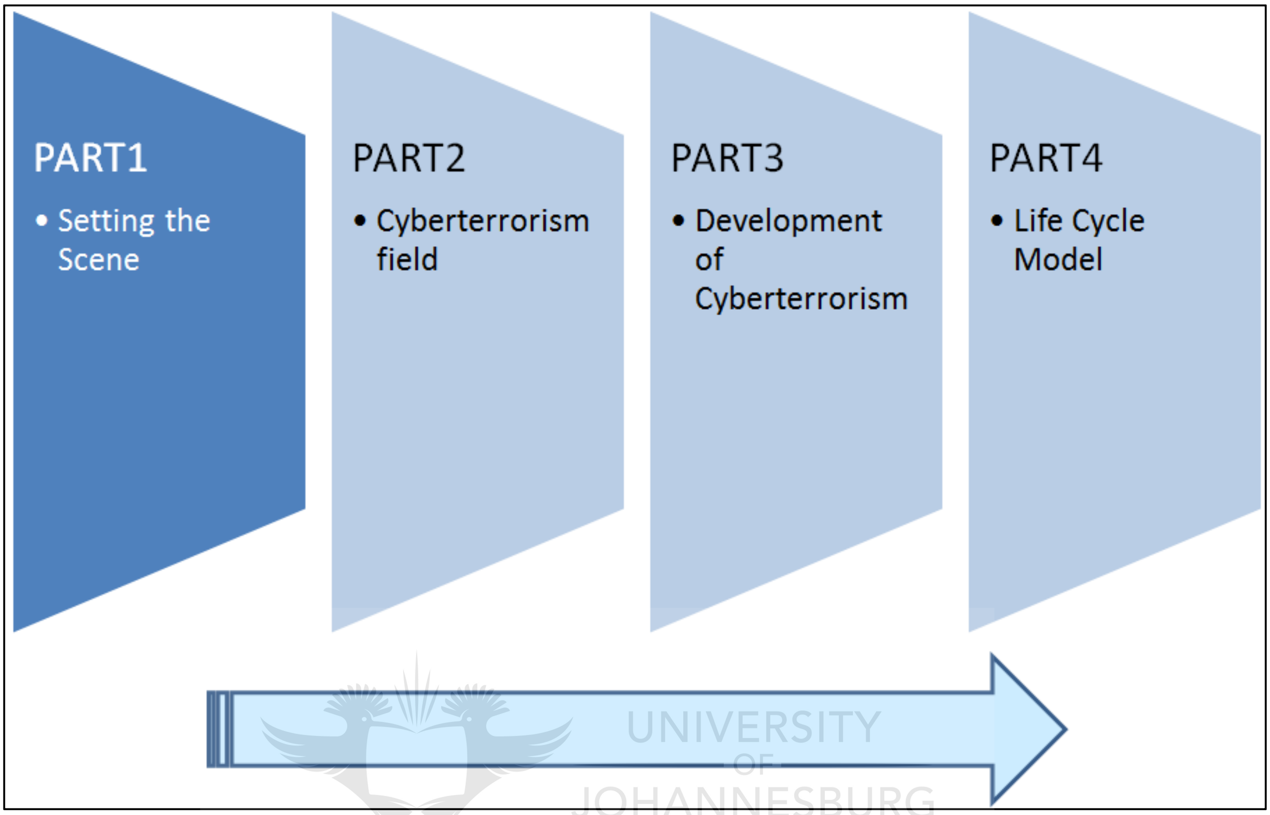


Figure 2: Part 1 of the CLC Model Development Study (Own Compilation)

Part 1, Setting the scene provides a brief motivation to the necessity of understanding cyberterrorism practices. It consists of three chapters which are summarised as follows (The breakdown of all of the chapters is given in Section 2.3):

Chapter 2, Introduction provides the background to the study of the field of cyberterrorism. The chapter addresses the research problem, objectives and methodology for developing the Cyberterrorism Life Cycle Model. The chapter also discusses the limitations of the study. Chapter 3 is an introductory chapter in that it covers the administrative components of the study.

Chapter 3, Background introduces a number of important aspects in the field of cyberterrorism. The chapter provide insight into the operations of terrorist groups, as well as the various influencing factors that are important aspects for the development of the life cycle model.

Chapter 4, Logic Tester looks at the implementation of testing the proposed definitions of cyberterrorism. This chapter provides a practical and dynamic method of testing cyberterrorism scenarios.

Once the introductory aspects in Part 1 are covered, the reader should be familiar with popular examples of terrorist groups, activities, as well as some of the basic forces influencing the development and execution of cyberterrorist acts. Part 2 will then provide further background by exploring the field of cyberterrorism more deeply by discussing influential forces and the use of the Internet. Chapter 2 will now provide the formal introduction to the field with the discussion of essential concepts and popular examples.

2 Introduction

> *"While the vast majority of hackers may be disinclined towards violence, it would only take a few to turn cyberterrorism into reality."*
>
> *- Dorothy Denning*

Chapter 2 introduces the topic of cyberterrorism. The chapter provides a background to the field and discusses the approach of the research by explaining the research problem, objectives and methodology for developing the CLC Model. The chapter commences with an argument for the necessity of the study.

ICT provides a myriad of opportunities for users to carry out business, training, shopping and various other recreational and professional activities. However, associated with its capabilities comes cybercrime and the potential for ICT infrastructure to be exploited. Wilson (2008) mentions that cybercrime is growing into a more organised and established transnational business with the potential for renting various technological online skills to various types of customers, including nations states or agents or groups stemming from terrorist groups. Automated tools can now be used as weapons to target nation states and possible affect national security.

Estonia is an example of digital invasion in which the country was targeted on almost every digital front with a wave of attacks aimed at essential electronic infrastructure (Davis 2007). The attacks crippled government systems and left users unable to make use of on-line services like newspapers and banks.

The origin of the attacks stemmed from the movement of a war memorial originally erected in Tallinn to honour Russian-Estonians who were killed during clashes with the Nazis in World War Two (Traynor 2007, Vamosi 2008, Von Solms 1996). The Russian government was assumed to be responsible for the attacks but upon investigation it was discovered that the attacks came from around the world. However, the political decision to move the war memorial was still a contributing factor that set off the upheaval and resulted in the digital onslaught campaign.

Nations cannot afford attacks on governmental and other critical systems. Disruption of these services interferes with economic, political and strategic activities. Therefore, terrorists recognise the importance of critical information infrastructure (CII) and have realised the impact that attacks on these sectors can have. A digital attack is not limited by physical boundaries and through a cyberterrorist attack, perpetrators can reach high-profile targets. Cyber terrorists or enemy specialists as they have become known, attack a country's critical infrastructure through cyberspace, either using indirect methods like carrying out Denial-of Service attacks, which influence the availability of information services or direct methods like targeting a national electricity grid (Von Solms, Van Niekerk 2013). As mentioned, Estonia is an example of such type of attacks.

Terrorism has entered into a new wave, as the latest arena to be targeted is cyberspace. The Internet now provides for more innovative uses by terrorists. Weimann (2014) points out that terrorist groups have moved their online presence to outlets like Youtube, Twitter, Facebook and Instagram. The Internet has become a playground to reach a multitude amount of potential recipients, recruitees and enemies electronically. Social networking sites, blogs, forums, gaming sites, chat rooms, and discussion groups are typical examples through which recruitment takes place. The global popularity of social networking technologies has led to a large pool of potential recruitments.

Cyberterrorism has developed as an emerging threat in the ICT environment. Various advantages are offered by ICT including, affordability, remote accessibility, ease of use and the ability to reach an enormous amount of targets. An ordinary cyber attack could incorrectly be perceived as cyberterrorism. However, a closer inspection of cyberterrorism will reveal that it has differing reasons, attack goals, techniques and effects than cybercrime. Cyberterrorism, similar to terrorism in general, stems from religious, social, ideological and political motivations. Cyberterrorists tend to seek a high impact to create publicity for their cause, whereas cybercriminals prefer to have their activities remain undetected in order to disguise their fraudulent transactions, theft or acts of espionage.

Terrorism brings with it a wave of potential devastation and uncertainty. Terrorism can now span global borders in that ICT has become both a prime target and weapon to perpetrate and cause onslaughts on innocent victims and high-profile points of interest.

2.1 Research Problem

In the past, terrorism operated mainly in the realm of bombings, gas attack and kidnappings. It has shifted into a new domain as the latest battleground for terrorism has now become cyberspace. The main problem to be addressed in this research is the demonstration of the development of a cyberterrorist. Innovative and traditional usage of the Internet will be investigated to indicate the influential roles they play in the development and coordination of cyberterrorist activities. Another important issue that that will be addressed in this research is the supportive role that the Internet plays to terrorism. Through the compilation of a life cycle model, the growth and progression of a cyberterrorist can be studied and better understood to identify possible countermeasures and intervention methods.

Since cyberterrorism relies on both behavioural influence to initially motivate and thereafter technical skills to execute an attack, there is no defined systematic process that explains the life cycle of cyberterrorism. The supportive role of the ICT for terrorism is also misunderstood. As such, there is a requirement to better structure the various aspects relevant to the field of cyberterrorism. The main aim of the study is to compile a life cycle model that demonstrates the development of a cyberterrorist and how ICT can support terrorism. The model will serve as an analysis tool to help understand the influential drivers that contribute to the growth of a cyberterrorist.

2.2 Research Objectives

This thesis aims to provide insight into the dynamic interaction of various influential and emerging drivers in the field of cyberterrorism by building a life cycle model. The main premise of the thesis is to show that there are various behavioural and technical aspects that influence the development of cyberterrorism. Since the field is influenced by a multitude of motivational and operational drivers, it is necessary to explain the field using various types of modelling techniques. This will help demonstrate to the reader the dynamic nature of the significant drivers that are relevant to cyberterrorism.

The proposed model for cyberterrorism (CLC) will be compiled from the study of influential drivers that are based on different modelling techniques. This includes a logic tester to initially classify a cyberterrorism incident based on its defining properties (Chapter 4). Chapter 5 discusses a framework of the influential factors in the field of cyberterrorism. Chapter 6 discusses how the Internet is used by cyberterrorists for traditional and innovative uses. Chapter 7 investigates social factors influencing the development of cyberterrorism using the Partial Least Square Path Modelling (PSL PM) technique. Cyberterrorism is then mapped to the Observe-Orient-Decide-Act loop in Chapter 8, before it is modelled using ontologies in Chapter 9. Possible countermeasures are covered in Chapter 10. Chapter 11 presents the CLC model which is compiled based on the drivers presented in Chapters 3-10. In addition aspects of the CLC model are simulated in order to show the dynamic factors captured in the CLC model (in Chapter 12).

The main objective of this thesis is to compile a model that traces the development of a cyberterrorist by demonstrating how the Information Communication Technology (ICT) can be used both in the pursuit and support of terrorism. The importance of this life cycle model lies in revealing the deceptive and ingenious methods that terrorist organisations could employ to attract members into their group and thereafter train members to plan and execute terrorist missions. The research objectives builds on showing how ICT can serve as a powerful command and control tool in the support of terrorism. The life cycle model can also depict the movement and attraction of terrorists into cybercrime syndicates and their innovative use of technology.

To achieve, this objective it is necessary to investigate the various influential factors that are relevant in the field of cyberterrorism. This research follows the approach of investigating the relevant factors to establish a model, which depicts the interaction of these factors that could also lead to the identification of countermeasures to help combat cyberterrorism. The following sub-objectives support the main objective and build up to findings of the proposed model:

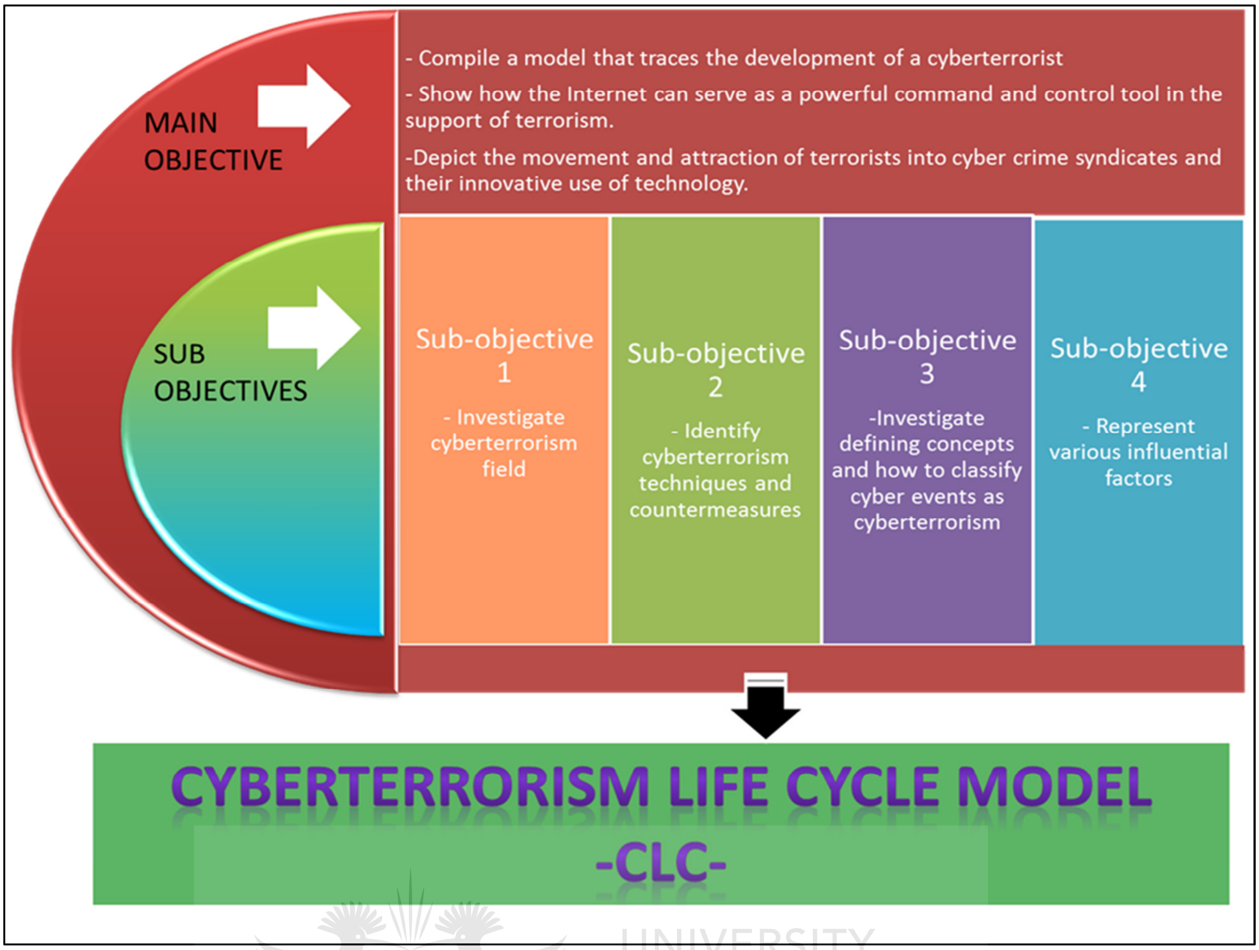

MAIN OBJECTIVE
- Compile a model that traces the development of a cyberterrorist
- Show how the Internet can serve as a powerful command and control tool in the support of terrorism.
-Depict the movement and attraction of terrorists into cyber crime syndicates and their innovative use of technology.
SUB OBJECTIVES
Sub-objective 1 - Investigate cyberterrorism field
Sub-objective 2 - Identify cyberterrorism techniques and countermeasures
Sub-objective 3 -Investigate defining concepts and how to classify cyber events as cyberterrorism
Sub-objective 4 - Represent various influential factors
CYBERTERRORISM LIFE CYCLE MODEL
-CLC-

Figure 3: Objectives of the Study (Own Compilation)

- **Sub-objective 1:** Investigate the cyberterrorism field. A detailed literature study on the field of Cyberterrorism introduces the discipline. In fulfilling this objective, it is possible to identify some important components of the life cycle model.
- **Sub-objective 2:** Identify current cyberterrorist techniques. By looking at the techniques currently applied to carry out cyberterrorism, it is possible to identify possible countermeasures.
- **Sub-objective 3:** Investigate defining concepts and how to classify cyber events as cyberterrorism. It is important to understand whether an incident is actually a cyberterrorist attack or an unclassified cyber event.
- **Sub-objective 4:** Representing the various influential factors to show their interaction and impact. Cyberterrorism is influenced by both motivational drivers, as well as technical measures. It is important to show the dynamic interaction of both motivation and technical measures.

The study will also describe cyberterrorism by using different modelling techniques. The main objectives and sub-objectives direct the research carried out in Parts 1-3. The end of every chapter contains a list of drivers that contribute to the development of the CLC model. Chapter 11 in Part 4 combines all of these drivers and presents the CLC model.

The objectives described for this study are achieved by using various modelling techniques to provide insight into the field of cyberterrorism. This will ensure that context and understanding of the field can be gained. The output of the research will not only be a knowledge gathering exercise but also strive to make an original contribution to the field of cyberterrorism. Due to the wide scope of cyberterrorism and vast span of modelling techniques available, this study can lead to various avenues of supplementary future research.

2.3 Research Plan

The focal point of this study is cyberterrorism. The research entails exploring the field of cyberterrorism using various modelling techniques in order to identify influential factors that are relevant to the field of cyberterrorism. Thereafter a life cycle model will be compiled in order to depict these various influential forces. The study is divided into four parts and thirteen chapters.

Part 1: Setting the Scene

Part 1 investigates and provides the initial background to cyberterrorism. It consists of three chapters that describe the introductory concepts in the field of cyberterrorism. Once the reader is familiar with examples and incidents provided in Part 1, deeper analysis of the field will commence.

- Chapter 2, Introduction, provides the reader with the context for this study. It describes the research problem, objectives, approach, deliverables and limitations.
- Chapter 3, Background to Cyberterrorism, investigates the current state of cyberterrorism relative to the ICT environment. The chapter provides definitions of terrorism and cyberterrorism. Furthermore, this chapter introduces the examples of incidents, terrorist groups, driving forces and relation of cyberterrorism to cybercrime.
- Chapter 4, Logic Tester, looks at a practical implementation of testing the definitions specified for cyberterrorism. This will help classify a cyberterrorism attack.

Part 2: Cyberterrorism Field

Part 2 provides further background to the field of cyberterrorism. It comprises of three chapters of this research study. These chapters introduce the main operating forces, techniques and objectives of cyberterrorism and thus establish the baseline theory. It further develops the knowledge gained in Part 1. The majority of this part looks at determining the main drivers that influence cyberterrorism.

- Chapter 5, Framework for Cyberterrorism, presents a framework of the main operating forces, techniques and objectives. The factors in the framework are not exhaustive but aim to provide the users with the necessary background to understand the factors that influence cyberterrorism. The framework aims to give the reader sufficient knowledge to realise the scope of cyberterrorism.

- Chapter 6, Terrorism use of the Internet: Exploitation and Support Through ICT Infrastructure builds on the framework presented in the previous chapter by discussing in detail, techniques of cyberterrorism, as well as how the Internet can play a supporting role terrorism in general. This chapter aims to indicate the scope of techniques.
- Chapter 7, Determination of Influential Factors using Partial Least Squares Path Modelling (PLS PM), looks at the analysis of survey data to identify the influence of specific social factors in influencing the development of cyberterrorism. The data was obtained from a survey carried out with Dr Tom Holt from the University of Michigan. The author was able to distribute the survey to South Africans and collect these responses.

Part 3: Development of Cyberterrorism

Part 3 forms an important part of this research. This part has three chapters and consists of further models of cyberterrorism that provide for deeper analysis and insight into the field.

- Chapter 8, High-Level Mapping of Cyberterrorism to the Observe-Orient-Decide-Act Loop, looks at a more dynamic representation of the interaction of the various influential factors of cyberterrorism. The knowledge gained in this chapter plays a vital role during the compilation of the CLC model in Chapter 11. This chapter fuses the various influential factors together in order to convey to the user how they relate to each other.
- Chapter 9, Need for an Ontology, discusses the implementation of an ontology to assist with the classification of an event as cyberterrorism. The previous chapters investigated the various factors that are influential to the field of cyberterrorism and this chapter uses this knowledge to build a model that can help determine whether a cyber incident is actually cyberterrorism. This chapter looks at the implementation of a practical model that be used to identify the core characteristics of cyberterrorism and help identify cyberterrorism events.
- Chapter 10, Deterrence of Cyberterrorism, provides a baseline model to develop a countermeasure strategy against cyberterrorism. The chapter addresses countermeasures from both a strategic and technical perspective. Countermeasures are important for the combat of cyberterrorism and thus is vitally important that they be reflected in the CLC model in Chapter 11

Part 4: Life Cycle Model

Part 4 is the crux of this research. It comprises three chapters and presents the pinnacle and conclusions of this study. Part 4 links the entire research study together by presenting the Cyberterrorism Life Cycle Model, built up from the first three parts of the document.

- Chapter 11, Cyberterrorism Life Cycle Model, presents the pinnacle of the study. This chapter combines the various influential drivers into a model and is based on the information gathered in Parts 1 to 3 to represent a reflective, structured model made up of five dimensions.
- Chapter 12, Simulation of CLC Model, describes the implementation of the simulation of the CLC model in order to capture a more dynamic representation of the influential factors.
- Chapter 13, Conclusion, presents the concluding remarks and justifies the development for the CLC model showing the growth and progression of a cybeterrorist.

Research deliverables

Table 1 presents a summary of the previously discussed research plan and indicates the deliverables that are relevant to each chapter. The first ten chapters relate and build on each other to establish the baseline foundation that leads to the compilation of the Cyberterrorism Life Cycle model, presented in Chapter 11. The table also maps the four sub-objectives introduced in Figure 3 to deliverables in a specific chapter. The sub-objectives are not strictly sequential, yet all contribute to establishing the foundation of the research field. Instead, the sub-objectives help in clarifying the different factors relevant to cyberterrorism. These factors thus lead to the establishment of the holistic CLC Model that incorporates all the ideas revealed by the sub-objectives.

Table 1: Project Deliverables (Own Compilation)

Part	Chapter	Deliverable
1 Setting the Scene	Chapter 2	Cyberterrorism background Maps to sub-objective 1: Investigate cyberterrorism field
	Chapter 3	Cyberterrorism definition Maps to sub-objective 3 : Investigate defining concepts and classification of cyberterrorism
	Chapter 4	Logic tester to classify cyberterrorism Maps to sub objective 3 : Investigate defining concepts and classification of cyberterrorism
2 Cyberterrorism Field	Chapter 5	Framework of influential factors Maps to sub-objective 4: Represent various influential factors
	Chapter 6	Cyberterrorism techniques and support role of Internet Maps to sub-objective 2: Identify cyberterrorism techniques and countermeasures
	Chapter 7	PLS Path Model depicting influence of social factors on cyberterrorism Maps to sub-objective 4: Represent various influential factors

Part	Chapter	Deliverable
3 Development of Cyberterrorism	Chapter 8	Model of mapping of cyberterrorism to Observe-Orient-Decide-Act Loop Maps to sub-objective 4: Represent various influential factors
	Chapter 9	Ontology for cyberterrorism Maps to sub-objective 3 : Investigate defining concepts and classification of cyberterrorism
	Chapter 10	Model of countermeasures to combat cyberterrorism Maps to sub-objective 2: Identify cyberterrorism techniques and countermeasures
4 Life Cycle Model	Chapter 11	Cyberterrorism Life Cycle Model Maps to sub-objective 4: Represent various influential factors
	Chapter 12	Simulation of CLC Model Maps to sub-objective 4: Represent various influential factors
	Chapter 13	Closure

The chapters indicated in Table 1 present all of the deliverables. The next section discusses the research approach for the study.

2.4 Research Approach

The main research methodology for this project is explorative and developmental. The research methodology consists of initially studying existing data, and thereafter structuring and linking the information together in various models. Each proposed model in this research aims to analyse a certain aspect of the field to provide for more understanding and insight. The first section of the research focuses on defining the field of cyberterrorism and introducing the user to common terrorist groups and practices. Based on this background information, the reader is familiarised with the reasons and means that terrorists employ.

Thereafter, a further literature study is carried out to investigate in greater detail the operating forces, objectives and techniques of cyberterrorism. The study therefore progresses from a broad discussion of cyberterrorism in Part 1, to a framework of the influential forces and a model of the use of the Internet that will later feed into the CLC model.

Figure 4 presents the high-level approach of the research carried out in this study. It maps directly to Figure 3 with sub-objectives 1-4 leading directly to the development of the CLC model. Figure 4 presents the research approach as a grouped list with each sub-objective providing useful information that eventually feeds into the compilation of the CLC model. Furthermore, each sub-objective covers a more specialised area of research that can be used in the CLC model. The representation shows that the information gained throughout the research study form the building blocks to compile a dynamic CLC model that reflects the cyberterrorism field.

Throughout the study, figures similar to Figure 4 will depict how each sub-objective is addressed. These figures will help show the reader the necessity of carrying out the initial research before the development of the CLC model can commence.

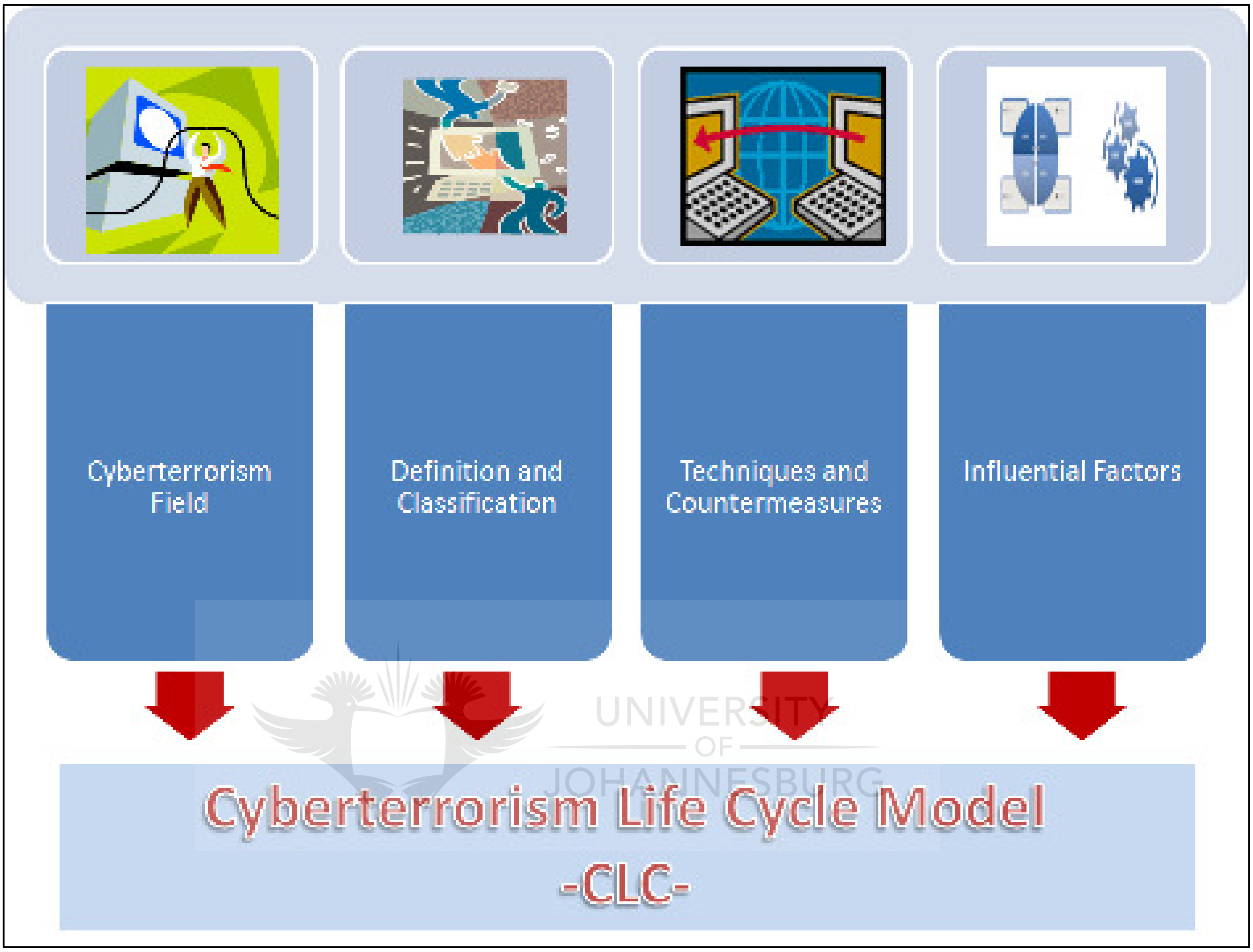

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 4: CLC Model Focus (Own Compilation)

Cyberterrorism spans both the political, religious and ideological world of terrorism as well as the wide-ranging field of cybersecurity which includes cybercrime. The direction of this research study is to show the high-level motivations of political, religious and ideological reasoning, as well as various technical techniques. In addition, countermeasures are also covered at a high-level strategic and technical level.

The study does not cover the scope of the legal issues that relate to cybercrime or public diplomacy at national and international level. The result of the study is to show the dynamic interaction of the various drivers and thus the proposed research study tackles a new problem of representing the interaction of the various strategic, motivational and technical drivers.

Based on the information presented in Chapter 2, it is possible to create a roadmap for the development of the CLC model. Figure 5 shows the high-level roadmap that will guide the reader throughout the document.

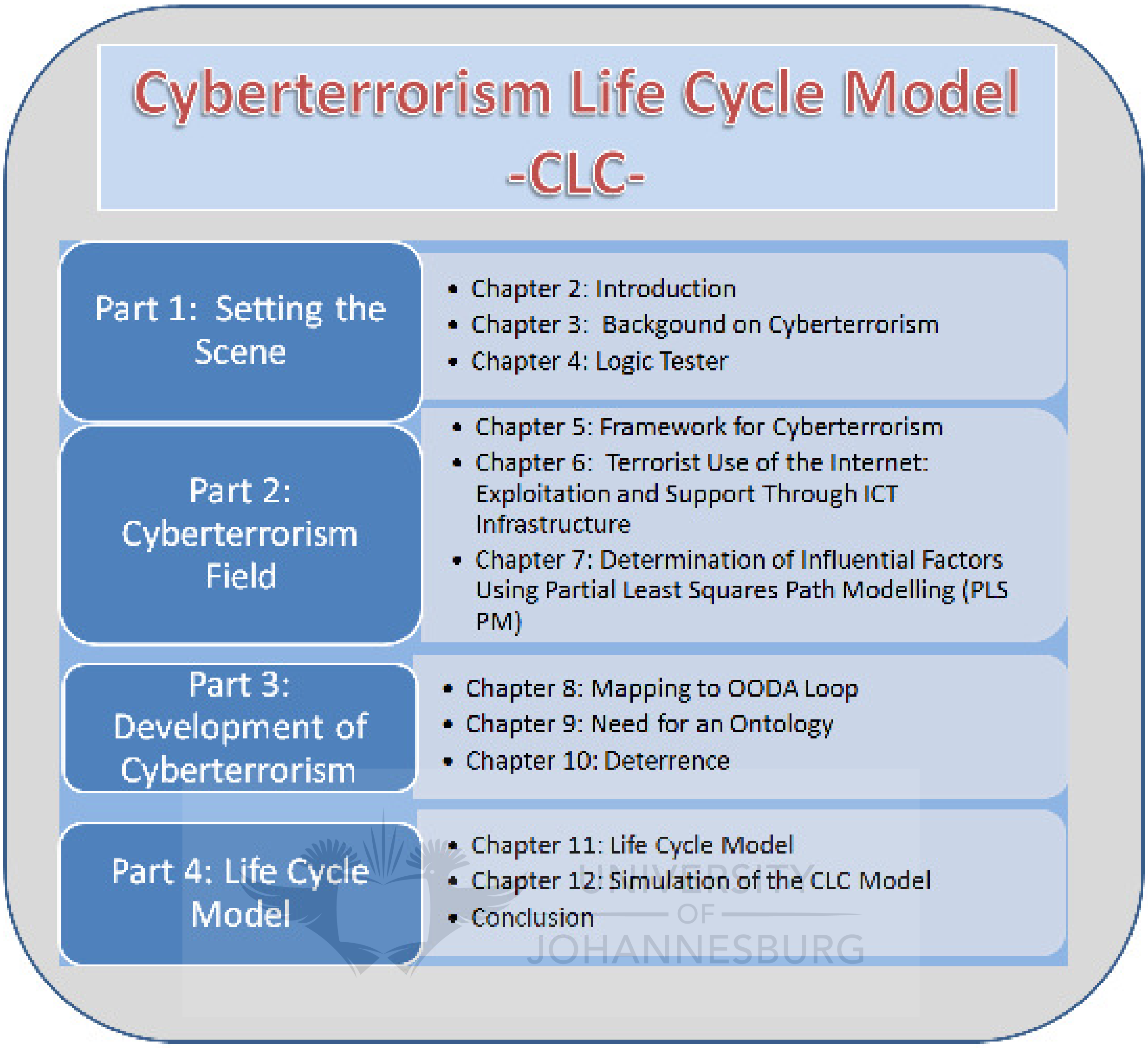

Cyberterrorism Life Cycle Model
-CLC-
Part 1: Setting the Scene
• Chapter 2: Introduction
• Chapter 3: Backgound on Cyberterrorism
• Chapter 4: Logic Tester
Part 2: Cyberterrorism Field
• Chapter 5: Framework for Cyberterrorism
• Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
• Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)
Part 3: Development of Cyberterrorism
• Chapter 8: Mapping to OODA Loop
• Chapter 9: Need for an Ontology
• Chapter 10: Deterrence
Part 4: Life Cycle Model
• Chapter 11: Life Cycle Model
• Chapter 12: Simulation of the CLC Model
• Conclusion

Figure 5: CLC Model Development Roadmap (Own Compilation)

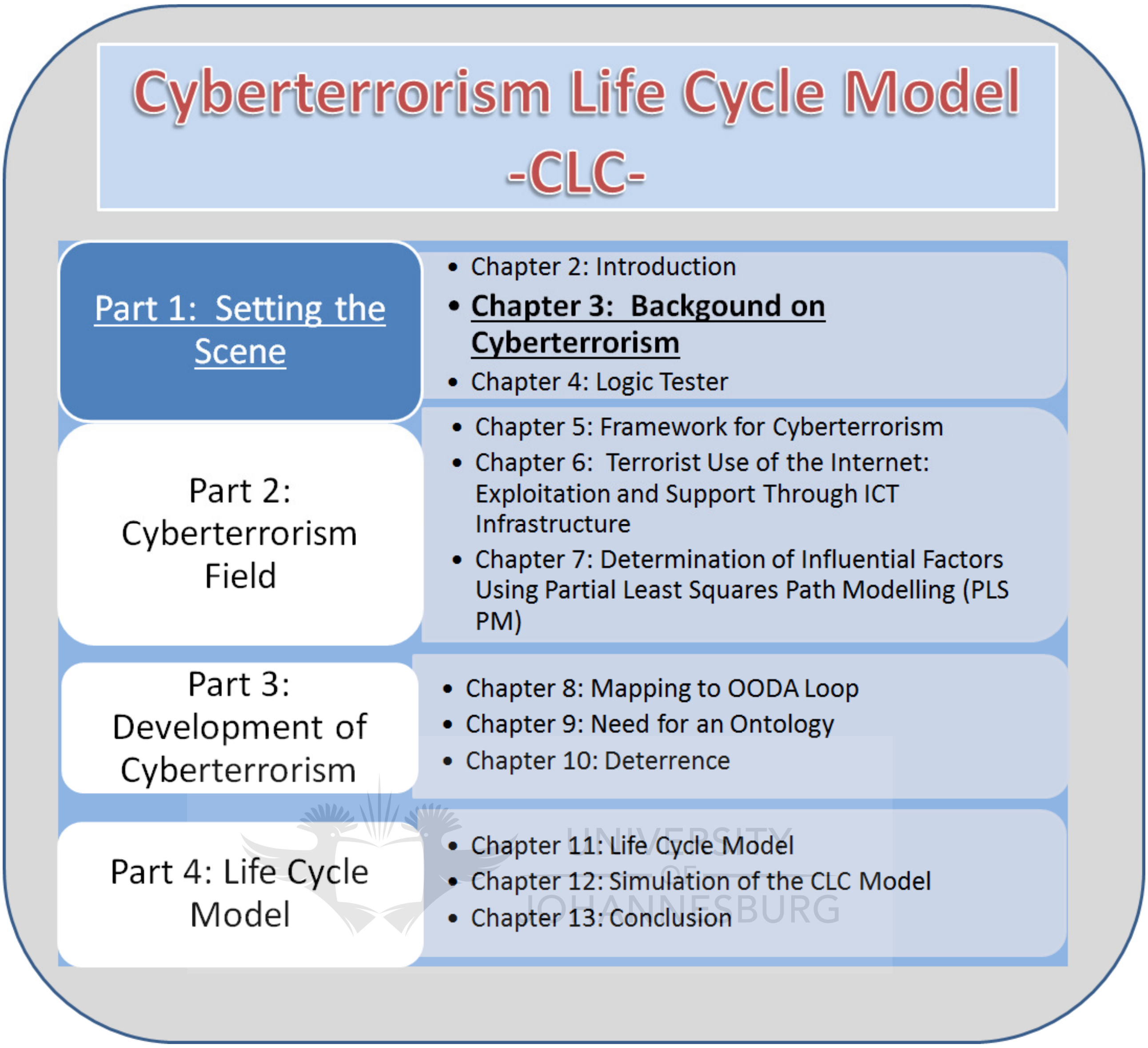
2.5 Limitations

Cyberterrorism is a complex field in that it spans terrorism, cybercrime and cybersecurity and various motivational and technical considerations. Research in the field has to be carried out at a strategic and technical point of view, which is not always controlled by the same authoritative bodies. The legal perspectives of cyberterrorism pose a serious challenge and thus does not form part of the scope of this study.

2.6 Summary

Chapter 2 orientates the reader with the planned research. It provides the outline of the research approach and states the objectives of the study. Chapter 2 helps provide guidance with the aid of figures and tables of the layout of the proposed research and thus help visualise the research plan and scope of the study.

Chapter 3 will now introduce the reader to a number of important aspects in the field of cyberterrorism. This includes the defining concepts, as well as descriptions of a number of terrorist groups and incidents. This introduction is important as it familiarises the reader with the essential characteristics of cyberterrorism, as well as orientates the reader with topical and relevant examples. Chapter 3 addresses both the first and third objective in that it covers the field of cyberterrorism, as well as the defining concepts, which will later help classify cyberterrorism incidents in both Chapters 4 and 9. Chapter 3 is also the first chapter to list a number of drivers that will be used in the compilation of the CLC model.



Cyberterrorism Life Cycle Model -CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- **Chapter 3: Backgound on Cyberterrorism**
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

3 Background on Cyberterrorism

"A cyber- attack could have the same impact as a well-placed bomb. The cyber-terrorism threat is real and rapidly expanding. The risks are right at our doorsteps and in some cases they are in the house."

- Rober Mueller FBI Chief

Part 1 focuses on setting the scene for cyberterrorism. The previous chapter introduced the study at high-level and also discussed the research approach in order to develop the Cyberterrorism Life Cycle (CLC) model. Cyberterrorism lies at the heart of this research effort as it introduces defining concepts which are essential for establishing the CLC model.

Chapter 3 now formally commences the literature study of cyberterrorism. The focus of this chapter will be cyberterrorism, and its related technological techniques and areas of impact.

Figure 6 shows that the cyberterrorism field, as well as the definition and classification thereof will form the focus of Chapter 3. The objective introduces the field and helps establish the foundation of the research to compile the CLC model. It describes the field of cyberterrorism and provides the defining concepts of both terrorism and cyberterrorism. Chapter 3 also discusses various examples of terrorist groups and cyberterrorist attack examples.

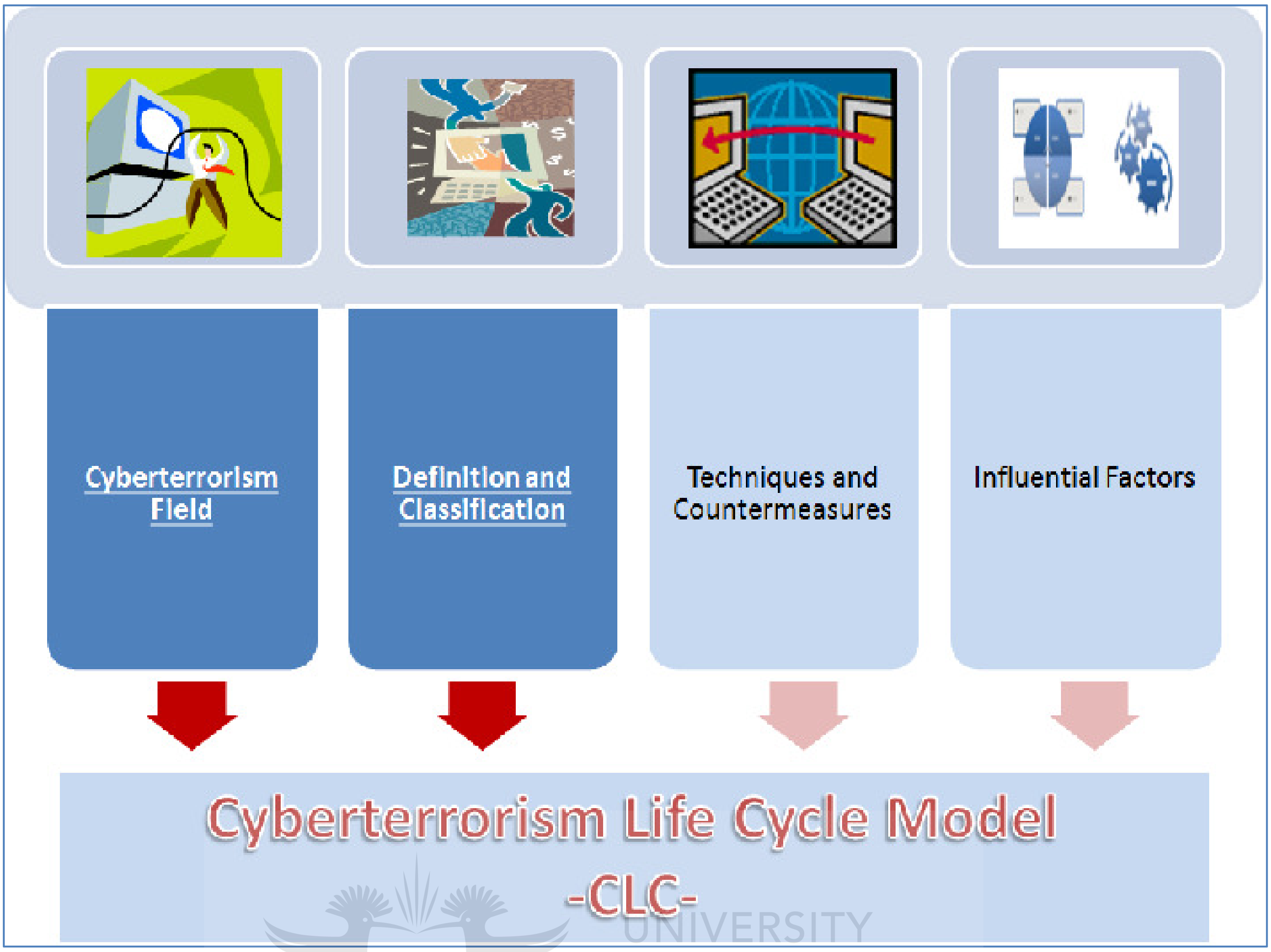

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 6: CLC Model Focus - Cyberterrorism Field with Definitions and Classification (Own Compilation)

This chapter helps develop the foundation knowledge of what constitutes cyberterrorism. This is important for the classification of cyberterrorism incidents.

3.1 Introduction

The terrorist attacks of 11 September 2001 resulted in an aftermath of revolutionary changes. Invaluable lives were lost through a terrorist attack that shocked the world and leaves a legacy for generations to come.

As a result, security in the airline industry was tightened to new levels. The bravery and commitment of the emergency response sector was commended. National policies and the focus on terrorism grew, as the implications of future attacks were put in the spotlight. The tragic 9/11 attacks triggered a roar of public outcry and also raised the need for stronger attention with dealing with terrorist behaviour.

Previously terrorism was only associated with violent activities like bombings, hijackings, plane crashes and nuclear explosions. However, due to the globalisation of digital interaction, the possibility of using cyberspace as a battlefield has also emerged. Colarik (2006) explains that detonating a bomb can create a huge impact but the costs of creation and delivery are high. Instead if a computerised attack is carried out, it can be just as disruptive (even more so) but the costs can be considered minimal in comparison to a bomb. Thus, for a terrorist who may be trying to express some political, social, ideological, or religious message, the world of cyberspace encapsulating the Internet and various networks are becoming a popular medium of choice.

Information and communication support are advancing the technology capabilities of terrorists (Colarik 2006). Technological advancement can help support cyberterror or serve as the target of attacks. De Borchgrave, Sanderson and Harned (2007) explain that the Internet assists terrorists with supportive functions like training, organisation, networking, recruitment and funding. On the other hand, terrorists could also select Information Communication Technology (ICT) infrastructure or systems as their targets and attacks on these systems would have an enormous impact. The US Army Training and Doctrine Command (2006) states that these infrastructures support everyday activities. These operations are very fragile and incapacitating these systems would leave a shattering effect on the defence and economic security of a country.

Cyberterrorism is often debated from two points of view. Desouza and Hensgen (2003) explain that one camp argues that cyberterrorism has not hurt anyone while the other argument tries to show that the threat is real and refers to the economic losses that result from a huge virus sent out over the Internet. The claim that cyberterrorism does not pose a threat comes from the belief that a cyber attack has never really claimed a life. Cyber attacks can cause financial losses, annoyance, and inconvenience but has never killed a person. This line of reasoning tries to show that the Internet is useful for recruiting members or planning operations but it is not the target of mainstream terrorists who want to leave a huge impact. Schneier (2003) has explained that die-hard terrorists are more interested in causing harm than gathering information and that networks can be excellent tools for carrying out propaganda.

However, from the other point of view, life could be lost if critical infrastructures were interfered with. For example if essential services like hospitals, electricity or the airport were tampered with, the effect could be a loss in life. Cyber attacks carried out on infrastructures could become a growing threat, as terrorists gain experience and technology (US Army Training and Doctrine Command 2006). As society's dependency on ICT systems also increases, so does the threat of manipulating the systems to cause widespread terror. Cyberspace has become plagued by hackers and attackers who are all trying to find ways to manipulate systems. Be it economic, pleasure, fraud or even terrorism, if critical digital systems are infiltrated the results could be catastrophic.

3.2 Terrorism

3.2.1 Historical Definitions

In order to understand the concept of cyberterrorism, it is important to clarify the concept of terrorism initially. The idea of terrorism stems from as early as the seventies and most of the defining theories are still relevant and applied today.

The US still utilises the definition provided in the US Code Title 22 Section 2656f (d) since 1983 (US Government 1983). It states that terrorism refers to premeditated political violence carried out against non-combatant groups by sub-national or clandestine organisations or agents with the intention of creating an influence on their target.

International terrorism refers to terrorism that relates to citizens or territorial regions in in more than a single country.

Terrorist groups are any groups that practice or have key sub groups engaging in international terrorism.

Furthermore, the key statutory concepts defined in the United Kingdom Terrorism Act of 2000 (United Kingdom Government 2000) specify that:

(1) ‘Terrorism’ means the use or threat of action where:

   a. The action falls within subsection (2)

   b. The use or threat is designed to influence the government or to intimidate the public or a section of the public, and

   c. The use or threat is made for the purpose of advancing a political, religious or ideological cause

(2) Action falls within this subsection if it:

   a. Involves serious violence against a person

   b. Involves serious damage to property

   c. Endangers a person’s life, other than that of the person committing the action

   d. Creates a serious risk to the health or safety of the public or a section of the public, or

   e. Is designed to seriously interfere with or seriously to disrupt an electronic system

(3) The use or threat of action falling within subsection (2) which involves the use of firearms or explosives is terrorism whether or not subsection (1) (b) is satisfied

According to Ruby (2002), the definition of terrorism emphasises three critical aspects.

Firstly, the motivation is politically motivated. Therefore, violent acts like robbery, homicide or kidnapping that stem from personal or criminal goals are not terrorism. This shows that the social and psychological seeds of personal or criminal acts differ from those associated with terrorism.

Secondly, terrorist acts are aimed at non-combatants. Non-combatants relates to members of the civilian population who are not members of the military or involved in hostile military operations. However, terrorist activities can be carried out on military members during peacetime.

The third aspect of the definition states that sub national groups or clandestine agents carry out terrorist acts. This means that nation states cannot commit terrorism. To clarify this point, Ruby (2002) explains that during declared war or announced conflict there is an expectation of attack. This expectation also includes the premise that the attack will likely be on industrial or military complexes. However, clandestine groups do not normally expect an attack and since terrorism is usually random and unexpected it could have a crippling effect.

Nevertheless, national entities can operate in a clandestine manner. For example if a special task force is sent to another country to bomb a building in order to convince that government to change its policies, this will meet the sub national aspect of the definition and such acts would still be seen as terrorism.

Furthermore, terrorism creates fear in not only the victim but also the audience unrelated to the victim. In addition, terrorism could threaten violence and thus create fear without any act being carried out. Thus, far-reaching fear is another critical component of the definition.

3.2.2 Later Definitions

In October 2004, the United Nations Security Council (UNSC) (2004) passed Resolution 1566, which defines terrorism and states that no terrorist acts will be condoned for political or ideological reasons:

Terrorist attacks justified by political, racial, ethnicity, religion, philosophy, ideologies reasoning may include:

- The targeting civilians to cause death or critical injury
- Taking of hostages in order to create a state of terror in a public area on a group of specific people
- Intimidation of the population of forcing of the government or international organisation

Moreover, Ruby (2002) discusses some of the key concepts related to the definition of terrorism. He presents an argument first proposed by Taylor (1988). This argument relates to the classification of terrorism based on the legal, moral or behavioural perspectives.

From a legal point of view, different countries may view acts differently. Therefore, the legal perspectives may be blurred. From a moral point of view, an act can be classified as terrorism if there is no moral justification for the violent act. Many political groups may be willing to carry out violent acts if they believed that they are being morally acceptable. The third perspective from Taylor is behavioural. The behavioural aspects are based on behaviours alone irrespective of the laws and morals associated with the act. This perspective is a good viewpoint in that it does not rely on intricate psychological classifications. However, in many instances, there are political or ideological events that are not terrorist in nature.

From a psychological point of view, terrorism evokes the emotions of terror, fear and grief. Terrorist activities appear to be random and senseless and using violence can affect the civilian population. Another psychological aspect is their motivation, which can be political, religious, social or ideological.

Furthermore, both the Philippines and Australia consider terrorism as being related to the interference of electronic systems or affecting critical infrastructure. Australia's Security Legislation Amendment (Terrorism) Act (Australian Government 2002) indicates that terrorism can consist of actions that:

a) Creates a serious risk to the health or safety of the public or section of the public

b) Seriously interferes with, seriously disrupts, or destroys an electronic system including, but not limited to

   i) An information system, or

   ii) A financial system, or

   iii) A system used for the delivery of essential government services, or

   iv) A system used for, or by an essential public utility, or

v) A system used for, or by a transport system

The Philippines' Anti-Terrorism Act (Phillipines 2003) describes terrorism as acts that can cause serious interference with, or serious disruption of essential service, vital facility, and critical infrastructure.

3.2.3 Terrorism Definition Summary

A key aspect of terrorism is that it is carried out outside the rules of society. Overall, many acts may not be clearly defined as terrorism. For example, if a nation's citizens are being tortured and they rebel against a corrupt government, would this be considered terrorism? This is a tricky question to answer and the debate will continue to rage over the key constituents of a terrorism act. However, some key concepts emerge and will be summarised. The author therefore proposes her own working definition of terrorism based on existing definitions:

Threats or actions that fall into and either sub-section (1) or (2) and sub-section (3).

1. Threats or actions to intimidate the government or the public, or
2. Threats or actions to promote a political or ideological issue
3. Threats or acts of serious violence
    a) Against people, or
    b) Causes major damage to property, or
    c) Harms a human life other than the person performing the act, or
    d) Causes a risk to health or safety of people or critical service, or
    e) Aims to cause interference with electronic systems, or
    f) Carried out by clandestine groups or sub-national groups
4. EXCEPTION: A threat or action that falls into condition 3 and involves firearms/explosives is terrorism even if condition 1 is not met.

The critical aspect of terrorism has initially been introduced. The discussion will move on to the clarification of cyberterrorism.

3.3 Cyberterrorism

The discussion now addresses the establishment of a formal definition of cyberterrorism. According to Desouza and Hensgen (2003), cyberterrorism is defined as a purposeful act motivated by personal or political reasons that aims to disrupt or destroy stable organisations or nations using electronic devices targeted at ICT systems like computers, programs and other methods of electronic communication, exchange and storage. Terrorists use coercion to generate support for their cause and can commit violent attacks to force government to meet their demands. Thus, intimidation and publicity are key objectives for terrorists.

Cyberterrorism brings together the ideas of bringing about a reign of terror using the realm of cyberspace. Cyberterrorism thus creates the possibility of using of computer and network technologies to support extremist and aggressive behaviour, stemming from political, religious or social motivations in order to leave a forceful and sometimes brutal effect.

Denning's (2000) testimony before the Special Oversight Panel on Terrorism states:

"*Cyberterrorism is the convergence of terrorism and cyberspace. ... unlawful attacks and threats of attack against computers, networks, and the information… done to intimidate or coerce a government or its people in furtherance of political or social objectives...to qualify a cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear."*

Furthermore, Foltz (2004) looks at the definitions from a number of experts, including Denning, Pollitt and Bronskill and summarises that cyberterrorism is politically motivated attacks or threats of attacks, which are intended to:

- interference with the political, social (Denning, 2000), or economic operations of a group, organisation, or country; or
- promotion of physical violence (Pollitt, 2001) or the unrighteous use of power; or
- combination of actions that may include common terrorist acts (Bronskill 2001).

Furthermore, one of the most popular definitions stems from the Federal Bureau of Investigations (FBI) (2002) . It says that cyberterrorism is the:

"*Pre-meditated politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents*."

In summary, when viewed from the outlook of terrorism in general, cyberterrorism comprises the methods and motivations leading to the exploitation of ICT and should consider the following issues:

- A political or ideological motive
- Theatrical or performance dimension
- Civilian targets
- Criminal and legal implications
- Digital means of threat
- Fear as an outcome
- Non-state perpetrators
- Random or indiscriminate attack
- Threat of violence against people or property

Cyberterror does not necessarily result in violence but does involve the generation of fear and can be considered as the unlawful use of force or violence carried out against information, computer systems and networks with the aim of intimidating or coercing a government, the civilian population, or any group thereof, to promote political, ideological or social objectives.

Various aspects relevant to the definition of cyberterrorism have been discussed. There are varying views and standpoints. Much debate over the definition still rages on and the concept may continue to be interpreted in many contexts. Based on the various definitions from literature, the author thus proposes the following definition:

Cyberterrorism aims to cause interference with electronic systems through threats or actions that fall into either sub-section (1), (2) or (3) and sub-section (4).

1. Threats or actions to influence the government or intimidate the public
2. Threats or actions to promote a political or ideological issue
3. Infliction of harm with the aim of creating fear and shock
4. Threats/actions that:
    a) Harms a human life other than the person committing the act, or
    b) Causes a risk to health or safety of people or critical service, or
    c) Uses digital or physical means to target ICT infrastructure, or
    d) Carried out by clandestine groups or sub-national groups

In the context of cyberterrorism **ideological** issues relates to social, religious and other activist or ethical beliefs. Ideological is the umbrella term for these types of issues driving cyberterrorism**.** Throughout this research, one or more of these terms will be referred to.

The remainder of this study will utilise these defining statements. The definitions will be re-visited in Chapter 4. The discussion now moves on to other issues relevant to cyber terror: potential scenarios, incidents and driving forces.

3.4 Potential Scenarios

Now that the definition of cyberterrorism, have been explored the definition can also be applied to the method of preparations, means of execution and target of attack. Table 2 shows a classification of cyberterrorism based on preparation, means and target. In addition, the definition established by the author (in Section 3.3) is also considered. Potential scenarios are given in order to show the application of the definition and classification.

Table 2: Other Cyberterrorism Definition Application (Own Compilation)

Preparation	Means	Target	Cyberterror	Example
Digital	Digital	Digital	Y	Look for vulnerabilities in search engines, hack system, crash server of government website
Digital	Digital	Physical	Y	Research power plants specifications online, Interfere with electronic systems at a power plant, cause an electrical explosion
Digital	Physical	Digital	Y	Insider recruited to search on the Internet, then buys network card, plugs in card on server, ministerial website server crashes
Digital	Physical	Physical	N	Research on Internet about how to build a bomb, detonate bomb at warehouse
Physical	Digital	Digital	Y	Buy a card, program card, interfere with electronics of server at the stock exchange
Physical	Digital	Physical	Y	Read a book about functioning of power plant, interfere with electronic system at power plant, cause an electrical explosion
Physical	Physical	Digital	Y	Read a book, build a bomb, explode server at cellphone company
Physical	Physical	Physical	N	Read a book, build a bomb, explode empty warehouse

The definition for cyberterrorism can also be applied in other ways. This will be carried out in later chapters.

A debate rages that there has never been any shocking cyber terror attack. Denning (2012) asserts for a politically motivated attack to be considered as cyber terror, it would have to be sufficiently serious to incite terror equal to that caused by violent physical attacks. However, Weimann (2004) says that the distinction between the potential and the actual damage inflicted by cyberterrorism has been ignored. Elrom (2007), too talks about the differentiation between the possibility and the capabilities that could create real chaos and even crash critical infrastructure systems.

Instead of taking that viewpoint that a cyber terror attack is neglible since it is too far-fetched, this research study aims to study the capabilities and impact of cyberterrorism. Furthermore, Prof Goodman from Georgia Tech (Elrom 2007) when addressing the issue of cyberterrorism in November 2004 stressed the importance of the taking cyberterrorism seriously as it could become more of a threat later. Denning has also declared that future terrorists may see the great potential of cyberterrorism than the terrorist of today (in Elrom 2007). She has also said that the next generation of terrorists are experiencing a digital world in which hacking tools provide for a much more powerful, simpler easier and accessible environment (in Elrom 2007).

The discussion now moves on to typical scenarios of cyberterrorism to indicate approaches for carrying out cyberterrorism. Squitieri (2002) envisaged attacks on the following targets:

- A centre for disease control like those dealing with potential attacks involving biological warfare
- Financial networks like shutting down the flow of banking data
- Computer systems that run water-treatment plants that could contaminate water supplies
- Computer networks operating electrical grids and dams
- Facilities which control information flow over the internet
- Communication networks, telephone and emergency centres
- Air traffic control, rail and public transportation systems

Estonia became the target of a series of cyber attacks in April 2007. Targets that came under fire from Denial-of-Service attacks included the Estonian parliament, financial institutions like banks, government targets like the ministries, as well as broadcasters and newspapers (Von Solms 2008). This cyber onslaught resulted in Estonia losing the availability of critical services including the presidential ministries, parliamentary web sites, banks, news broadcasters and other communications services. This incident demonstrates the effect of a substantial cyber attack on a small state largely dependent of ICT technology. In its wake, Estonia has implemented various cyber policies and changes in government to address similar incidents. The case of Estonia is studied globally to gain a better understanding of proactive and reactive measures to institute from a defensive point of view.

The threat of cyberterrorism has strong ties to cybercrime. However, a deeper analysis of the role that ICT infrastructure plays in cyberterrorism can help provide insight in the influencing factors that drive cyberterrorism. The Denial-of-Services on the Estonian networks is just one example of the disastrous consequences of cyber attacks. Now that a few hypothetical scenarios have been proposed, actual incidents are now discussed. This help show how cyberterrorism can be carried out.

3.5 Incidents

A few incidents will now be discussed to describe actual scenarios and briefly indicate the range of attack motivations. Supervisory Control and Data Acquisition Systems (SCADA) are often prime targets for cyber attacks, as the damage is far wider reaching and the impact greater than attacking a stand-alone machine for example. Political driven attacks and revenge retaliation are amongst other reasons driving cyberterrorism.

3.5.1 Australian Sewerage

In November 2001, Vitel Boden was convicted for his attack on the sewerage system in Australia (Lemos 2002). With the use of a wireless radio and stolen control software, the former consultant on the water project tool released one million litres of sewerage along the Queensland coastline. After having being refused a full-time position, the disgruntled employee sought revenge. This incident indicates the advantage that insider knowledge and accessibility to necessary control software can have. The result was a loss of marine life, discolouration of the creek and a horrendous odour for the nearby residents. Whilst this incident is revenge driven, it does indicate the possibility and effect of an attack to key infrastructure.

3.5.2 India Pakistan Conflict

An actual example of cyberterror stems from the conflict between the nations of India and Pakistan. The tension between the two states has boiled over into the electronic domain with each targeting the other over the Internet. G–Force and Doctor Nuker are two Pakistani hacker groups that have been linked to incidents involving the Indian Parliament, the television network Zee, the Asian newspaper and the Bhabha Atomic Research Centre (Elmusharaf 2004, Puran 2003, Supercourse lectures 2008, Vatis 2001). Five megabytes of sensitive nuclear research data is believed to have been downloaded by unauthorised parties. This indicates the exploitation of critical systems and the political motivation driving such activity.

3.5.3 Estonian Denial-of-Service

A well-known example is the wave of cyber attacks against Estonia in 2007. The upheaval stems from the movement of a war memorial in Tallinn honouring Russian-Estonians who lost their lives fighting Nazis in World War Two (Traynor 2007, Vamosi 2008, Von Solms 2008). The relocation by the Estonian government caused great dissatisfaction, mainly among the Russian camp. In retaliation, several websites of Estonian organisation were hit with multiple requests.

The targets included parliament, banks, political parties, ministries, newspapers and broadcasters (Von Solms 2008). In response to the cyber onslaught, accessibility to foreign sites was closed down. This would try to ensure that local users could still gain access. North Atlantic Treaty Organisation (NATO) help was sought to identify the source of the attacks and try to strengthen the Estonian defences (Traynor 2007). The distributed Denial-of-Service attacks saw many governmental and communications organisations flooded with thousands of requests. Initially the attacks were believed to have originated from Russia, but later investigations show global activity using zombie networks from around the world could be attributed to the attacks.

3.5.4 Georgia Russia Animosity

Another example is that of the conflict between Georgia and Russia. A summary of the findings from Yau (2008) and Traynor (2007) follows. The controversy stems from the battle over the Georgian province of South Ossertia and had since moved into cyberspace. A series of Denial-of-Service and web defacing incidents occurred in 2008. The Georgian presidential web site and other governmental sites were targeted.

Thereafter, warnings appeared on blogs cautioning users to be mindful that information on official sites may have been tampered with. Reports show that the Georgian Ministry of Foreign Affairs set up a blog hosted by Google stating, “A cyberwarfare campaign by Russia is seriously disrupting many Georgian websites including the Foreign Affairs.” The infamous cybercrime group RBN (Russian Business Network) placed posting on their blog that the messages on the Georgian websites should not be trusted. One such posting read as follows: “We provide an important reminder to use caution with any websites that appear of a Georgian official source but without any recent news… as they may be fraudulent.” Other blog messages warned that many of the Internet servers in Georgia were being controlled externally (largely by Russian servers).

The initial attacks were seen to focus on the communications, parliament and news organisations (Yau 2008).. The National Bank of Georgia was not spared and had their web site defaced with the placement of images of 20-th century dictators. An image of the Georgian president Mr. Saakashvili was also placed on the site. Other findings show that the Internet traffic was being redirected through Russian telecommunications firms. Russian telecommunications companies hosted centres with controlling software that rerouted Internet traffic. It was also found that the Russian-language web site stopgeorgia.ru hosted DDOS software for download.

Other malicious activity included botnets sending a flood of useless data at Georgia computers. The attacks were believed to be linked to the St-Petersburg based criminal gang Russian Business Network (RBN) due to the use of the same attack tools and commands and even the detection of the source of the attacks matching computers the gang was known to control (Traynor 2007).

Thus typical activities that seem to occur are Denial-of-Service attacks (causes disruption to critical services and leaves a wave of dis-connectivity and associated uncertainty) and web defacement (to alter the contents of web sites and spread other political/social messages). Hacking and botnets are used to facilitate these types of malicious activities.

In the field of cyberterrorism, various security exploitation techniques can be used to carry out an attack but an essential aspect is the driving forces behind the attack. Therefore, it is important to look at the motivation or driving force which drives attacks.

3.6 Driving Forces

Various forces like political views and religious objectives can drive terrorism. In some cases, the principles can overlap which makes differentiation difficult. However, studying the driving forces that lead to terrorism can help shed light on the underlying motivation of a terrorist, which results in threatening behaviour. Armistead (2004), Nelson et al. (1999) and Weimann (2004) have explained the following types of terrorism:

- **Religious**: existence of strong theological values and thinking.
- **Ethno-national separatist**: aim to create a new political order, established based on view of ethnic dominance.
- **Revolutionary (Terrorism to the left):** intention is to capture political power.
- **Far-right extremist (Right wing):** based on belief system of superiority.
- **New Age:** tend to focus on one specific contentious issue (for example anti-abortion rights).
- **Hackers:** technical attackers who possess skills to infiltrate and damage systems. Hackers can be driven by activism, financial rewards or simply by the need to challenge themselves.

Whelpton (2009) also mentions the Retributional group as another type of terrorism. Retributional terrorists strongly believe that a fitting punishment should be delved out in order to compensate for a past wrongdoing. This type of reasoning is revenge-driven. Whelpton (2009) explains that the mental condition of such individuals is a normal appearance, without any obvious indicators for psychosis, but reference to the incident may trigger anger and resentment. This type of behaviour can also stem from Post Traumatic Stress Disorder. These types of attackers are rather fragile as their mental state could be unstable.

The distinction behind ordinary cybercrime and cyberterrorism lies mainly in the motivation behind attacks. In the section just discussed, the motivation behind typical terrorist behavior is discussed. The next section will look at more incidents to further demonstrate the reasoning and methods of attack.

3.7 Further Incidents

In Section 3.5 a few incidents were discussed as a means of introducing the range of cyberterrorism attacks. This section will further elaborate on the range, motivation and types of attacks that have been carried out in the past. In many instances, perpetrators aim to cripple critical targets and thus deny access to critical services in an effort to create publicity for their cause. Cyberterrorism attacks are a means of making bold statements for political, social, religious or ideological groups. Now that the motivations have been introduced, the subsequent discussion on further incidents can shed light on why terrorist groups carry out attacks. These examples are taken from Denning (2000) and Nagpal (2005).

3.7.1 White Supremacist

A computer hacker linked to a White Supremacist group, attacked a Massachusetts Internet Service Provider (ISP), which resulted in unavailability of service and damage to a section of the ISP's record keeping system. The incident occurred in 1996. The ISP then attempted to discontinue the hacker's malicious actions of racist messages under the guise of the ISP's name. In retaliation, the hacker published a message stating, "You have yet seen true electronic terrorism." Fortunately, the hacker did not take any further action. This attack shows the execution of web defacements, data modification as well as Denial-of-Service (DoS) attacks in order to promote racist tendencies.

3.7.2 Spanish Protests

The Institute of Global Communication (IGC) was the victim of a flood of email messages in 1998 by Spanish protestors. The flood of messages resulted in the delivery blockage of mail to San Francisco based ISP users. The email bombardment stemmed from the protest against the IGC hosting websites for the Eusakal Heira Journal who was a New-York based publication who provided support for the Basque independence.

Due to the website supported by IGC, the protestors felt that the IGC were condoning the terrorist material from the group Fatherland and Liberation of ETA who are said to be behind the assassinations of Spanish political and security officials, together with attacks on military installations. Spam was sent to chief IGC staff and member accounts in order to flood their web pages using fake credit card orders. This wave of action threatened other organisations using IGC services. The widespread outcry through mail bombings led to the IGC being driven to close down the terrorist supported web site.

3.7.3 Tamil Guerrillas

1998 saw ethnic guerrillas bombard Sri Lankan email accounts with over 800 mails a day. This onslaught lasted two weeks and consisted of a message stating, "We are the Internet Black Tigers and we are doing this to disrupt your communications". This type of terrorist behaviour was difficult to control as the Sri Lankan government prohibited the Liberation Tigers of Tamil Eelam from their web protestation but could do little to shut down their website, which was based in London.

3.7.4 Anti-Abortion

A New Age incident occurred when an anti-abortionist group published a list of doctors carrying out abortions on a web site. Once the doctor's names were published, the public were invited to add information like the doctors' home address, licence plate number and even family names. Due to the disclosure of information, several doctors were attacked and some even murdered. When a doctor was murdered, their name was scratched out on the web site.

As a result, the ousted doctors were reduced to a life of fear and forced to disguise themselves. They also had to resort to protecting themselves with bodyguards and bulletproof vests. Consequently, the case was brought to court and the judge ruled that the publication of such material was the equivalent of death sentences and therefore the site had to be removed. In addition, the affected parties were granted $100 million in damages.

3.7.5 Summary of Incidents

This section provided further examples of incidents. Cyberterrorist incidents may occur in isolation - in retaliation or to publicise a certain cause. However, various operational terrorist groups may be carrying out cyberterrorism as part of their regular activities. The next section therefore addresses activities of well-known terrorist groups to show the support that ICT provides.

3.8 Known Terrorist Groups

In the previous section, a few examples of cyberterrorism were given. The discussion now moves on to the practices of a few well-known terrorist groups. The upcoming sections will focus on how the different groups use ICT as part of their terrorist activities. The discussion will also show the range of motivating forces that drive terrorism as well.

3.8.1 Al Qaeda

The international terrorist group Al Qaeda frequently features in the news headlines. Al Qaeda's main goal is to reinstate a strong Islamic presence throughout the Persian Gulf. While Al Qaeda is well known for its violent attacks, they have also embraced ICT technology and communicate via electronic forums like bulletin boards and emails. This helps to conceal their activities and discovery by counter terrorism agencies. Already in 2004, a report showed that Al Qaeda performed e-fraudulent activities and electronic assaults on French financial institutions (Kramarenko 2004).

3.8.2 Aum Shinrikyo

The Aum Shinrikyo cult's main area of operation is Japan and the group are notorious for carrying out biological terrorist attacks. One of their most famously remembered attacks is the 1995 intentional Sarin gas leak in the Tokyo subway (Olson 1999). Consequently, their cyberterrorism activities was exposed by the Japanese police department in 2000, when it was discovered that Aum Shinrikyo was responsible for the creation of one of the police department's computerised vehicle tracking programs. Before this revelation, Aum Shinrikyo had been able to use the program to gain access to information regarding the locations of marked and unmarked police vehicles (Grobler 2009).

Furthermore, the Japanese police later uncovered that Aum Shinrikyo served as sub-contractors for computer programming companies and developed software for at almost eighty Japanese businesses and ten government agencies. The involvement of Aum Shinrikyo with the software development was a major breakthrough as their connection to the software development was difficult to detect.

3.8.3 Hezbollah

Hezbollah supporters are mainly found in Lebanon and the United States. Hezbollah's main objectives are to create an Islamic theocracy in Lebanon and to remove non-Islamic influences in the Middle East (Grobler 2009). Past practices have been violent in nature and include bombing the United States Embassy, the marine barracks in 1983, as well as the United States Embassy Annex attack in Beirut in which took place in 1984.

From as far back as 1998, Hezbollah operated three websites: the central press office can be reached at (www.hizbullah.org), the second site (www.moqawama.org) describes its attacks on Israeli targets and the third site (www.almana.com.lb) provides news and information (Denning 2000). They have also been known to deface websites and the extent of their cyber activities to support terrorist capabilities may have grown in sophistication over the years.

3.8.4 Hamas

Hamas has a strong presence in Israel and Jordon and their viewpoint is against the Israeli state and in support of forming an Islamic Palestinian state. Previously, Hamas have carried out extensive suicide bombings. Similar to other terrorist groups, Hamas makes uses of the Internet for communication and circulating its philosophy in order to recruit members. It has been reported that Hamas encrypts communications like maps, pictures and emails to hide details relating to terrorist attacks (Denning 2000).

3.8.5 Hammerskin Nation

Hammerskin Nation consists of white power extremists with a strong following in countries like the United States, Australia, Germany, Canada, and England. Their use of ICT to support their terrorist activities includes using the Internet to communicate to members, increase membership through recruitment, and provide links to white power music vendors (Grobler 2009).

3.8.6 StormFront

Like Hammerskin, Stormfront is an example of a white power extremist group. However, this group operates from South Africa. Their origins lie in an online bulletin board system from the early 1990s. In 1995, this then lead to the establishment of a website by a former Ku Klux Clan leader and prominent white nationalist activist Don Black (Grobler 2009). The group received strong media attention in the United States after the broadcast of a documentary by CBS/HBO. The special documentary called Hate.com focussed on white supremacist organisations operating on the Internet. Stormfront were alleged to be involved in influencing an online Fox News poll dealing with racial segregation.

One of Stormfront's members served as a candidate for political office for a major political party. In this, way, their views could be spread to many. Furthermore, the extent of their persuasive practices is also demonstrated by their sophisticated use of the internet. The Stormfront website published material relating to their philosophy, science, home schooling and self-defence. The web site also posted news stories, specific content intentionally targeting children as well as links to other racist groups. In this way, Stormfront built a virtual community to support white extremists' members- families, children and single members.

3.8.7 Boeremag

Another terrorist group that had a strong presence in South Africa is the Boeremag. This group also utilised digital platforms to generate support in South Africa. Newsgroups, email and Short Message Service (SMS) were all used for communication between members. While such activities cannot be seen as acts of terrorism, it does indicate the supportive role that ICT played in aiding the terrorist group. Furthermore, Global Positioning Systems (GPS), helped members plan and execute activities. When members went on trial for their crimes, the stored GPS co-ordinates of revisited locations were used as evidence in their court cases (Grobler 2009).

3.8.8 G-Force Pakistan

In the early 2000's the hacking group G-Force Pakistan was believed to be the most active hacking organisation operating on the Internet. Their goal was to liberate Kashmir through their endeavours and protest action. As part of their campaign to promote liberation, members defaced websites and posted blasphemous and insulting messages (Elmusharaf 2004). G-Force Pakistan's attacks were targeted at the Indian community.

3.8.9 Modern Cyberterrorism

Overall, established terrorist groups are increasingly engaging in the use of ICT so as to promote and assist their movements. More recent examples of hacktivists that hover on the edge of cyberterrorism is the groups Anonymous and LulSec. These groups expose agencies and corporations with systems that have poor security and in doing so have caused embarrassment to these organisations, as well as released sensitive information. The disclosure of information has introduced the risks of identity theft, fraud and other cybercrimes. Furthermore, these groups have threatened to carry out DOS attacks against the Internet's root name servers which could have tremendous consequences.

Now that a few terrorist groups and their potential use of technology in their campaigns have been explored, it is also important to discuss the effects of cyberterrorism.

3.9 Effects

Cyberterrorism can have a major impact of important systems and services. These effects can be economical and operational, as well as the inconvenience of service disruption. Some of the most pertinent effects can include:

1. **Economic and Operational**
    a) Loss of sales: fear of purchasing from a company vulnerable to terrorist attacks
    b) Increased staff: to carry out security or disaster recovery after a terrorist attack
    c) Increased insurance: premiums can be increased after a large claim due to a terrorist attack

d) Loss of intellectual property: theft of classified intellectual property can result in disclosure of trade secrets

e) Forensic investigation: investigating an attack will require a forensic investigation

f) Loss of future revenue: damage to reputation can result in loss in sales

g) Replacement of equipment: equipment can be damaged in a terrorist attack and need to be replaced

2. Indirect

a) Loss of confidence and credibility: customers may no longer trust the security of the organisation

b) Damage to business relationships and public image: a publicised attack can damage organisational reputation

c) Loss of trust by customers: customers may choose to conduct business with more secure companies

3. Inconvenience

a) Network delays: slow service can frustrate customers which may even result in loss of business

b) Disruption to services: inability to access required services

Overall, the effects can range from small to large- scale depending on the impact.

3.10 Conclusion

Chapter 3 introduced the field of cyberterrorism by describing a few incidents and examples of terrorist group activity. This chapter also addressed the distinction between cybercrime and cyber terror.

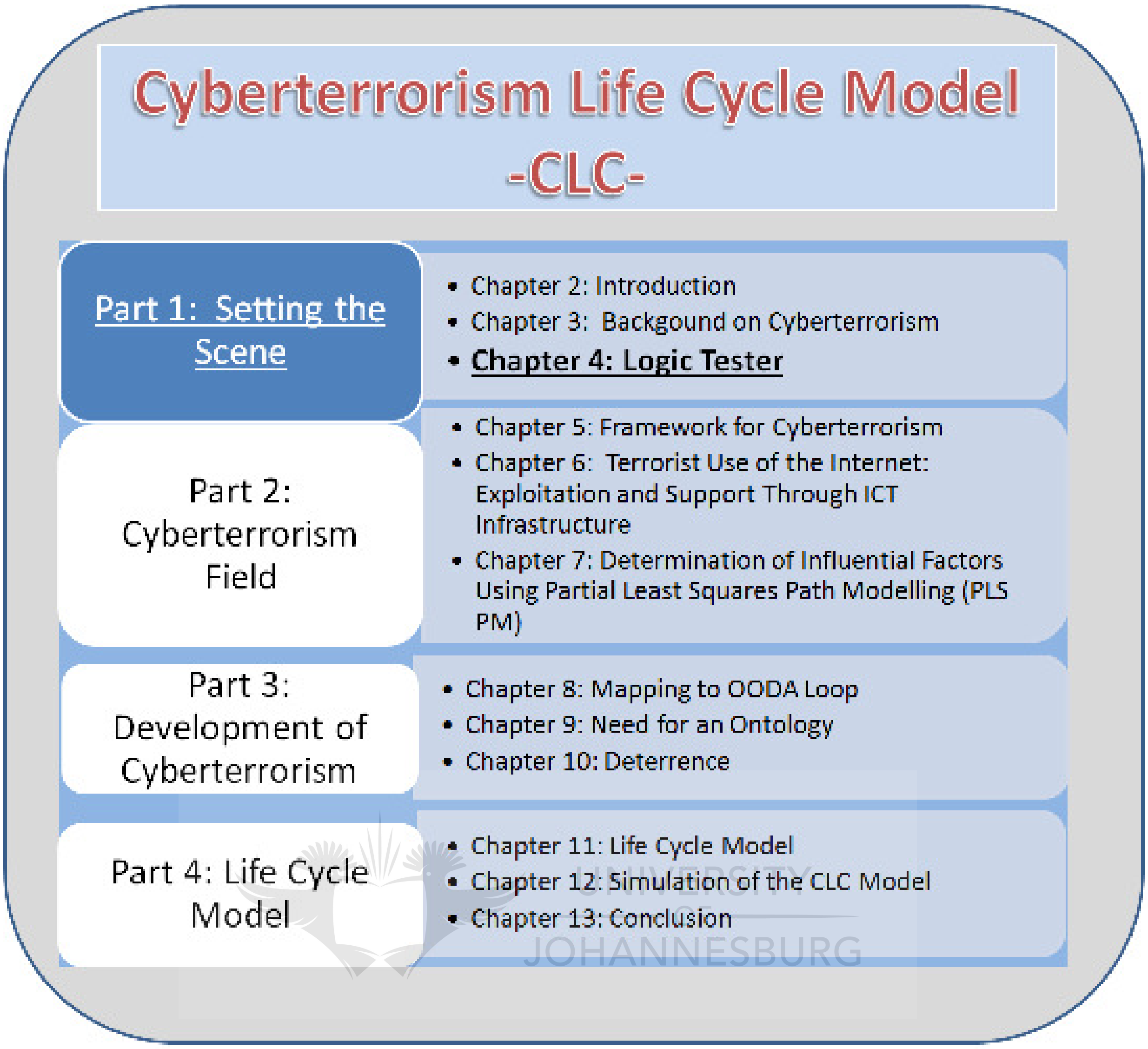
In the cyberterrorism discussion in this chapter, the foundation knowledge is established by explaining various definitions and thereby proposing a summary definition. In addition, this chapter also explored driving forces in the field by discussing the different types of terrorism based on motivating forces.

In summary, the following drivers identified from Chapter 3 contribute to the development of the CLC model:

- The scope of terrorism has now spread to the world of ICT. ICT infrastructure can serve as both a weapon to support an attack or as the target. This idea is important in differentiating between support and attack goals which will be covered in the CLC model (Section 4.2).
- Some of the support functions that can be carried out include training, recruitment, networking and funding (will be discussed in more detail in Section 6.4. The support functions will be covered in greater detail in the CLC model (Section 6.4).
- A formal definition of cyberterrorism establishes the foundation knowledge. The definition also contributes to the CLC model by providing a basic explanation of the field (Section 3.2).
- Cyberterrorism is mainly motivated by political, social or religions reasons. The CLC model will incorporate the different motivating reasons (Section 4.3 and 3.6).
- The descriptions of potential scenarios in this chapter contribute to identifying targets of cyberterrorist attacks which include governmental and critical systems. The CLC model will include the identification of prime targets of attack and facilitation (Section 3.4).

- The incidents and descriptions of the groups crashing critical systems provided in this chapter demonstrate the different practices that are used to carry out cyberterrorist attacks. The CLC model will describe the different practices (Section 3.5 and 3.7).
- Preparation, means and target can be a combination of digital and physical aspects (Section 3.4).

This chapter addressed the motivating reasons driving cyberterrorism by initially providing a few incidents of cyberterrorism, together with practices of known terrorism groups. In this chapter, terrorist groups are also classified. Thereafter, the supportive role of ICT is described. Overall, the reader can gain insight into the motivation of cyberterrorists. Chapter 4 will now test out the definitions of cyberterrorism.



Cyberterrorism Life Cycle Model -CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- **Chapter 4: Logic Tester**

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

4 Logic Tester

> *"These sorts of outsourced cybermilitia attacks are a harbinger of an emerging age of warfare that aims to destabilise societies and economies by throwing communication into chaps, either before or instead of a conventional attack. It's now possible to exercise a grey area of options in an attempt to intimidate a nation-state, either neighbouring or around the world, while maintaining plausible deniability for the incursions."*
>
> *-Joe Gandelman, Editor-in-Chief of the Moderate Voice Hub*

4.1 Introduction

The previous chapter provided a discussion of various aspects defining Cyberterrorism. A definition was established which summarised these core aspects (in Section 3.3). This chapter will look at testing the definition by describing a logic tester implemented in Microsoft Excel.

Figure 7 shows that the focus of Chapter 4 will be on defining and classifying cyber attacks as cyberterrorism. It consists of a practical implementation to test whether an incident can conform to the definitions established in the previous chapter and thus be classified as cyberterrorism. This chapter addresses the sub-objective of clarifying cyberterrorism definitions and helping to classify cyber attacks.

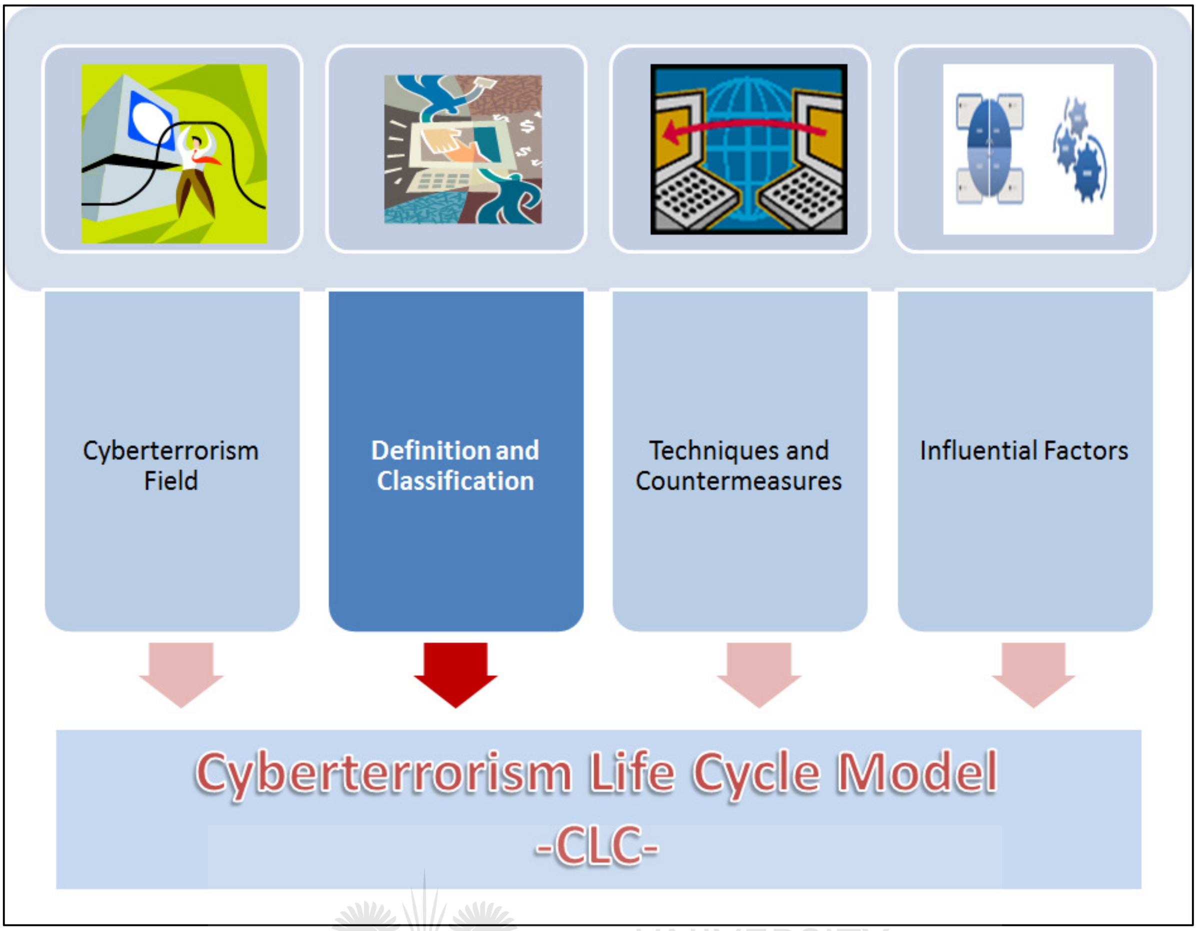

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 7: **CLC Model Focus Chapter 4 - Cyberterrorism Definitions and Classification (Own Compilation)**

Logic is the assessment of reasoning to determine validity (Oxford Dictionary 2014). In this case, the validity of the cyberterrorism definition will be tested. The Logic Tester is used to test the definition proposed to determine whether it can be practically applied to cybercrime incidents and whether they constitute cyberterrorism. This chapter commences with a discussion on the difference between cyberterrorism and cybercrime. These are two important concepts that are sometimes confused. This chapter also summarises concepts related to cyber in order to show how the definition was established and how it is applied in the Logic Tester. This helps justify to the reader the application of the defining concepts in the Logic Tester.

4.2 Cyberterrorism and Cybercrime

In some cases, cybercrime attacks are perceived as being “cyberterrorism”. However, not all cyber attacks are acts of cyberterrorism but could be cybercrime. In this section, the difference between cybercrime and cyberterrorism is explained to clarify the distinction between the two types.

Cyberterrorism consists of two fundamental concepts: cyberspace and terrorism. Cyberspace refers to the abstract global realm, which consists of connected ICT infrastructure including networks, computers, data, systems, processors and controllers. It is a virtual world created by the interconnectivity of networks and information technology. Cyberterrorism is the forceful use of intimidation, or violence against ICT infrastructure in order to influence the government or civilians in furtherance of political, ideological, religious or social objectives. While this definition briefly summarises cyberterrorism, the supportive role of ICT infrastructure is not covered, nor its relation to cybercrime. Therefore, a more detailed discussion is required. This will help clarify the concept of cyberterrorism and how it fits into cybercrime.

Janczewski and Colarik (2008) explain that a new group of potential attackers has emerged in the form of cyberterrorism and this group can be added to the club of “traditional” criminals. With cyberterrorism, computers, networks and cyberspace are used as the target of attacks. In the same light, cybercrime are criminal acts that make use of computer environment, resources, and tools. The key difference is that while both cyberterrorists and cyber criminals may attack computers and networks, the underlying motivation differs. Lachow (2008) has stated that while cyberterrorists try to make a political change and direct their attacks at victims through computer-based violence or destruction, cybercriminals are trying to benefit economically from their victims by carrying out various exploits like fraud, identity theft and blackmail (ransomware).

When a cyber criminal attack has an element of deep fear (system destruction or threat of violence) prompted by a political, social, religious or ideological issue, it can be considered cyberterrorism. Although carrying out an attack in cyberspace is not traditionally associated with terrorism, the generation of fear or interference with critical life-dependant systems could leave a significant impact synonymous with conventional forms of terrorism. When a cyber attack is carried out that strongly promotes a social or political view or even threatens the lives of people, the fear that is generated is comparable to that of a bombing. For example, citizens would be petrified if the computer systems at an airport or railway line were attacked and these vital modes of transport were uncontrollable. Havoc could ensue if aeroplanes or trains were to run without any system control. The creation of fear is a significant component of terrorist acts and the generation of fear through cyber attacks should not be undermined. Terrorists thrive on the psychological edge that is created through the generation of doubt, fear and anxiety.

Henceforth, a vital component of differentiating between cyberterrorism and cybercrime will be the motivation of the perpetrator together with a study of the type of activities carried out. Janczewski and Colarik (2008) explain that the distinction between cyber terror and cybercrime does not merely depend on the mechanics of the event but instead on the intent that drove the person’s actions. Overall, cybercrime does not entail causing wide-scale terror, whereas cyberterrorism does strive for political, social, religious or ideologically motivated attacks on ICT in order to create attention.

Furthermore, Nelson, Choi, Lacobucci, Mitchel and Gagnon (1999) have stated that the political nature of terrorism is what differentiates it from traditional criminal activities, which are largely driven by financial benefits or even personal animosity. On the whole, many computer and network related activities can be used to support cyberterrorism at an execution level but the high-level objectives greatly differ from traditional cybercrime which may include financial gain, economic loss, espionage, annoyance, revenge, fraud. If someone responds to an attack for defensive reasons, this is not considered criminal behaviour. For example, police officers in many instances have to offensively bring down a violent criminal. Similarly, in the defence industry, officers may need to carry out retaliatory action to prevent further injuries or damages. Moreover, Ahmad and Yunos (2012) explain that cyberterrorists actions may cause prejudice to national security and public safety while cyber criminals mainly aim for monetary gain from individuals or groups.

Another contentious issue pertains to computers, networks and cyberspace being the instruments in cyberterrorism or the target of attack. Nelson et al. (1999) states that with respect to cyberterrorism, information can be either a weapon or the target that helps achieve the terrorist goals. Thus, influential to cyberterrorism will be the role that the ICT component plays. Does it facilitate a terror attack or is it the target of the attack?

An important argument to consider is that a political, social, religious or ideological attack on ICT infrastructure should result in the generation of fear, for it to be seen as cyberterrorism. Subsequently, cyberterrorism requires that computer, networks, technology and other components of cyberspace are the target of the attack. Nevertheless, computer and networks related can be used to support terrorist activities in general but their functionality for support activities may not constitute cyberterrorism. For example, various terrorist groups publicise their followings on websites which contain poems, biographies, essays, music, donation requests and contact information. Advertising a group differs greatly from creating a powerful virus to destroy a power plant.

Pollitt (1998) has stated that computers can be referred to as weapons as they act indirectly. The same analogy can be applied to any other weapon. Guns cannot shoot by themselves. In the hands of an assailant, both guns and computers could cause irrevocable damage. It is not the guns itself that kill people; rather it is the people that use the guns. In the context of cyberterrorism, one should consider the intention of the actor and not just their choice of weapon or method of delivery (Desouza, Hensgen 2003). Consequently, the intention of the perpetrator determines whether an attack can be classified as cyberterrorism. With cyberterrorism, an essential aspect of the definition shows the intention to create fear. The next section therefore contains a discussion relating to the motivation of fear.

4.3 Motive of Fear

Embar-Seddon (2002) discusses the difficulty of understanding terrorist attacks together with the fear that is created from the absurdity and randomness of attacks. Terrorist attacks are often unpredictable and news of an attack can cause outrage, fear and anger. When technology is used to execute an attack, fear can be heightened as the channel of delivering the attack is abstract and lacks a solid conceptual structure. The resulting implications are speculative. Connectivity provided by ICT has opened up a world of doors in terms of communication and lack of boundaries but on the other side of the double-edged sword is that impact of a cyber attack can be so much wider than a traditional terrorism act. Without confines of borders and physical access, terrorist groups can plan and orchestrate an attack from the virtual medium of cyberspace. The anticipation of an attack creates anxiousness, which also plays to terrorists’ motives.

Therefore cyberterrorism can be seen as malicious activities promoting a social or political motive. Harmful activities include violence or the threat of violence which aim to cause damage to persons or property or generate fear. Embar-Seddon (2002) further explains that cyberterrorism can be at least as terrifying as the more traditional tactics. Prime targets are computers, networks, and information of critical infrastructures as the impact would be greater and would generate more fear if critical services were disrupted. Sensitive information is also a valuable asset. Whitman and Mattord (2010) has explained that some of the characteristics that give information value in organisations include the confidentiality, integrity and availability of the information. Placed in the wrong hands, the public distribution of personal information, credit card details or corporate sensitive data would cause great outrage.

Pollitt (1998) defines cyberterrorism as the premeditated, politically motivated attack carried out against information, computer systems computer programs and data which may result in violence against noncombatant targets by sub national groups or clandestine agents. Perhaps one argument that can be further made is that cyberterrorism may not always result in acts of violence. In many cases, intimidation techniques can involve threats which in itself put a nation or state into a mode of alert. Stohl (2006) has defined cyberterrorism as a purposeful act or the threat of violence to create fear and/or compliant behavior in a victim and/or audience of the act or threat.

Thus, from a technological point of view cyberterrorism encompasses attacks against computers, programs, networks and data. The issue of pre-meditation in the definition implies that planning and organisation are key aspects of cyber terror attacks.

Government, critical systems and the civilian population often come under fire as greater outrage and publicity can be generated from attacking high-profile targets. Credit is often claimed for attacks in an effort to gather support for a course and make intentions well known. The act is intended to produce effects beyond the immediate physical damage (Embar-Seddon 2002).

Cyber terror, like any other form of terror involves the promotion of ideological, social or political agendas. The tools, and targets are merely reaching into cyberspace and IT based devices and infrastructure. The acts may not be as violent as an explosion, but from a basic point of view the fear that is generated remains. Immense anxiety and concern can stem from the possibility of imminent attacks. The malicious parties can thus create great apprehension in the hearts of a nation with warnings of violence or disruptions to critical services. Thus the underlying goals of fear creation and publicity may still be achieved. Thus, terrorism may have moved into the Digital Age but the fundamental principles of violence, fear and promotion of objectives still prevails.

Another area that causes confusion is the differentiation between hackers, hacktivism and cyberterrorism. Hackers pose a threat as they write exploit code and try to penetrate systems. They usually receive payment for their services or want public recognition for their capabilities. Hacktivism refers to hacking for political reasons. However, how does this differ from cyberterrorism since cyberterrorism also stems from a political motivation? The important aspect to remember is that cyberterrorism involves the infliction of terror. Hackers may try to gain unauthorised access to a system for the enjoyment of the challenge. While hackivists may have some political or social agenda, Ilvonen and Virtanen (2013) explain that hacktivists may just be trying to draw attention to a point they are trying to make. However, with cyberterrorism there is a much more malicious goal in terms of generating fear or co-ercing a government into a certain action and not just publicising a point in an open forum. Ghosh, Prelas, Viswanath and Loyalka (2010) state that cyberterrorism is the abuse of information technology to create violence, damage and fear. Using technology, to cause direct violence, indirectly to damage infrastructure or creating fear in people for a political goal can be considered cyberterrorism. Hacktivists may cause annoyance and slight fear but do not inflict violence or tremendous damage and fear. Hacktivists are usually bent on propaganda rather than damage to critical infrastructures (Industrial Control Systems Cyber Emergency Response Team (IS-CERT) 2005). Thus, cyberterrorism can be distinguished from hacking mainly by the level of violence inflicted together with the fear and damage caused.

Cyberwarfare was explained as actions carried out by a nation-state to infiltrate another nation's computers or networks with the aim of causing damage or disruption (Singel 2010). Furthermore, Pollitt (1998) discusses cyberterrorism and the mis-use of information technology, which may result in violence against noncombatant targets by sub national groups or clandestine agents. Thus, the differentiation between cyberwarfare and cyberterrorism is that cyberterrorism involves non-state actors whereas cyberwarfare may entail governmental and military cyber attacks with the goal of defending national state security. This finding is also an important aspect of the cyberterrorism definition.

Various concepts relating to cyber space and cyberterrorism have been discussed. A summary is now given of these various cyber related concepts.

4.3.1 Summary of Cyber Concepts

Cyber is most commonly associated with computers, the Internet and communication across networks. Related concepts include cyberwarfare, cybercrime, cyber security, cyber espionage and hackivism. The beginning of this study commenced with a terminology list where these terms were briefly explained. This section addresses the links between these terms.

Estonia's cyber security strategy states that threats in cyberspace can be classified in many ways (Cyber Security Strategy Committee 2008). For example, motivational driven attacks can be categorised in three ways: cybercrime, cyberterrorism and cyberwarfare. The strategy also explains that as advanced technologies and attack methods make it difficult to define with any certitude or clarity, the motives driving an attack, threats can also be classified based on methods employed and on the extent of damage inflicted. Thus, various actors are using cyberspace as a battlefield with differing motivations. Germany's cyber strategy explains that criminals, terrorists and spies use cyberspace to carry out attacks and do not stop at state borders (Federal Ministry of the Interior 2011). The strategy also points out that criminals terrorists and spies may not only be the ones carrying out cyber attacks but they may stem from the military as well. Furthermore, the UK cyber security strategy states that various groups like criminals, terrorists, foreign intelligence service and militaries are all operating in cyberspace (United Kingdom Cabinet Office 2011). Due to the anonymous nature of the Internet is difficult to distinguish between these various adversaries.

One of the distinguishing features of cyberwarfare and cyberterrorism is that cyberwarfare takes place between nation states. However, non-state actors carry out cyberterrorism.

The discussion shows that the lines between cybercrime, cyberwarfare and cyberterrorism are blurred. However, through this dissertation the area of cyberterrorism will be defined and clarified by looking at the influential factors that describe amongst others the motivational reasons, techniques and impact. This will help in placing the field of cyberterrorism in context of cybercrime and cyberwarfare. Throughout this research, the factors that are critical to cyberterrorism will be discussed with the goal of providing insight into how cyberterrorism forms part of cybercrime and cyberwarfare.

Ashenden (2011) summarises various assertions made by Dunn Cavelty (2010) and presents a cyber-escalation ladder of various cyber threats. The model helps to frame the various cyber related concepts. Figure 8 shows the threat model.

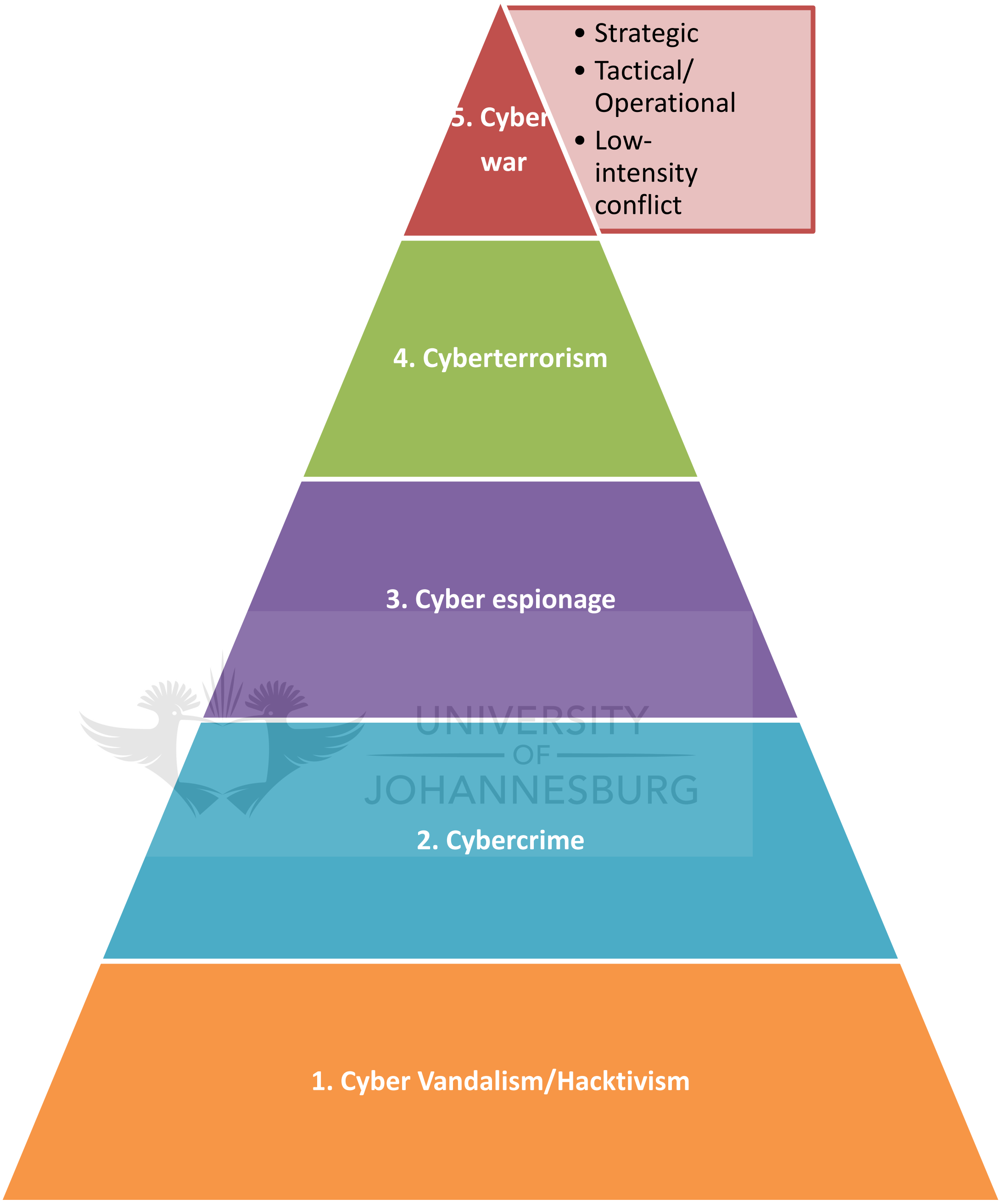


Figure 8: Cyber Threat Model (Dunn Cavelty 2010)

Furthermore, Lehto (2013) explains the threat model as follows:

- **Level 1**- consists of cyber hacktivism, which entails cyber vandalism, hacking and hactivism. When carried out against a company or individual, it can result in great economic losses. An example is previous hacker activities by the group Anonymous.
- **Level 2**- consists of cybercrime, which involve the carrying out of criminal activities using electronic networks and information systems.

- **Level 3**- consists of cyber espionage which is obtaining secret information (sensitive, proprietary or classified) from the individuals, companies or opposing groups to gain political, military or economic advantage which are carried out using illicit means on the Internet, networks of computers.
- **Level 4**- cyberterrorism is the use of networks to attack critical ICT systems and their controls. The aim of cyberterrorism is to damage systems and create fear to force politicians to meet demands or create publicity,
- **Level 5**- Cyberwarfare is made up of three entities: strategic cyberwarfare, tactical/operational cyberwarfare and cyberwarfare in low-intensity conflicts. The definition of cyberwarfare is still debated but is commonly used to refer to operations between state-actors in cyberspace (which may form part of military operations).

Now that various definitions from various experts in the field have been provided and analysed, the discussion moves on to testing the definition in the Excel developed Logic Tester.

4.4 Logic Tester Context

The beginning of this chapter explained that the purpose of the Logic Tester would be to determine the validity of the reasoning in the definition. The previous sections in this chapter justified the reasoning of the definition. Another purpose of the Logic Tester is to show how the definition can be practically applied to classifying a cyber incident as cyberterrorism if it meets certain conditions specified in the definition. The Logic Tester is therefore implemented using these conditions from the definition as input.

The reader is reminded that the definition established by the author in Chapter 3 stated that:

Cyberterrorism aims to cause interference with electronic systems through threats or actions that fall into either subsection (1), (2) or (3) and sub-section (4).

1. Threats or actions to influence the government or intimidate the public
2. Threats or actions to promote a political or ideological issue
3. Infliction of harm with the aim of creating fear and shock
4. Threats/actions that:
    a) Harms a human life other than the person committing the act, or
    b) Causes a risk to health or safety of people or critical service, or
    c) Uses digital or physical means to target ICT infrastructure, or
    d) Carried out by clandestine groups or sub-national groups

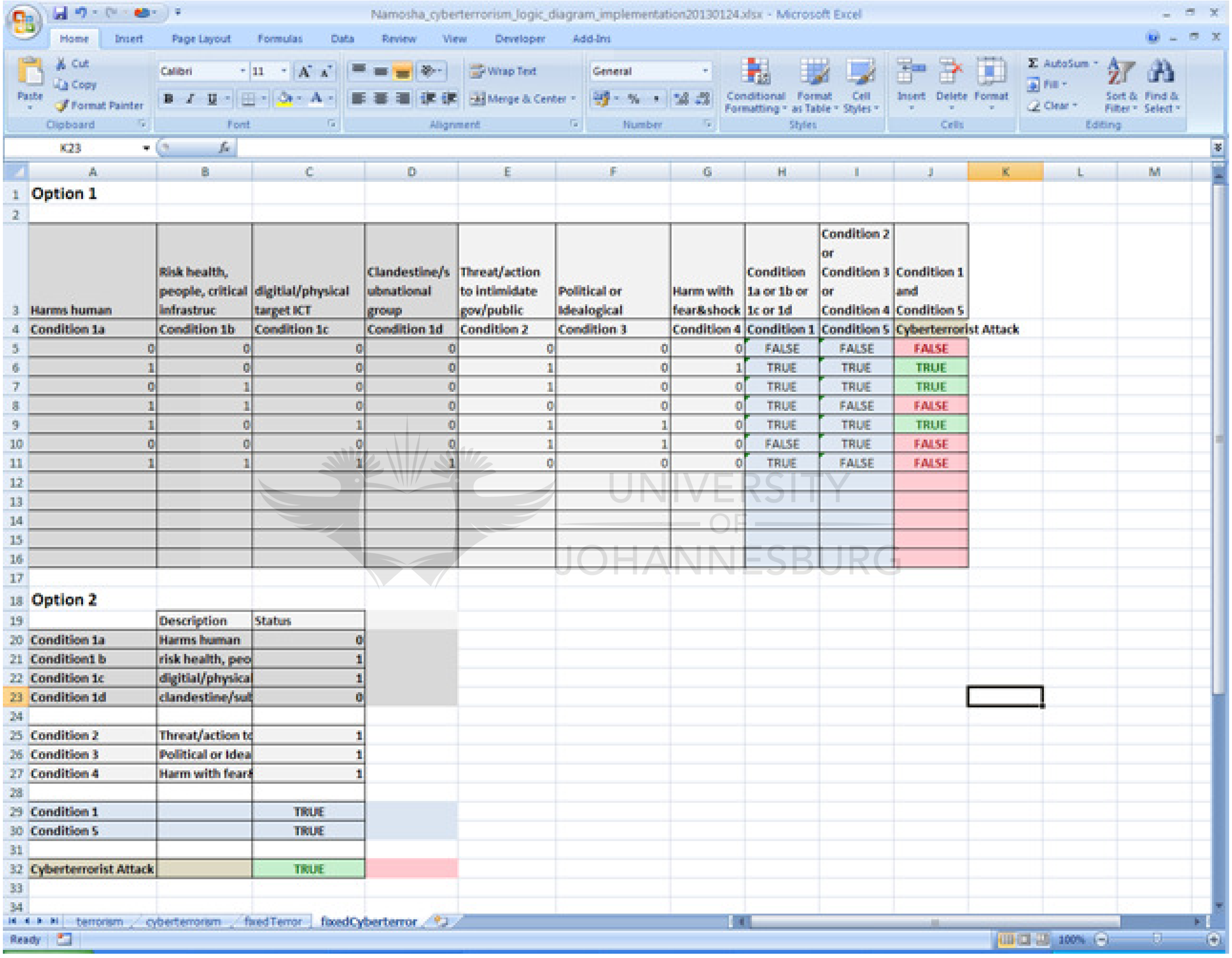
This definition is represented as conditions in a Microsoft Excel worksheet to determine whether an incident can be classified as cyberterrorism.

4.5 Logic Tester Worksheet

Conditions to describe an incident are specified as Yes/No (1 or 0 in the worksheet). The leading statement of the definition states "*Cyberterrorism aims to cause interference with electronic systems through:*" Therefore, this initial statement should be true before checking the other conditions.

The conditions are captured in the Microsoft Excel Logic Tester Worksheet and the output is a classification as to whether the specified conditions meet the criteria of being cyberterrorism (Figure 9). The logic tester is implemented using Boolean logic based on the definition. Thus, the conditions are represented as and/or statements.

Option 1 allows one to capture all the possible combinations while *Option 2* allows the capture of one set of conditions at a time. The two options are implemented in the same manner and only differ in layout. Users can choose to analyse all the conditions combinations (*Option 1*) or choose to focus on a specific combination (*Option 2*).



Option 1

Harms human	Risk health, people, critical infrastruc	digitial/physical target ICT	Clandestine/subnational group	Threat/action to intimidate gov/public	Political or Idealogical	Harm with fear&shock	Condition 1a or 1b or 1c or 1d	Condition 2 or Condition 3 or Condition 4	Condition 1 and Condition 5
Condition 1a	Condition 1b	Condition 1c	Condition 1d	Condition 2	Condition 3	Condition 4	Condition 1	Condition 5	Cyberterrorist Attack
0	0	0	0	0	0	0	FALSE	FALSE	FALSE
1	0	0	0	1	0	1	TRUE	TRUE	TRUE
0	1	0	0	1	0	0	TRUE	TRUE	TRUE
1	1	0	0	0	0	0	TRUE	FALSE	FALSE
1	0	1	0	1	1	0	TRUE	TRUE	TRUE
0	0	0	0	1	1	0	FALSE	TRUE	FALSE
1	1	1	1	0	0	0	TRUE	FALSE	FALSE

Option 2

	Description	Status
Condition 1a	Harms human	0
Condition1 b	risk health, peo	1
Condition 1c	digitial/physical	1
Condition 1d	clandestine/sul	0
Condition 2	Threat/action to	1
Condition 3	Political or Idea	1
Condition 4	Harm with fear&	1
Condition 1		TRUE
Condition 5		TRUE
Cyberterrorist Attack		TRUE

Figure 9: Logic Tester Implemented in Microsoft Excel (Own Compilation)

In order to implement the definition in the Logic Tester, the definition had to be broken down into conditions with a new numbering scheme. In the logic tester, the mapping of the definition to the condiitons is shown in Table 3. The definition statements in Table 3 are numbered differently than the definition given in Section 4.4. The leading statement of the definition " *Cyberterrorism aims to cause interference with electronic systems through threats or actions that fall into either subsection (1) or (2) or (3) and sub-section (4)* " is not numbered in the original definition. In Table 3, this statement is split and the second part of the statement is numbered as Condition 1. Statements 1, 2 and 3 of the definition are incremented by 1 in Table 3 and become Condition 2, 3 and 4. The sub-sections of Statement 4 (in the original definition) relate to Condition

1 in Table 3 and are thus labelled Condition 1a, 1b, 1c and 1d respectively. The initial part of the leading statement of the definition is encompassed in Condition 5. This re-numbering of the definition was used for the implementation in the Logic Tester and did not change the established definition but merely transformed it into a different format in order to program the Logic Tester.

Table 3: Mapping of Definition to Logic Tester

Definition	Condition
1) Threats or actions that fall into sub-section (5)	**Condition 1**
2) Threats or actions to influence the government or intimidate the public, or	**Condition 2**
3) Threats or actions to promote a political or ideological issue or	**Condition 3**
4) Infliction of harm with the aim of creating fear and shock;	**Condition 4**
5) Threats/actions that:	
a) Harms a human life other than the person committing the act, or	**Condition 1a**
b) Causes a risk to health or safety of people or critical service, or	**Condition 1b**
c) Uses digital or physical means to target ICT infrastructure, or	**Condition 1c**
d) Carried out by clandestine groups or sub-national groups	**Condition 1d**

The logical operation in the Logic Tester is shown in Table 4.

Table 4: Mapping of Logical Operators to Definition

Logical Operation Required	Condition
5) Threats/actions that: a) Harms a human life other than the person committing the act, **or** b) Causes a risk to health or safety of people or critical service, **or** c) Uses digital or physical means to target ICT infrastructure **or** d) Carried out by clandestine groups or sub-national groups	**Condition 1a or 1b or 1c or 1d = Condition 1**
2) Threats or actions to influence the government or intimidate the public, **or** 3) Threats or actions to promote a political or ideological issue **or** 4) Infliction of harm with the aim of creating fear and shock	**Condition 2 or Condition 3 or Condition 4 = Condition 5**
Condition 1 **AND** Condition 5 TRUE = Cyberterrorism Attack	

4.6 Examples

4.6.1 Example 1: Web Server Hack

A terrorist group hacks into a web server and defaces a web site with derogatory comments against the government. This can be seen as a threat to intimidate the government. An example of this type of attacks is Pakistan hacker groups who have regularly defaced Indian websites to protest the Indian government. These types of attacks often insult the government and promote another political party in order to influence a part of society to support their breakaway group. The derogatory messages may insult the policies and actions of the current government and claim better service should be provided.

In line 6 of Option 1 (Figure 9), the conditions specified true are :

- Uses digital or physical means to target ICT infrastructure (*Condition 1c* is true since the web server has been compromised).
- Threats or actions to influence the government or intimidate the public (*Condition 2* is true since the posted comments try to influence the public to develop hostile feelings against the government).

According to the definition this is a cyberterrorist attack, as *Condition 1* and *Condition 5* are true (since *Condition 1c* is true and for *Condition 5* to be true *Condition 2 or 3 or 4* should be true).

4.6.2 Example 2: Server Attack

If an attacker were to break into a critical server controlling the railways of power grids for example, widespread terror could ensure. Railways and power grids are critical infrastructures that provide essential services to the public. An attack on critical infrastructure could cause widespread panic and even death. Such systems need sensitive controls to ensure that accidents and tampering do not occur.

In line 7 of Option 1 (Figure 9), the following conditions are true:

- Causes a risk to health or safety of people or critical service (*Condition 1b is true since contradictory train schedules or power cuts can seriously affect the health and safety of the population*).
- Threats or actions to influence the government or intimidate the public (*Condition 2 is true if a terrorist organisation claims responsibility. A power cut or railway crash can be highly intimidating to the public as they could fear another attack and the effects thereof*).

According to the definition this is a cyberterrorist attack, as *Condition 1* and *Condition 5* are true (since *Condition 1b* is true and for *Condition 5* to be true *Condition 2 or 3 or 4* should be true).

4.6.3 Example 3: Medical Equipment Tampering

A terminally ill patient lies in a hospital in a critical condition. Currently, life-support machines are maintaining respiration and the intake of fluids. The terminally ill patient may have requested his doctor to switch off the machines should he reach an irrecoverable state.

In line 8 of Option 1 (Figure 9), the following conditions are true:

- Harms a human life other than the person committing the act
- Causes a risk to health or safety of people or critical service

Hypothetically, a person tampering with medical equipment can result in a patient dying. The victim could have had serious medical complications and manipulating the machines is a form of euthanasia. The incident would not cause any shock, as the person was seriously ill.

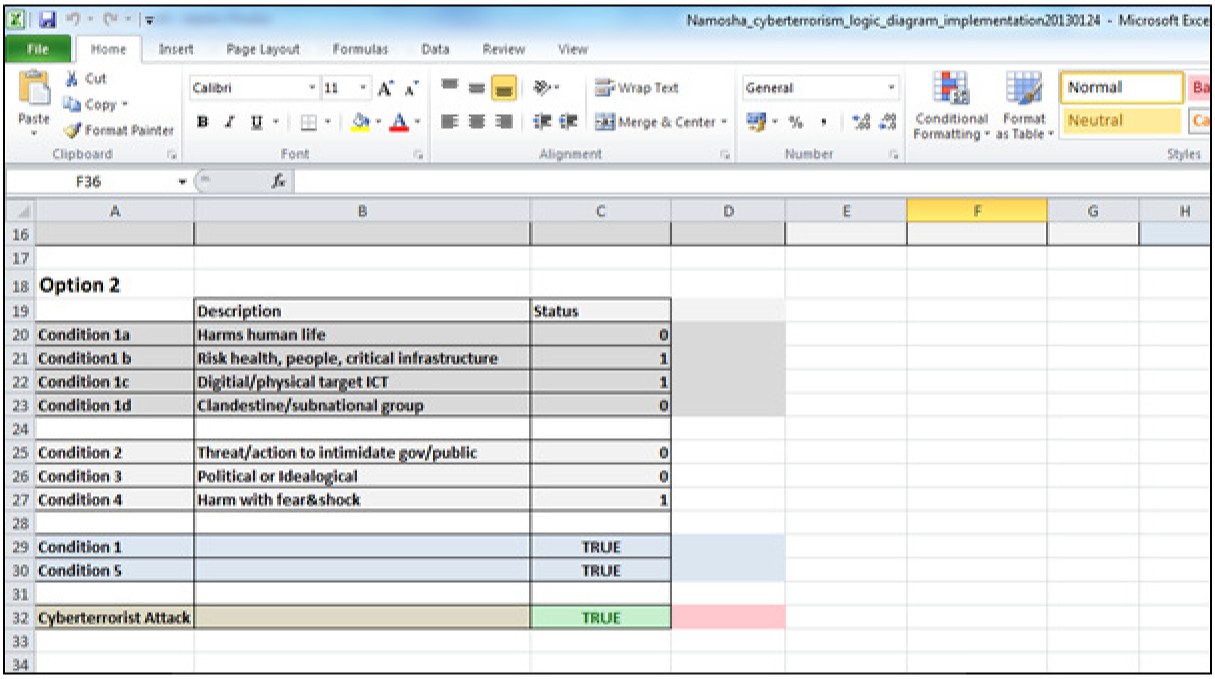
This does not meet the conditions of the definition, as only *Condition 1* is true. *Condition 5* is not true since there is no attempt to influence the government, political motivation or aim of creating fear and shock.

4.6.4 Example 4: Australia Sewerage Example

Section 3.5 discusses various examples of cyberterrorism incidents. One of these examples is the release of sewerage on the Australian coastline. This example can be evaluated against the Logic Tester. A summary of the incident is as follows:

- Former employee refused full-time position
- Use wireless radio and stolen control software
- Released litres of sewerage along Queensland coastline

The mappings to conditions are shown in Figure 10. (*Option 2* is just another view of the Logic Tester where the conditions are specified one at a time whereas *Option 1* can capture all the combinations of the conditions).



Option 2

	Description	Status
Condition 1a	Harms human life	0
Condition1 b	Risk health, people, critical infrastructure	1
Condition 1c	Digitial/physical target ICT	1
Condition 1d	Clandestine/subnational group	0
Condition 2	Threat/action to intimidate gov/public	0
Condition 3	Political or Idealogical	0
Condition 4	Harm with fear&shock	1
Condition 1		TRUE
Condition 5		TRUE
Cyberterrorist Attack		TRUE

Figure 10: Logic Test for Australian Sewerage Example (Own Compilation)

The following conditions are true (based on the author's interpretation of the example):

- Causes a risk to health or safety of people or critical service (*Condition 1b*). Sewerage spillage can affect the health of the public.
- Uses digital or physical means to target ICT infrastructure (*Condition 1c*). The system was attacked using wireless technology and insider knowledge to bypass controls.
- Infliction of harm with the aim of creating fear and shock (*Condition 4*). Sewerage spillage can be highly upsetting to the public. This endangers their own lives and causes negative effects on the ecological environment.

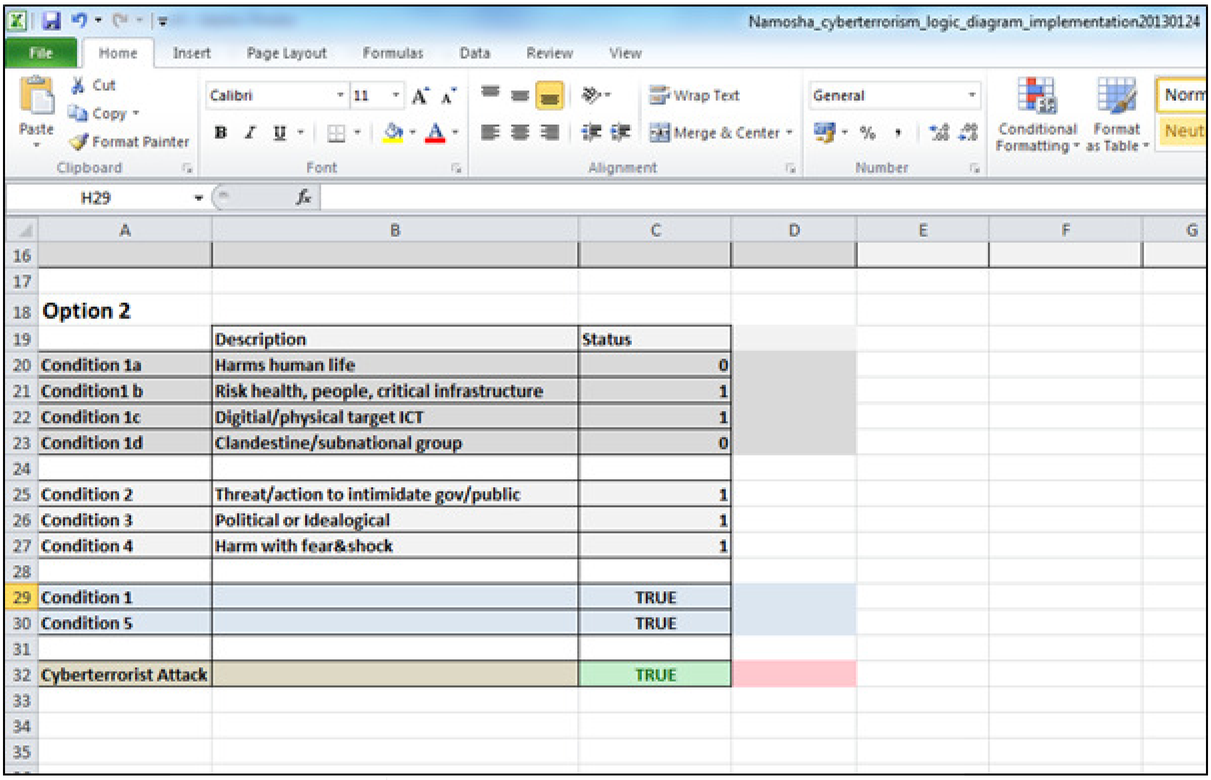
According to the definition this is a cyberterrorist attack, as *Condition 1* and *Condition 5* are true (since *Condition 1b and 1c* are true and for *Condition 5* to be true *Condition 2 or 3 or 4* should be true).

4.6.5 Example 5: Estonia Cyber Attacks

Another wide-impact example was the series of cyber attacks carried out against various Estonian systems in 2007. The incident is summarised as follows (Traynor 2007, Vamosi 2008, Von Solms 1996):

- War memorial to honour Russian-Estonians who lost their lives fighting Nazis in World War II is moved.
- Websites like parliament, banks, political parties, ministries, newspapers and broadcasters were flooded with Denial-of-Services attacks.
- Zombie networks from Russia and around the world caused the attack.

The conditions for this example as mapped to the Logic Tester are shown in Figure 11.



	A	B	C	D
16				
17				
18	Option 2			
19		Description	Status	
20	Condition 1a	Harms human life	0	
21	Condition1 b	Risk health, people, critical infrastructure	1	
22	Condition 1c	Digitial/physical target ICT	1	
23	Condition 1d	Clandestine/subnational group	0	
24				
25	Condition 2	Threat/action to intimidate gov/public	1	
26	Condition 3	Political or Idealogical	1	
27	Condition 4	Harm with fear&shock	1	
28				
29	Condition 1		TRUE	
30	Condition 5		TRUE	
31				
32	Cyberterrorist Attack		TRUE	
33				
34				
35				

Figure 11: Logic Test for Estonian Incident (Own Compilation)

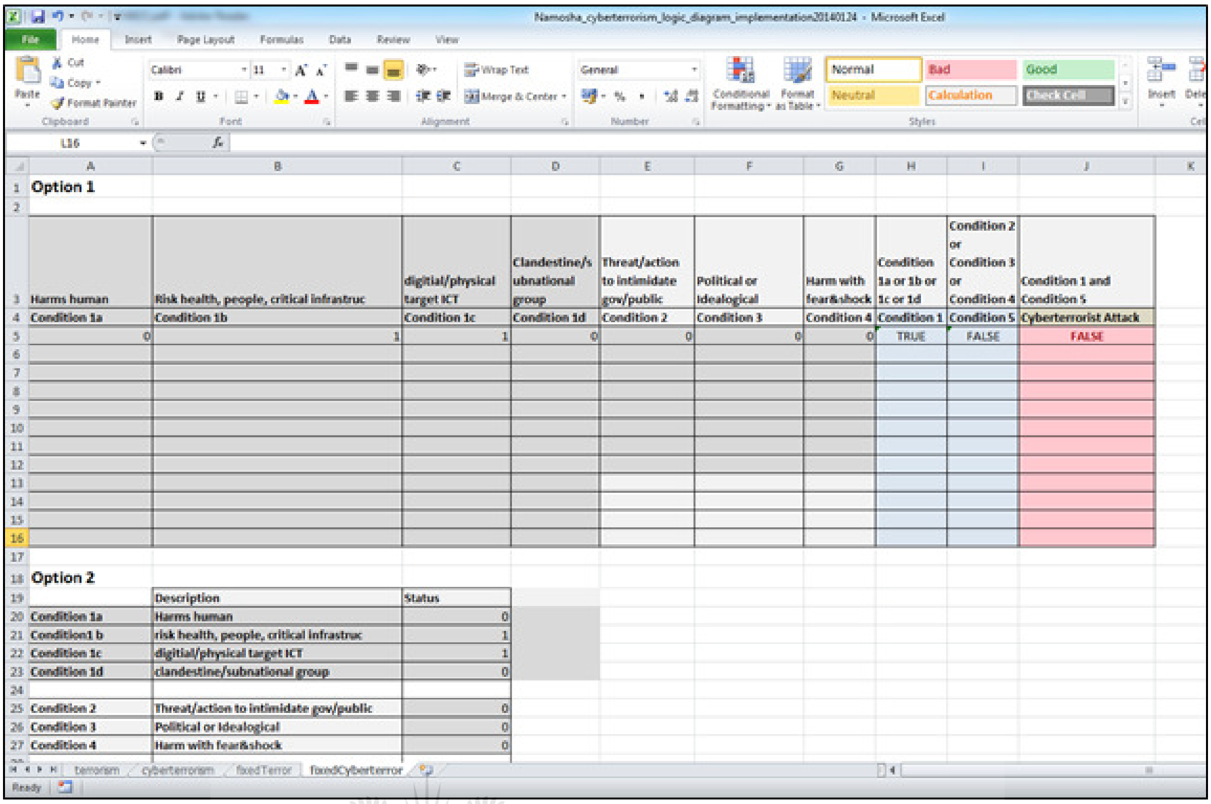
The following conditions are true (based on the author's interpretation of the example):

- Threats or actions to influence the government or intimidate the public (Condition 2) Governmental and public targets were flooded with Denial-of-Service attacks.
- Threats or actions to promote a political or ideological issue (Condition 3) The incident occurred due to the movement of the war memorial which upset sectors of the population.
- Infliction of harm with the aim of creating fear and shock (Condition 4). The incident caused shock as many essential services were unavailable.
- Causes a risk to health or safety of people or critical service (Condition 1b). News reporting and governmental services were all unavailable due to the flood of message.
- Uses digital or physical means to target ICT infrastructure (Condition 1c). The targets were web sites and electronic forms of communication.

According to the definition this is a cyberterrorist attack, as *Condition 1* and *Condition 5* are true (since *Condition 1b and 1c* are true and for *Condition 5* to be true *Condition 2 or 3 or 4* should be true and in this example *Condition 2, 3 and 4* can be considered true).

4.6.6 Example 6: HB Gary Hack and Anonymous

Aaron Barr, the CEO of the security firm HBGary announced that he would be able to reveal the identities of members of the Anonymous group through traces on social networks (Bright 2011). In retaliation, Anonymous reacted by breaking into the servers of HBGary, exposing company documents and also broke into Barr's email account. The conditions for this example as mapped to the Logic Tester are shown in Figure 12.



Option 1

Harms human	Risk health, people, critical infrastruc	digitial/physical target ICT	Clandestine/subnational group	Threat/action to intimidate gov/public	Political or Idealogical	Harm with fear&shock	Condition 1a or 1b or 1c or 1d	Condition 2 or Condition 3 or Condition 4	Condition 1 and Condition 5
Condition 1a	Condition 1b	Condition 1c	Condition 1d	Condition 2	Condition 3	Condition 4	Condition 1	Condition 5	Cyberterrorist Attack
0	1	1	0	0	0	0	TRUE	FALSE	FALSE

Option 2

	Description	Status
Condition 1a	Harms human	0
Condition1 b	risk health, people, critical infrastruc	1
Condition 1c	digitial/physical target ICT	1
Condition 1d	clandestine/subnational group	0
Condition 2	Threat/action to intimidate gov/public	0
Condition 3	Political or Idealogical	0
Condition 4	Harm with fear&shock	0

Figure 12: Logic Tester for HB Gary Hacks (Own Compilation)

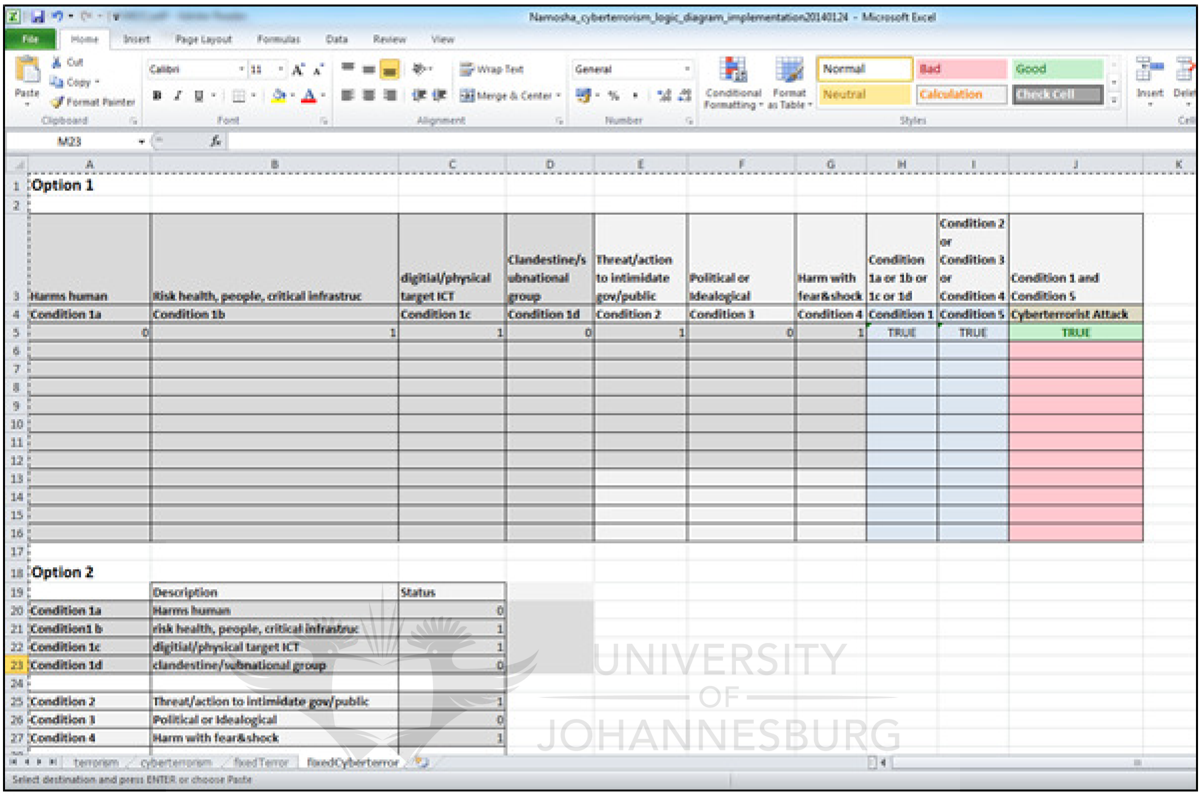
The following reasoning can be applied:

- The attacks were not meant to harm human life.
- Causes a risk to health or safety of people or critical service (Condition 1b) is true as the company servers were attacked.
- Uses digital or physical means to target ICT infrastructure (Condition 1c) is true. The targets were servers, web sites and electronic forms of communication.
- Anonymous is considered a hacktivist group- hacking with an activist motivation. They are not seen as clandestine/sub national groups,
- The threat was not meant to intimidate the government or public but rather retaliatory.
- The attacks were not politically or idealogically motivation.
- The attack did not threaten human life and therefore did not have an element of fear or shock.

According to the definition, this is not a cyberterrorist attack since only Conditio 1b (Risk to health or safety of people or critical service) and Condition 1c are true (Use of digital or physical means to target ICT infrastructure).

4.6.7 Example 7: Stuxnet

Stuxnet, a cyber worm attacked the Iranian nuclear facility by slowly deteriorating the centrifuges. It made use of zero-day vulnerabilities that changed the power of the centrifuges causing them to switch between high and low speeds (Farwell, Rohozinski 2011). The conditions for this example as mapped to the Logic Tester are shown in Figure 13.



Namosha_cyberterrorism_logic_diagram_implementation20140124 - Microsoft Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
M23

Option 1

Harms human	Risk health, people, critical infrastruc	digitial/physical target ICT	Clandestine/subnational group	Threat/action to intimidate gov/public	Political or Idealogical	Harm with fear&shock	Condition 1a or 1b or 1c or 1d	Condition 2 or Condition 3 or Condition 4	Condition 1 and Condition 5
Condition 1a	Condition 1b	Condition 1c	Condition 1d	Condition 2	Condition 3	Condition 4	Condition 1	Condition 5	Cyberterrorist Attack
0	1	1	0	1	0	1	TRUE	TRUE	TRUE

Option 2

	Description	Status
Condition 1a	Harms human	0
Condition1 b	risk health, people, critical infrastruc	1
Condition 1c	digitial/physical target ICT	1
Condition 1d	clandestine/subnational group	0
Condition 2	Threat/action to intimidate gov/public	1
Condition 3	Political or Idealogical	0
Condition 4	Harm with fear&shock	1

Figure 13: Logic Tester for Stuxnet (Own Compilation)

The following conditions are true (based on the author's interpretation of the example):

- Threats or actions to influence the government or intimidate the public (Condition 2). A nuclear plant was attacked.
- Infliction of harm with the aim of creating fear and shock (Condition 4). The incident caused widespread shock as a nuclear plant was attacked.
- Causes a risk to health or safety of people or critical service (Condition 1b. The malfunctioning of essential services at a nuclear plant poses a significant risk to the health and safety of people.
- Uses digital or physical means to target ICT infrastructure (Condition 1c). The targets were controls systems at a nuclear plant.

According to the definition this is a cyberterrorist attack, as *Condition 1* and *Condition 5* are true (since *Condition 1b and 1c* are true and for *Condition 5* to be true *Condition 2 or 3 or 4* should be true and in this example *Condition 2 and 4* can be considered true).

In this way, various other examples and incidents can be applied to the Logic Tester to determine whether it should be classified as cyberterrorism. In the accompanying video, the testing of the first five examples are shown. The conditions for each example are entered into the Logic Tester to return a positive or negative result confirming whether the example can be classified as cyberterrorism or not.

However, the conditions specified in the implementation (based on the established definition) are not the only perspectives that should be considered. Cyberterrorism is a diverse field and therefore other factors will be influential. The discussion now moves to another application of the definition.

This chapter shows that there are various ways of classifying a cyberterrorism attack. Various conditions can be evaluated. However, it is not always possible to classify an attack clearly. This issue will be re-visited later on in the study when other factors are identified to be relevant in the field of cyberterrorism.

4.7 Conclusion

This chapter provided a practical implementation of evaluating the definition of cyberterrorism. This is useful in testing whether a cyber event can be classified as cyberterrorism. This chapter meets the sub-objective of investigating defining concepts and the classification of cyber events as cyberterrorism.

In summary, the following drivers identified from Chapter 4 contribute to the development of the CLC Model:

- The differentiation between cybercrime and cyberterrorism is an important aspect that is often confused. In order for a cybercrime or attack to be considered as cyberterrorism, there needs to be an element of terror through threats, disturbances or the infliction of violence. The CLC model, will take into consideration an ordinary cybercrime and those that take the form of cyberterrorism (Section 4.2)
- The driving forces behind cyberterrorism stems from different objectives. Cybercrime can be relating to causing annoyance, economic loss, fraud and espionage whereas cyberterrorism is linked to causing fear. The CLC model will cover the different objectives behind cyberterrorism that will demonstrate its distinction from cybercrime in general (Section 4.2).
- Cyberterrorism aims to cause interference with electronic systems (Section 4.2)
- Threats or actions need to influence the government/intimidate the public or promote a political/ideological cause or inflict harm with the aim of creating fear/shock as well as (Section 4.2):
  - Harms a human life other than the person committing the act, or
  - Causes a risk to health or safety of people or critical service, or
  - Uses digital or physical means to target ICT infrastructure or
  - Carried out by clandestine groups or sub-national groups

This chapter discussed and tested out the concepts introduced in the definition in order to identify important ideas that contribute to the field of cyberterrorism. At the commencement of this study it was stated that various influential factors may affect cyberterrorism. Therefore, it is essential to study the field from a number of perspectives to analyse and refine findings. In Part 2, the initial background to cyberterrorism will be extended. While this chapter looked at the defining concepts, Chapter 5 proposes a framework that discusses various other concepts that are relevant to the field, as well as describes how they contribute to the execution and support of cyberterrorism. Part 2 looks at identifying important factors relevant to the field of cyberterrorism, which will contribute to the development of the life cycle model.

Part 2 Cyberterrorism Field

This study, CLC-Cyberterrorism Life Cycle is broken down into four sections (originally shown in Figure 2). Figure 14 presents the status of the CLC model development study. Part 1 has been completed. Part 2, Cyberterrorism field investigates the current cyberterrorism field by studying the influential factors and use of the Internet for exploitation and support. It consists of three chapters of the study.

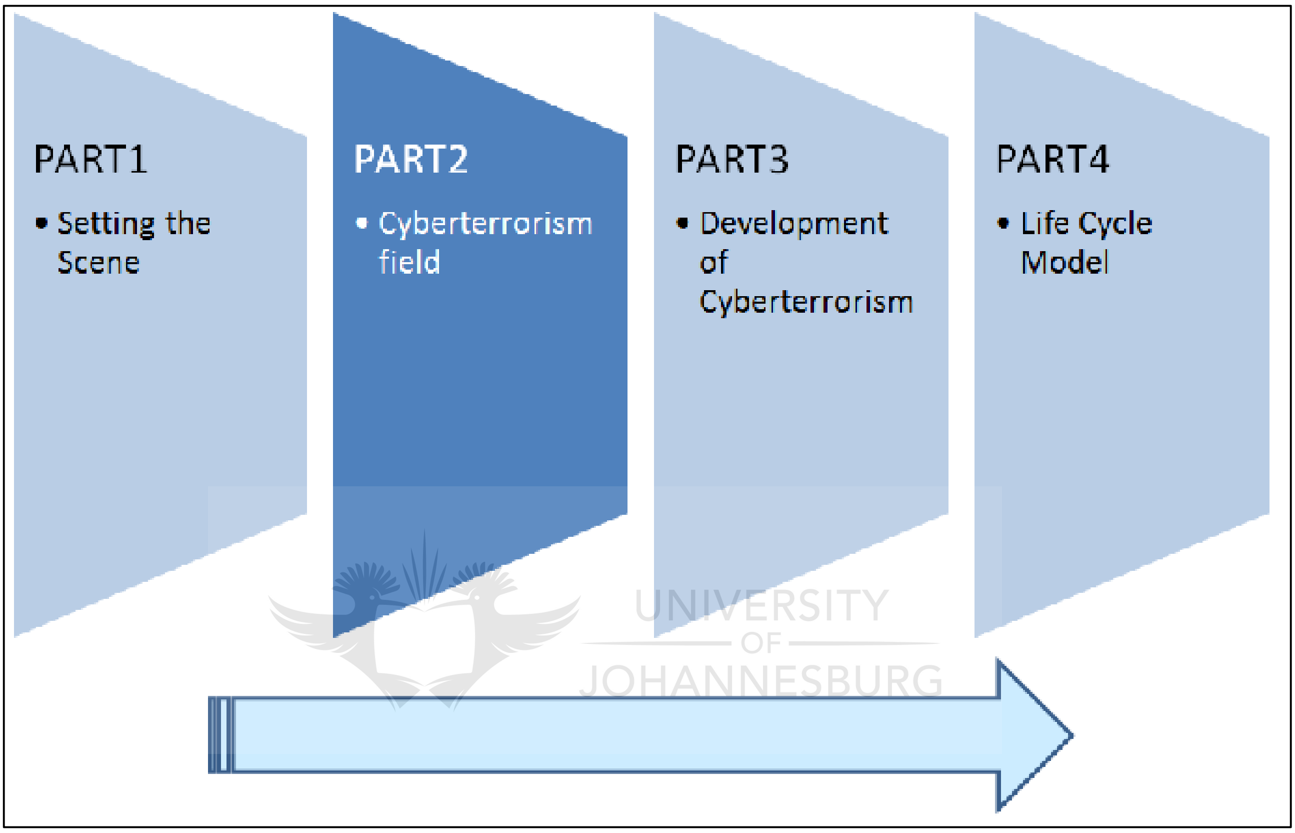


Figure 14: Part 2 of the CLC Model Development (Own Compilation)

Part 2 consists of three chapters:

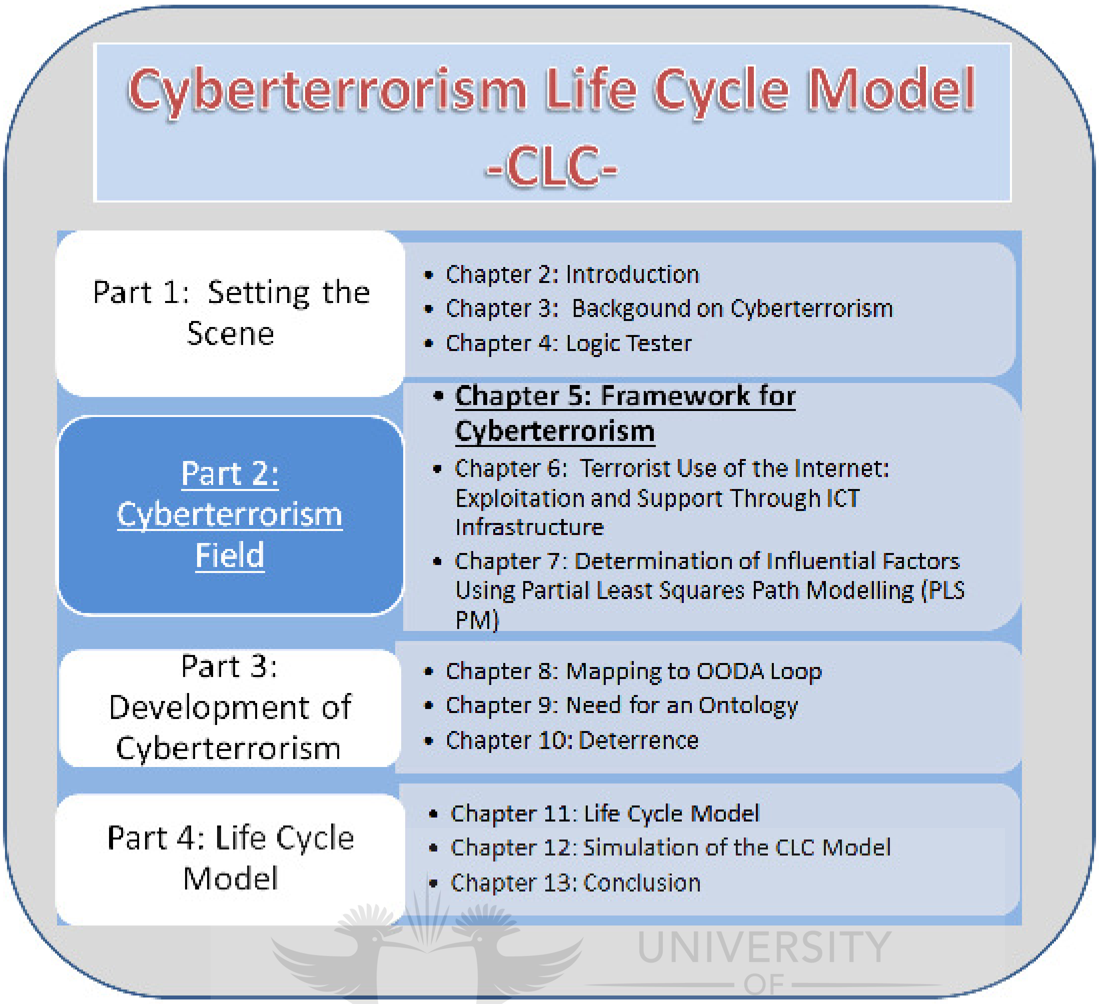
- Chapter 5, Framework for Cyberterrorism
- Chapter 6, Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7, Determination of Influential Factors using Partial Least Squares Path Modelling (PLS PM)

Chapter 5, Framework for Cyberterrorism, proposes a framework based on a literature study of the main influential factors contributing to the field of cyberterrorism. The framework addresses operating forces, techniques and objectives. The framework is by no means exhaustive but provides the necessary background knowledge to contextualise the reader. In this way, the reader will be orientated with the wide scope of cyberterrorism and be introduced to some of the most pertinent influential factors.

Chapter 6, Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure, addresses the use of the Internet by terrorists to exploit or support their activities in general. The chapter looks at current cyberterrorist techniques and demonstrates to the reader the ingenious ways of exploiting ICT infrastructure.

Chapter 7, Determination of Influential Factors using Partial Least Squares Path Modelling (PLS PM) determines the potential impact of a few social factors by carrying out an investigation using the PLS PM statistical technique.

In Part 3 an onotology will be presented. The ontology was used as a means of structuring the field and showing the relationships identified in earlier parts in an ordered manner.



Cyberterrorism Life Cycle Model -CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- **Chapter 5: Framework for Cyberterrorism**
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

5 Framework for Cyberterrorism

> *"While we must remain determined to defeat terrorism, it isn't only terrorism we are fighting. It's the beliefs that motivate terrorists."*
>
> *- Senator John Kerry (USA)*

5.1 Introduction

Part 1 focussed on setting the scene in the cyberterrorism world. Chapter 2 described the aim of the study and Chapter 3 introduced Cyberterrorism. Chapter 4 explained the application of a Logic Tester to the definition of cyberterrorism.

Part 2 will now look at further expansion of the field of cyberterrorism by investigating various factors that influence cyberterrorism. Chapter 5 will provide a detailed literature study on cyberterrorism. The discussion in Chapter 5 will be based on the author's establishment of a framework, which discusses the main operating forces, techniques and objectives of cyberterrorism. The framework was presented at the International Conference on Information Warfare and Security an appears in the International Journal of Information Warfare in 2009. The usefulness of the framework lies in determining the main influential factors of cyberterrorism, which will eventually be incorporated in the CLC model.

Figure 15 indicates the focus of this chapter will be the establishment of the foundational building blocks that contributes to the compilation of the CLC model. Chapter 5 initially addresses Sub-objective 2, Influential Factors (originally presented in Figure 3).

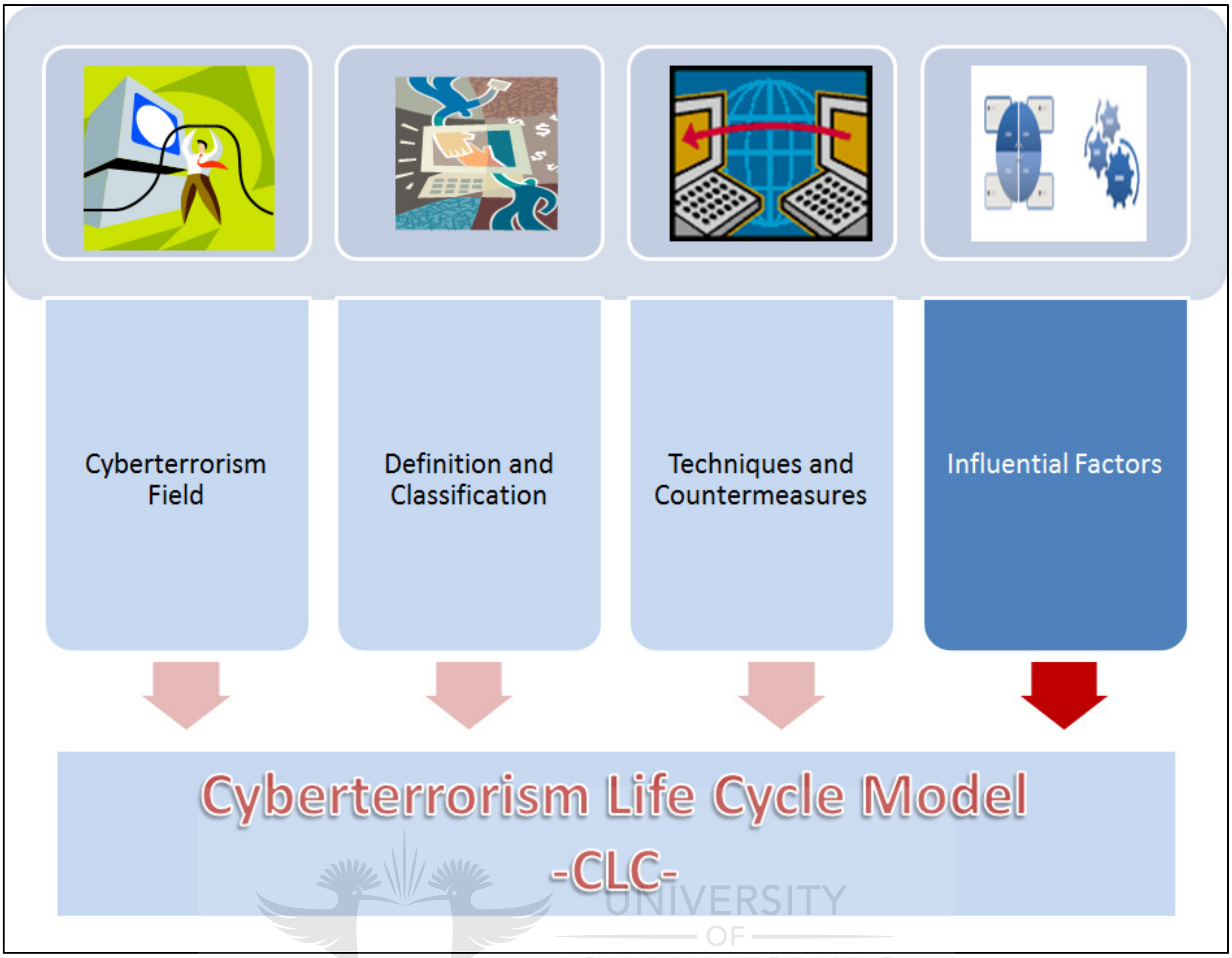

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 15: CLC Model Focus Chapter 5 - Cyberterrorism Influential Factors (Own Compilation)

5.2 Grounded Theory Method

In this chapter, an analysis of the cyberterrorism field is carried out. The conceptual framework that is proposed outlines the main aspects of cyberterrorism. The main basis of the framework is grounded theory as it shows how data can be collected and analysed. A similar approach was used to develop the framework. Grounded theory has extensively been discussed in literature as far back as 1965. A short summary of grounded theory is given from Strauss and Corbin (1994). Grounded theory is a general methodology to develop theory that is based on data that is gathered in a systematic manner and then analysed. The characteristics of Grounded theory are (Strauss & Anselm 1994):

a) The theory evolves during the research and occurs through the continuous interchange between analysis and data collection

b) Uses comparative analysis

c) Grounded theory is a general methodology to develop theory that is based on data that is gathered in a systematic manner and then analysed

d) If theories are already existing they can be elaborated through further data analysis

e) Grounded theory consists of creating theory and doing social research. It can be argued that the theory should be linked to actual research

f) Similarities to other methods of qualitative research are:

    i) Sources of data are the same. These include interviews, field observations, records like diaries, letters, historical accounts, autobiographies, newspapers, videos, paper and other media materials

    ii) Use quantitative data or combine quantitative and qualitative data

    iii) Can be interpretive work

g) Difference to other approaches of qualitative research are:

    i) Emphasis on theory development

    ii) Aimed at developing substantive theory

    iii) Through extensive data collection, there is explicit mandate to verify the resulting hypothesis. Verification must be completed throughout the research (without the assumption that the verification can be done with follow-up quantitative research)

    iv) Recurrent comparison and systematic method of asking generative and concept-related questions

The function of grounded theory is to help establish theoretically comprehensive data to explain a phenomenon (Ahmad, Yunos & Sahib 2012). Furthermore, Onions (2006) explains that the grounded theory method is inductive and is intended to result in emergent theory. Grounded theory is thus typically, a qualitative data approach whereby data can be interpreted and help contribute to theory development.

Charmaz (2003) discusses the various strategies of grounded theory. This may include simultaneous collection and analysis of data, a two-step data coding process, comparative methods, sampling to refine ideas and integration of the theoretical framework. Charmaz further explains that the coding process is actually the categorisation of data. In quantitative research, data needs to fit into defined set codes, but in grounded theory, as the data is interpreted, codes can emerge. Theoretical sampling aims to refine the categories to identify disparities. Overall, grounded theory entails studying various sources of data and comparing the data in order to gain insight into what is useful in the field.

This chapter looks at a conceptual framework to review various literature related to the field in order to determine what theory emerges. The next section consists of a framework for cyberterrorism that is based on grounded theory related to the field. This framework formed the foundational conepts of the cyberterrorism field but throughout the thesis, the grounded theory approach is used to iterate through various other sources and refine concepts.

5.3 Framework

This chapter presents a conceptual framework that outlines the critical concepts relevant to cyberterrorism. Glaser and Strauss (2009) explain that a researcher when initiating a formal study can commence with a loose conceptual framework of ideas, notions and concepts. The framework presented in this chapter addresses the main influential factors that contribute to cyberterrorism.

Using a grounded theory approach, the analysis of the data reveals the following initial perspectives of cyberterrorism: techniques, objectives, target, types, effects, characteristics and capabilities. These findings form the basis in initially conceptualising cyberterrorism. The framework aims to form a more explanatory synopsis that describes cyberterrorism in more detail. The framework thus forms a beneficial structured representation that helps contextualise the reader with the basic concepts of cyberterrorism relative to areas of cybercrime and ICT. Throughout this thesis, other findings will also be revealed to the reader as they are discovered.

The framework is shown in Figure 16. The high-level outline of the framework is made up of three main sections. These include the operating forces (Section 5.4), techniques (Section 5.5) and objectives (Section 5.6). Largely, the goal of the framework is to form a good baseline that shows the defining concepts and contributing factors to cyberterrorism. To compile the framework, a detailed literature study was carried out (using Grounded Theory techniques). Literature was analysed and compared in order to identify key concepts that contribute to cyberterrorism. This helped gain insight into the field of cyberterrorism. Overall, various viewpoints relating to cyberterrorism was evaluated and structured to form the framework. The framework helps indicate typical methods of attack and what drives supporters of terrorist groups to threaten and attack people and systems.

Largely, the framework indicates critical considerations relevant to cyberterrorism and shows links between the objectives of terrorists and the technical means that are used to carry out or support terrorism. The knowledge gained from the framework can help create an awareness of what cyberterrorism entails and clear up misconceptions, that cybercrime is cyberterrorism. Similar to Y2K, it is important to build up awareness in both the information technology community and the general population that threats on computers and networks stemming from terrorism can indeed be a threat (Janczewski, Colarik 2008).

Five operating forces have been established in the framework. These include: characteristics, target/focus, types, capabilities, and social factors. Furthermore, every operating force consists of a number of related sub-items. The operating forces explain the background from which cyberterrorism stems. Thereafter, the framework contains various high-level techniques. The high-level techniques account for the methods and classifications of attack, which are mainly invasive and offensive in nature. Thereafter, the objectives are considered. The objectives convey the offensive goals or support functions that are trying to be achieved. While terrorist types are described at a high-level under operating forces, the malicious goals and support functions explain more pronounced intentions than standard terrorist motivations.

The framework contributes to the field of cyberterrorism by providing an overview of the field and structuring various influential factors. The operating forces explain the advantages of carrying out cyberterrorism, prime targets to be attacked and the mind-set of a terrorist. The techniques section of the framework focuses on describing different types of attack tactics. The objectives section addresses the direct goals of the attacker and indicates that ICT infrastructure can play a supportive role to terrorism in general. This representation in the framework is vital to showing the operative mind-set of a cyberterrorist, as well as explaining how cybercrime and hacking can be used for cyberterrorism. The main contribution of the framework is that it will form the foundational layer of the CLC model. The framework will now be discussed in detail.

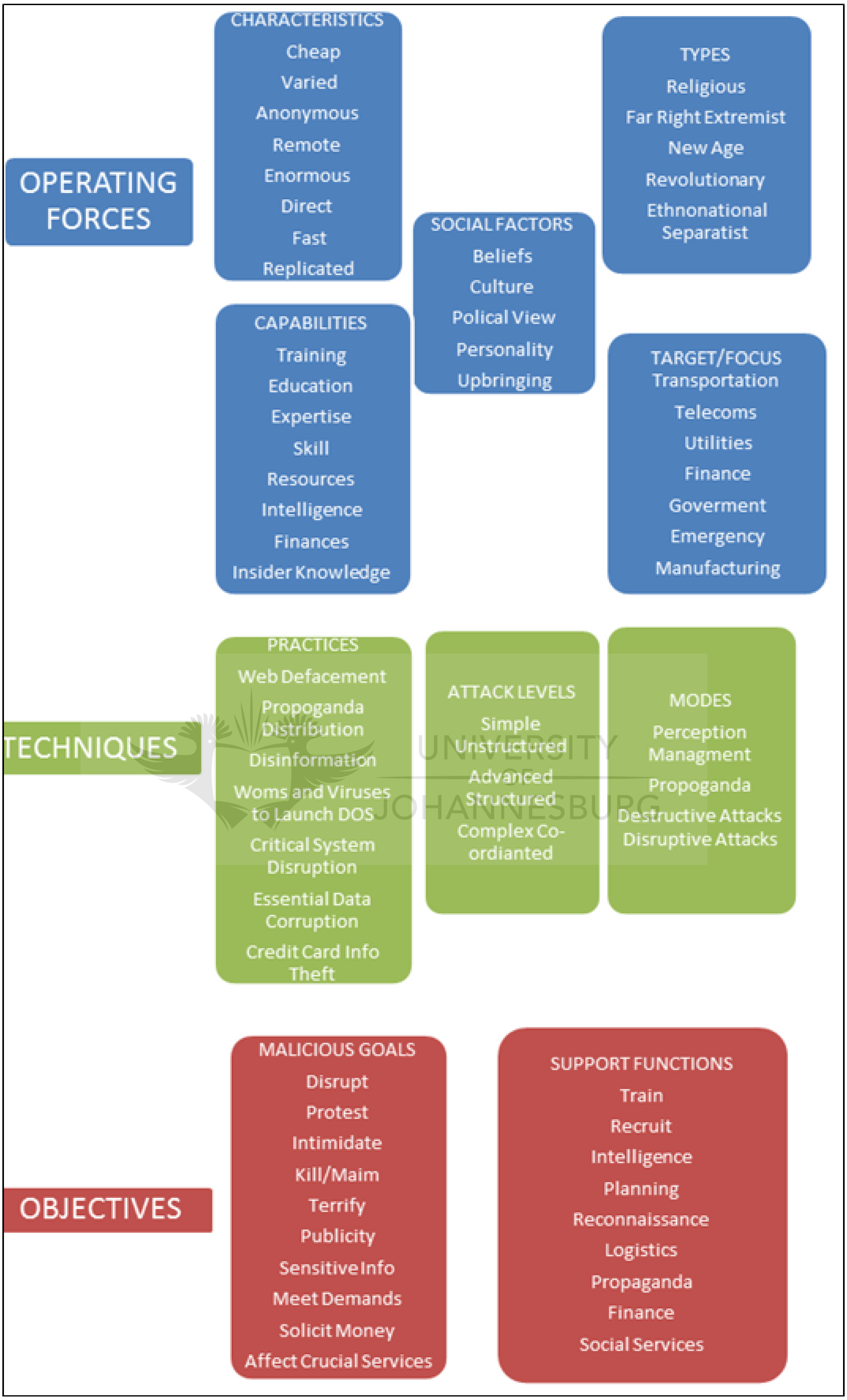


Figure 16: Framework of Cyberterrorism (Own Compilation)

5.4 Operating Forces

As mentioned earlier in this chapter, a grounded theory approach was used to develop the framework. Various literatures in the field were consulted and analysed. Thereafter, the framework was compiled as a summary of the cyberterrorism field. In the discussion of the framework, references are given to the source of the data. Typically, information about any field is scattered across literature. This framework structured cyberterrorism concepts to provide clarity. As the author came across different pieces of information relating to cyberterrorism, it was classified and placed into the framework. The framework proposes a number of operating forces (see Figure 16). Analysing these operating forces delves into the underlying influences that affect the development of cyberterrorism. These findings are based on a literature study of the field of cyberterrorism, as well as related areas of interest like cybercrime and hacking. The operating forces portray the characteristics of a cyberterrorist together with the features of cyberterrorism in general. Each of these Operating Forces will now be discussed.

5.4.1 Characteristics

The characteristics section was compiled by studying the advantages and benefits that cyberterror offers versus traditional terrorism practices like explosions, hijacking or kidnapping. Therefore, the study of the advantages of ICT helped identify opportunities that terrorists could benefit from.

According to Denning (2000), the advantage of cyberterrorism is that it can be conducted remotely, anonymously, as well less expensively as it does not require the purchase of explosives or sacrificing one's life in a suicide mission. In contrast to purchasing explosives, a computer and network connection is by far more affordable. Furthermore, Weimann (2004) states that cyberterrorists have the ability to directly reach a larger number of targets. In addition, the US Army Training and Doctrine Command Handbook (2006) discusses the reasons that cyberterrorism may become a preference over physical attacks. The reasons include: anonymity, varied targets, low investment, small risk of discovery of perpetrator, activate from nearly any location and less resources (US Army Training and Doctrine Command 2006). Further characteristics found in cyberterrorism are the speed and ease at which attacks can be carried out anonymously due to the capabilities of networked infrastructure. Using digital technology, attacks can be automated and replicated at a rapid rate, which reduces the level of effort required.

5.4.2 Capabilities

Capabilities refer to the significant underlying characteristics, traits and qualifications affecting the mind-set of a cyberterrorist. Upbringing and educational history will play a vital role in the early development of a potential terrorist. As an adult, experience expertise and skills can be acquired. Training will increase the aptitude of the individual. In addition, financial backing is an essential necessity to support ongoing terrorist activities. Co-ordination, planning and execution of attacks require funds. Furthermore, additional resources like equipment and tools are necessary to sustain operations. Insider information would provide an advantageous position. Another capability that would assist a cyberterrorist is reliable intelligence, as this would provide the necessary background and guidance for carrying out a mission. The capability section provides an outline of the various abilities, resources and facilities that would aid a terrorist in carrying out an attack. Next, the discussion moves on to the main social factors affecting the growth of cyberterrorism.

5.4.3 Social Factors

Social issues can influence the development of a terrorist as these provide the main stimulus that may lead to an interest in a specific cause. Jenkins (2006) explains that terrorism may generally stem from the ideas of morality, law, and the rules of war; while actual terrorists are influenced by culture, ideology and politics. This proposes a few social factors that could be influential considerations, namely beliefs, culture, political views, personality and upbringing. These intangible social issues will shape the initial foundation of the mind-set of a terrorist and therefore influence the future line of action that is pursued. Now that the basic reasons and issues influencing the development of cyberterrorism have been discussed, the techniques of cyberterrorists are explored. The next section summarises the different types of terrorism.

5.4.4 Types of Terrorism

The types of terrorism range from political views to religious principles. Section 3.6 classified terrorism into different types. However, the classifications of terrorism are not clear-cut and the types blur as various ideological principles overlap. This section discusses the different high-level motivating forces that instigate and compel terrorists to carry out their activities. Section 3.6 mentioned the driving forces briefly and therefore, this discussion provides a deeper analysis. Overall, terrorism stems from differing political, social, religious, ideological and philosophical viewpoints. Terrorists may use hacking skills to carry out their objectives.

Hackers possess the technical prowess to carry out advanced attacks on ICT systems. Hackers could be affiliated to an organisation or operate on their own. In the underworld of hacking, anonymity and skill are critical to building up a strong reputation with the use of pseudonyms. Due to the nature of work, hackers wish to gain notoriety for their successes and still keep their identity a secret. Typical targets can include financial systems, web and mail servers of large corporations, e-commerce sites and banks.

A political organisation could use the services of a hacker to break into a governmental website and make political statements or exploit vulnerabilities. Hackers use their advanced technical skills to take advantage of technological weaknesses. Hacking activities can have the following implications:

- **Financial costs**: theft of credit card numbers or funds, pharming attacks
- **Availability**: disruption in services like e-commerce or email, information hi-jacking through web defacement
- **Integrity** loss: access to sensitive data, data corruption or loss

To a large extent, hacking can be carried out by all types of terrorists. Either individuals with technical skills could become involved with a political, social or religious group and thus use their skills to carry out cyber terror attacks or members already involved with a terrorist organisation could develop the technical skills to carry out cyber attacks. The underlying behaviour will be motivated by political, religious, ideological or social causes. When Janczewski and Colarik (2008) discuss the differentiation between cyberterrorism and cybercrime, they state the answer does not lie in the mechanics of the event, but instead one should consider the intent behind the person's actions.

Weimann (2004) draws attention to a report, "Cyberterror: Prospects and Implications," by the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School (NPS) in Monterey, California in

August 1999. The report considers five groups of terrorists: religious, New Age, ethno-nationalist separatist, revolutionary and far-right extremist. These findings stem from a framework that categorises terrorists into these groups. Each of the types of terrorism will be briefly explained.

5.4.4.1 Religious

Already in 1996, Lacquer (1996) explained that religious terrorists consist of people with very strong-quasi religious views, which results in total certainly of these beliefs (or total moral terrorism) that justifies taking the lives of others. A typical example is Al Qaeda.

Such theological viewpoints can even justify using violence and the sacrifice of one's own life. As far back as 1999, Nelson et al. (1999) has stated that contrary to revolutionary terrorism, religious terrorism may inflict violence on much wider and unfocussed groups using advanced structured attacks. This approach provides for rewards that fulfil the ideology of the religious group carrying out the attacks. The next type of terrorism to be discussed is Ethno-Nationalist.

5.4.4.2 Ethno-Nationalist

According to Post (2005), Ethno-nationalist supporters fight to create a new political order grounded on the basis of ethnic domination/homogeneity. Examples of groups, which have sought political autonomy, are the Spanish Basque ETA, Sri Lankan Liberation Tamil Tigers of Eelam (LTTE), Palestinian Liberation Army, Provisional Irish Republican Army (PIRA), and the Kurdish Workers Party (PKK) in Turkey. Publicity and international recognition for their cause are some of the motives of Ethno-nationalists. Violence is also used. Contrary to religious extremists, ethno-nationalists focus on specific targets - usually those with a prominent profile. For example, typical targets can include symbols of the state like, public amenities or utilities, and even members of other ethnic groups.

The geographical location of a target can influence the type of attack that will be carried out. Close proximity to a potential target, for example a military base, may result in the execution of a physical attack. However, if the target were not within easy reach, a cyberterror attack would be ideal. Using ICT networks, the group could still achieve its objectives of launching an attack.

Ethno-national separatists try to gain support from local members, and rely on sympathy from the international community. In order to achieve this, violent actions have to be shown to be necessary for the cause. Through cyber attacks, services can be disrupted and this indicates protestation from the group. Cyber attacks have the benefit of eliminating causalities and injuries that occur because of violent and biological attacks.

In the light of this, cyberterror attacks, which cause an interruption in services, are probably a more appealing option as this form of protestation limits the loss of life but at the same time creates publicity for a cause. For example, attacking the web servers of government web sites or banks and defacing the web site can strike a strong political message. Furthermore, ethno nationalists could also make use of ICT to increase support for the movement and rally members.

5.4.4.3 Social Revolutionary (Terrorist of the Left)

Already in 1988, Targ stated that the revolutionary terrorism strategy is to seize political power (Targ 1988). Furthermore, social revolutionists aim to remove the capitalist economic and social order from power (Whelpton 2009). This type of movement has a radical social and political transformation agenda. Social revolutionary terrorism is also termed Terrorism of the Left and example groups are the Red Army Faction (who have been responsible for kidnappings and assassinations of people they hold responsible for the economic and political repression) as well as the Italian Brigades (who in the past have executed computer attacks). Generally, social revolutionists disagree with current structure and rules and therefore aim to seize power. Whelpton (2009) explains that as part of the social revolt a new and just society will be established.

The information infrastructure development of an area will determine whether a cyber attack would be useful. The level of "rurality or urbanism" can affect the impact of a cyber attack. If the government or state is heavily dependent on ICT, a cyber attack would the ideal platform to deliver an attack and transmit a message of cause. By carrying out focused attacks on governments and corporations, social revolutionary groups can convey their protestation against commercial and capitalist regimes.

5.4.4.4 Far-Right Extremism (Right-Wing)

According to Ehud Sprinzak (in Michael 2003), an Israeli political scientist, right-wing terrorism can be categorised as the process of "split-deligitimation" whereby not only the "outsider" groups (like foreigners, ethnic and religious minority groups) are targeted, but also the state itself, as they are considered as being unsuccessful or in poor standing due to the influence of outsiders. Furthermore, Whelpton (2009) explains that Far-right extremists could be racist organisations that are keen to use terrorism tactics to supress other racial and ethnic groups as they are seen as the enemy. Well-known examples of Right-wing groups include the Nazis and Italian neo-fascists. For this movement, cyberterrorism is not seen as an attractive option as there is the possibility of hurting one's group members if an unfocussed attack is carried out.

Far-right extremists tend to use ICT infrastructure to assist members by selling survivalist gear and propagating their cause through marketing and distribution of hate material. A key belief of Far-right extremism is the insistence that certain groups are superior and thus have the right to eradicate those that they consider inferior even if this entails the use of violence. Thus, the use of ICT for communication purposes serves the needs of Far-right Extremist. Disruptive cyber attacks tend not to fit into the objectives of this movement as they are trying to gain a psychological edge and demonstrate their dominance.

5.4.4.5 New Age

According to Gearson (2002), modern society is vulnerable to untraditional attacks. This type of terrorism stems from the development of violence as a form of protestation, especially when conventional methods of campaigning have been exhausted or unacceptable results occur. A typical New Age group is the animal rights group Animal Liberation Front (ALF) who are in opposition with pharmaceutical companies who conduct research on animals. Traditionally the types of attacks that would have been carried out are arson and sabotage.

Anti-abortion organisations and environmental groups are also examples of New Age Groups. New Age groups typically engaged in one main cause and not a wide range of issues as found with other activists. A New Age group could engage in the disruption of e-commerce and web-based advertising.

Overall, this section captures the main motivating factors that influence terrorism. It is by far a concise synopsis of the main reasons driving terrorism today. The next section addresses the focus of terrorist groups and typical targets that are attacked.

5.4.5 Target/Focus

Hacking attacks and cybercrime involving individuals or corporate organisations can in some instances incorrectly perceived to be cyberterror. Largely cyberterrorists wish to seek publicity for their movements through the execution of prominent attacks of confusion and terror. Therefore, the targets of cyberterrorism tend to have an important standing. Lewis (2002) has explained that cyberterrorism entails “the use of computer network tools to switch off critical national infrastructures (examples include energy, transportation networks, government operations) or to pressurise or intimidate a government or civilian population”. In this, way typical targets could include water facilities or transportation services like airports or railways.

According to Desouza and Hengsen (2003), the inherent dependency of businesses on electronics will allow cyberterrorists to search for ways to reveal vulnerabilities in critical services like financial institutions (banks,brokers), e-commerce sectors, transportation services, fuel supplies, power and governmental systems. Lewis (2002) states that the 911 emergency response systems, which is a specialised communications network dependant on the local telephone service, could be a prime target for terrorists. Emergency services like the ambulance, police, and fire department are thus examples of critical utilities that could be attacked. In addition, Foltz (2004) mentions cyberterrorism threats including interference or disruption of information and communications networks, emergency services, infrastructure systems, transportation systems, banking and finance systems and government services. Thus, according to Lewis (2002), Desouza and Hengsen (2003), as well as Foltz (2004), seven high level groups of typical targets thus emerge. Targets include transportation, utilities, financial sector, communications, public health and agriculture.

Table 5 provides more detailed examples of each high-level grouping. These findings reveal that critical systems are more likely to be the focus of attacks as attacks on critical infrastructure will have a far wider-reaching impact than targeting a low-profile individual user.

Table 5: Potential Cyberterrorist Targets (Own Compilation)

Transportation	Utilities	Financial	Communications	Emergency	Public Health	Agriculture and Food
Air	Water	Banks	Telephone	Police	Hospitals & Clinics	Feed Suppliers
Rail	Nuclear Power Plants	Stock Exchange	Radio	Fire	Health Department	Seed, fertilizer and Other Material Providers
Ports	Power Grids	Financial Institutions	Cell Phone Networks	Ambulance	Pharmaceutical Suppliers	Processing and Packaging Plants
Road	Oil & Gas Stations	Foreign Exchange	Internet	Search & Rescue	Mental Facilities	Storage Facilities

5.5 Techniques (see Figure 16)

This section addresses the practical methods of execution, as well as a classification of the level of attacks. Technical practices are initially described. Thereafter, the differing levels and modes of operation are explained. The classification of techniques describes those aspects of cybercrime and hacking that can be utilised to carry out cyberterrorism. Overall, this section focuses on the different attack methods and absolves fears that all cybercrime stems from cyberterrorism motives.

5.5.1 Practices

In this section, the high-level technical attack practices are listed. Typical practices that can be carried out include but are not limited to:

- Scanning systems for vulnerabilities and exploitation of these weaknesses
- Defacement of web sites showing protestation for a cause. Can also include discourteous comments and remarks relating to political parties, the government or other religious groups
- Spread disinformation
- Loss of availability of services through Denial-of-Services attacks (worms, viruses, bots)
- Causing disruption to systems by gaining unauthorised access and corrupting essential data
- Fraudulent financial activities like credit card theft, fake drugs and gambling
- Other fundraising activities

5.5.2 Attack Levels

The discussion on practices shows that there are differences in terms of the complexity and effect of the attack. This is indicative that the various attacks can be categorised to different levels. The report *Cyberterror: Prospects and Implications* from the Naval Postgraduate School (NPS) indicate that there are three levels of cyber acts (Desouza, Hensgen 2003): Simple Unstructured, Advanced Structured and Complex Co-ordinated. These levels are briefly explained as follows:

1. **Simply Unstructured**: refers to basic attacks carried out against individual systems using easily available tools. Target selection is usually carried out based on the availability of tools and detection of poor security procedures that can be easily bypassed. Examples of this type of attack are the deployment of worms and viruses.
2. **Advanced Structured**: is an attack that has more specific objectives in mind and are usually executed against multiple targets. To carry out this type of attack, the hacker needs to adapt tools and applications. Thus, the perpetrators usually have some programming skills and knowledge of the target (Nelson et al. 1999).
3. **Complex co-ordinated**: is the ability to create serious disruption to multiple targets simultaneously or successively. Various attacks are carried out from numerous sources. In order to be successful, detailed planning and orchestration is needed. Thus, this type of attack is usually run over many years and is operated by large groups capable of the necessary co-ordination and logistics.

Now that the different levels of attack have been explained, the modes of operation are discussed.

5.5.3 Modes of Operation

Another framework that can be applied to classify attacks is their wide-ranging modes of operation, which are closely related to high-level cyberterrorist objectives. According to Arquilla and Rondfeldt (2001), to make terrorism successful, significant efforts are placed into establishing organised networked groups instead of the promotion of isolated parties. Traditional terrorism operated in a hierarchical fashion but a networked based approach for communication has become far more effective than customary word-of-mouth instructions. Arquilla and Rondfeldt have proposed three broad offensive categories that information-age technology assists terrorists. These are:

- **Perception management and propaganda**: Communicating a cause to an inviting audience can be extremely powerful as it can help drum up support. Technological capabilities provide an ideal medium to attract more followers and members, find funding and influence people's views. Recruitment through chat rooms and bulletin boards can help find suitable candidates to further the group activities. Web sites serve as forum for marketing and provide exposure about the groups' activities. For example, the militant group Hezbollah has a web site, as well as its own broadcasting television station. The television stations show dramatic footage of physical attacks. In many cases, terrorist groups have created a web presence by establishing a web site.
- **Disruptive attacks**: Carrying out disruptive attacks results in the immobilisation of a site/service/system. The loss of service can be temporary or even permanent if detrimental damage is caused. Disruptive attacks can be carried out using include e-bombs, spamming, bots and hacking to deface web sites. The outcome of this mode of attack is a loss in reputation, as well as the financial repercussions. Blackmail and fund extortion are also other outcomes. For example: The Tamil Tigers executed an email bomb attack against the Sri Lankan diplomatic mission in 1996. Thousands of messages were automatically created and sent to the Sri Lankan embassy.

- **Destructive attacks**: Some viruses, worms and other exploitative tools can actually destroy a system or network. Malware has the ability to gain access to unauthorised data and corrupt it. This could lead to a system failure due to the corrupt data. Stuxnet is an example of a modern weapon that aimed to destroy the Iranian power supply. The weapon tried to destroy the equipment which would interfere with the service.

This concludes the techniques section. The next section focuses on the different objectives of cyberterrorism.

5.6 Objectives (see Figure 16)

Objectives can be divided into malicious goals and supportive functions that aid cyberterrorism in general. Therefore, there exists a differentiation between those intentions aimed at causing interference and difficulties with ICT (cyberterrorism) versus those practices that enable the grander scheme cyberterrorism.

5.6.1 Malicious Goals

Weimann (2004) mentions the objectives of terrorists. Firstly, he states that at a generalised level they seek to protest, disrupt, kill/maim and terrify people. Based on experience, in order to spread terror and grow their political clout, the most effective solution is to break things and kill people also known as BTKP (Giacomello 2004). According to Desouza and Hensgen (2003), the intention of terrorists is to force the population/government into meeting their demands. Terrorists may demand the release of political prisoners, money and the implementation of changes to the law. More specific to cyberterrorism, Weimann (2004) states that the unauthorised gaining access to sensitive information and the disruption of critical services are goals to be achieved. Such goals can cripple essential services causing fear and panic.

Gordon (2002) has explained that those concerned with terrorism may frequently stage incidents as the publicity gained from the audience feeds into their theme of manipulation. This point highlights another two objectives: the need to draw attention by staging incidents and gaining publicity from an incident. Malicious goals are more focused on the short-term goal of attackers. Long-term objectives of cyberterrorists pertains more to the motivating forces that drives them (this is discussed in Section 3.6 and Section 5.4.4). However, other goals involve the use of ICT to support terrorism in general. This is looked at next.

5.6.2 Support Functions

Terrorist goals mainly aim to inflict violence or threaten civilians or the government. Cyber technologies can be on the receiving end of these attacks. However, ICT infrastructure can also be used to assist terrorists in general. Supportive functions are not linked to any direct damage to systems but rather strengthen the activities of the terrorist organisation. Supportive functions help facilitate the execution of terrorist activities as well as help maintain operations to sustain the group.

Therefore, various ICT techniques, systems and devices may be employed to assist with planning, co-ordination, communication, intelligence and finances without being the target of a direct attack. Jenkins (2006) mentions the benefits of speciality tasks like training, recruitment, intelligence, planning, reconnaissance, logistics, propaganda, finance, and social services (assistance for families of suicide attackers).

Moreover, the US Army Training and Doctrine Command Handbook also explains how cyberspace can support terrorist operations. Support functions include (US Army Training and Doctrine Command 2006):

- **Planning:** prepare, communicate and posture
- **Recruitment**: publication of group's history on web sites, convenient hyperlinks to activate membership, and submit donations
- **Research**: provides accessibility to numerous databases, libraries and newsgroups

Overall, ICT can play a significant role in enabling terrorism in general as well as directly execute cyberterrorism attacks. As a support tool, ICT can facilitate other terrorist attacks. For example, a kinetic attack can be co-ordinated using email or social network to issue instructions and the target location. In such cases, the various technological components employed to plan the attack forms a supportive role as ICT was not the target of the attack but rather the tools of enabling a terrorist attack.

5.7 Conclusion

Cyberterrorism ushers in a new domain of concern found in the form of political or revolutionary activists disrupting or crashing critical system infrastructure. The electronic medium of computer and networks also signal in a new channel through which terrorist activities can seek to protest, intimidate, demand and cause interferences. The use of many computer security violations like web defacement or Denial-of-Service attacks through bots or viruses can be used to unleash this form of terror.

This chapter examined multiple factors to compile a structured framework that postulates the underlying issues relevant to the field of cyberterrorism. The framework presents a high-level summary, which aims to provide the reader with insight in this critical area of interest. The usefulness of the framework lies in the apt clarification of concepts and the establishment of foundational concepts that can further be examined in this research study.

The framework can be extended with new ideas as they emerge. For example, more practices and supportive functions may surface and can be added to the framework. This framework helps to acquaint the reader with the development of the mind-set of a cyberterrorist and thus brings awareness about a critical topic.

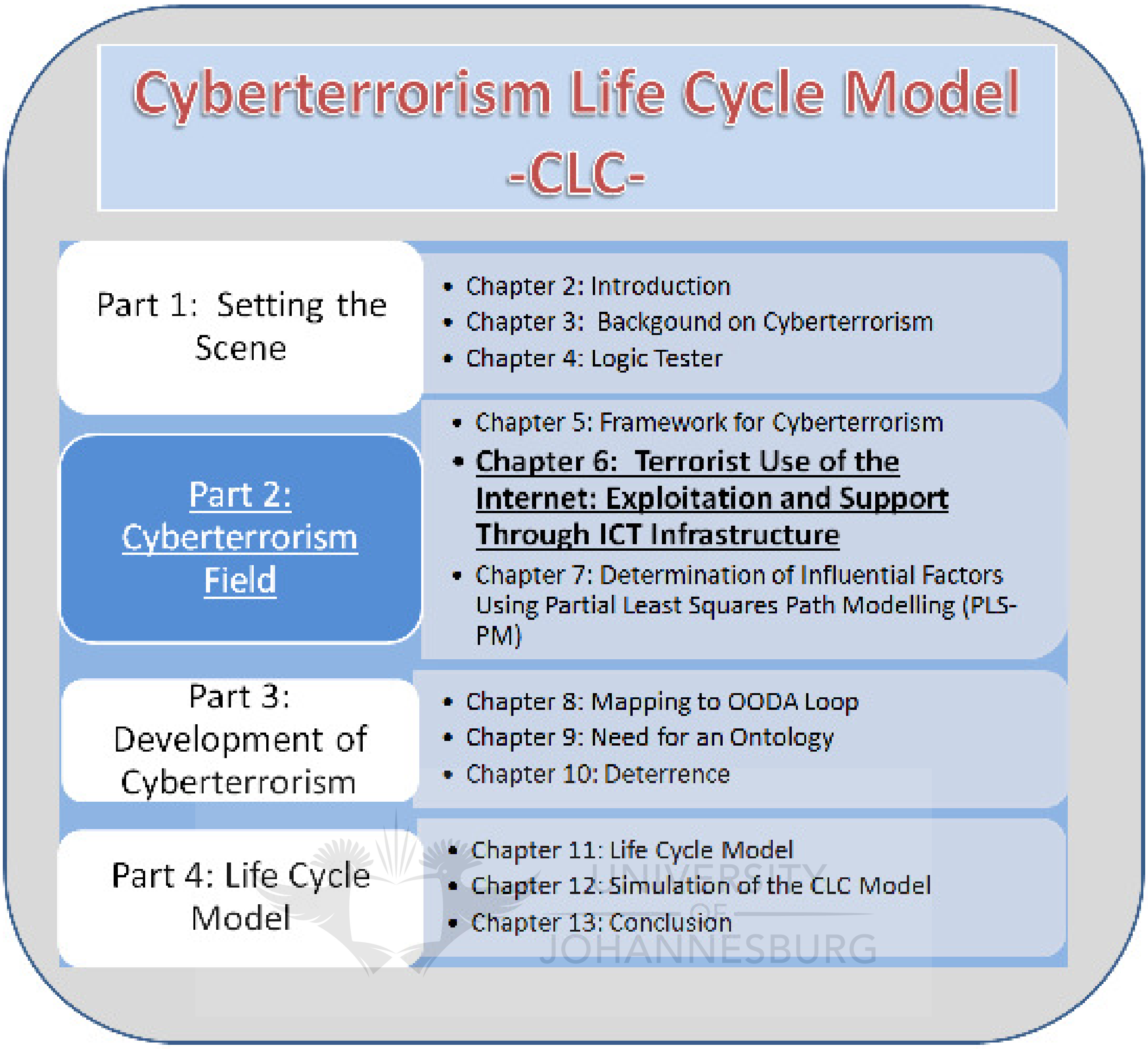
Overall, the framework intends to encapsulate critical considerations in the field of cyberterrorism and represent how these various issues are related. The framework can thus, provide a concise overview of cyberterrorism and place it in context of traditional cybercrime.

In summary, the following drivers identified in Chapter 5 contribute to the development of the CLC model:

- Cyberterrorism has sometimes been judged to be synonymous with cybercrime and cyber attacks. However, many fail to realise that many cyber attacks usually stem from traditional recreational hackers who are testing out their skills or attempting to commit some fraudulent activity. With regard to cyberterrorism, hacking skills and exploitative violations can be used to carry out attacks but it is essential to consider the motivation of the perpetrator. The CLC model will take into consideration the various technical practices that can be used to carry out cyberterrorism but will also expand on the high-level objectives and motivations to show its defining characteristics (Section 5.2).

- ICT has characteristics that assist in carrying out wide-scale high-impact attacks. This stems from the identification of the various advantages including, affordability, anonymity, variation, enormity, remote control, direct effect, automation, replication and speed. The identification of these characteristics will be used in the CLC model during the preparation phase (Section 5.4.1).
- Various social factors can influence the development of a cyberterrorist. These include: culture, beliefs, political views, upbringing and personality traits. These social factors will be shown to be a significant influential force in the CLC model (Section 5.4.3).
- In the framework, the different types of terrorism describe the different motivations behind cyberterrorism. This includes Religious, New Age, Ethno-national Separatist, Revolutionary Thinking and Far-right Extremism. The different motivations will be captured in the CLC model (Section 5.4.4).
- The capabilities that an individual/group has will determine the scope of the cyberterrorism attack. Some of the capabilities that an individual/group could possess include: training, education, expertise, skills, resources, intelligence, finances and insider knowledge. These capabilities will be reflected in the CLC model (Section 5.4.2).
- Cyberterrorism differs from cybercrime due to its distinct malicious goals. These include goals like: disrupt, protest, intimidation, kill or maim, terrify, publicity, access sensitive information, demands, soliciting money and affect crucial services. The CLC model will describe the specific malicious goals that differentiate cyberterrorism from other forms of cybercrime (Section 5.6.1).
- ICT can also play a support role to cyberterrorism. The supporting functions that ICT can play include: training, recruitment, intelligence, planning, reconnaissance, logistics, propaganda, finance and social services. The CLC model will show how ICT can also be used as a support function (Section 5.6.2).
- Cyberterrorism attacks will most likely be carried out against high-profile targets in order to maximise the damage and coverage of the attack. Typical targets include the following industries and areas: transportation, utilities, finance, communication, emergency, public health and agriculture. The CLC model will cover the different types of targets (Section 5.4.5).
- Cyberterrorists will employ specific technical and hacking methods to carry out their attacks. Practices include: web defacement, disinformation distribution, propaganda, worms and viruses, affecting critical data and systems, credit card theft. The CLC model will indicate the different types of practices that are carried out (Section 5.5.1).

Chapter 5 consisted of a literature study of the field of cyberterrorism in order to identify influential factors (Sub-objective 4). This literature study was presented as a framework and aimed to provide the user with background knowledge in the field of cyberterrorism. The chapter discussed the main operating forces and introduced some of the reasons motivating cyberterrorists, as well as some of the practices carried out on ICT. However, further work is needed in order to classify their practices and objectives. The next chapter takes a closer look at identifying and classifying the use of the Internet as a means of exploitation and support.



Cyberterrorism Life Cycle Model -CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- **Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure**
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS-PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

6 Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure

> *"The single biggest existential threat that's out there, I think, is cyber"*
>
> *- Michael Mullen Former Joint Chief of Staffs*

In Part 1, Chapter 3 introduced the field of cyberterrorism. It provides the background to the field by discussing the core definitions, a few examples and terrorist groups. Chapter 3 established some of the basic ideas and examples related to cyberterrorism. Chapter 4 discussed critical aspects relevant to the definition like the motive for fear and the clarification of cyber concepts.

Part 2 looked at further clarification of the field of cyberterrorism with Chapter 5 summarising cyberterrorism in a framework that covered operating forces, techniques and objectives. Chapter 5 briefly discussed some of the objectives and practices of cyberterrorists. This chapter will discuss in detail why and how the Internet can be used in the exploitation and support of terrorism. The research in this chapter is based on research published by the author at 2011 International Conference on Information Warfare (See Chapter 14 for paper details).

Figure 17 indicates the current focus in this chapter for establishing the building blocks for the CLC model. Chapter 6 addresses Sub-objective 3 Techniques and countermeasures (originally presented in Figure 3).

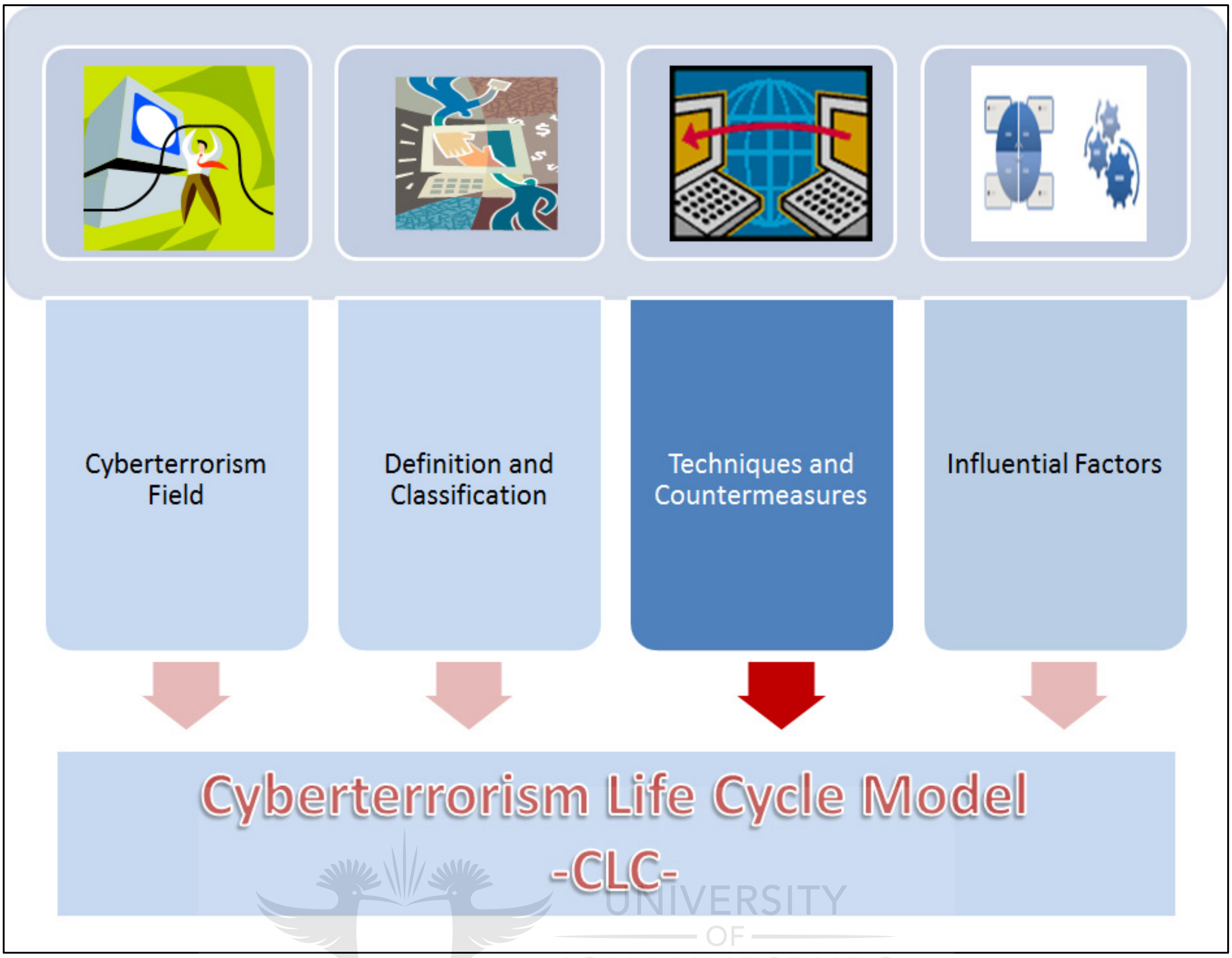

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 17: CLC Model Focus Chapter 6 - Cyberterrorism Techniques and Countermeasures (Own Compilation)

6.1 Introduction

The advancement of technology has enabled a wealth of useful capabilities. Terrorism has also grown to utilise ICT, especially the Internet. Massive informational resources can be accessed via the Internet. In addition, cyberspace offers an affordable and instantaneous method of communication from almost anywhere in the world. Consequently, the traditional hierarchical operations of terrorists groups have evolved and now embrace the convenience and capabilities of digital networked technologies. The framework presented in Chapter 5 briefly introduced some of the methods that terrorists employ using ICT. In this chapter, a closer look is taken at the different functions and methods that terrorists utilise ICT infrastructure for. This chapter therefore explains the technical and practical functions that ICT serves in facilitating terrorism.

Terrorists now use the Internet not only for traditional functions but have also embraced it for its more innovation capabilities. The digital domain provides a wealth of potential recruitees, members, recipients and also enemies to target. Talihärm (2010) states that the list of Internet-based terrorism actions includes propaganda, public relations, sharing information through instructions/manuals, fundraising, communication and recruitment.

This chapter addresses how the Internet can be used as both a uni-directional and bi-directional tool to aid support functions like training, propaganda, funding, recruitment and operations. The chapter also looks at particular methods of cyberterrorism, including web literature publications, anti-forensics social-networking tools, and fund-raising incentives. Other examples, such as cloaking and coding techniques are also discussed. In this chapter, the traditional Internet functions and terrorism support methods are mapped to the more innovative uses that terrorists are now employing.

6.2 Background

The Internet World Stats webpage (2013) reports that the latest number of world Internet users are 360 985 492. This represents a 34.3% penetration of the world population. While this statistic indicates that only a minority of the world population regularly engages in cyberspace activity, it does represent a vast amount of potential recruitees, members, recipients and enemies that global terrorist groups could reach digitally.

Most aspects of daily lives are touched by technology and in many homes and businesses, the Internet is a prominent feature. The Internet provides access to a wealth of information, and communication can be carried out around the world rapidly, conveniently and inexpensively. Due to these technological advancements, terrorists groups have also shifted their viewpoints on technology and are now adopting new ways of operating that take advantage of digital conveniences. The document "'al Qaeda: The 39 principles of Jihad'" was published in 2003 on the al-Farouq website. In the document, Principle 39 states that it is a sacred duty to perform electronic jihad. Furthermore, in the document, the group's members are urged to participate in Internet forums. The document claims that the Internet is an enabling opportunity to influence millions of people in seconds. Internet savvy members are encouraged to support the jihad cause by hacking into enemy websites and destroying them (Atwan 2006).

Furthermore, the book, "The secret history of Al Qaeda", provides an eyewitness account of al Qaeda men trying to flee from the United States bombardment of training camps, which took place in November 2001. A description from the book states that everywhere a person looked there was an al Qaeda member carrying a laptop and their Kalashnikov weapon (Atwan 2006). Such imagery is highly topical as it draws attention to an organisation that now operates using hi-tech electronic devices in order to organise, grow, function and essentially survive in the modern world. Looking back to the early 1980s, many groups in Afghanistan were strongly opposed to the use of any technology that originated or was designed in the West (Atwan 2006). However, due to the speed, reach and convenience of cyberspace, terrorist groups' can now embrace the use of technology.

Based on this principle, terrorist groups have now expanded their Internet usage from traditional functions to include more innovative purposes. This chapter will provide an overview of some of the typical functions, methods and examples that terrorists use the Internet for. Some functions and methods overlap each other and therefore, a strict one-to-one mapping is not feasible. Rather, the discussion aims to increase awareness of the technical and practical role that ICT plays in assisting and executing terrorism.

6.3 Functionality of the Internet

According to Piper (2008), terrorists make use of the Internet, due to the ease of use and reduced cost to spread information worldwide rapidly. The very nature of the Internet makes it an ideal channel for terrorist to engage in. Weimann (2005b) states the Internet has limited or even non-existent regulation that makes it an anonymous multimedia that has the powerful ability to influence traditional mass media coverage of events.

Originally, the Internet was created to enable communication between two computers but now due to the networked and storage capabilities, it provides access to a tremendous wealth of information that can be reached globally. Charvat (2010) explains that the Internet has formed part of the terrorism radicalisation process and is being used for propaganda, misinformation, grooming and misinformation (recruitment). Furthermore, Weimann (2014) explains that social media has become important tools for recruitment, propaganda, fund-raising and even training like building a bomb.

In Figure 18 the traditional and innovative functions of terrorist Internet usage are shown, as well as a mapping of methods to functionality type.

- **Recruitmen**t: engaging with individuals to attract their interest in a movement's cause. Potential members can then be selected and screened before joining the group. This is typically carried out through web literature and social networking tools.
- **Training:** dissemination of information to develop the skills and competency of new recruits and existing members. Topics can include information needed during a terrorist operation, use of tools and method of attack, goal of attack strategy. Social networking tools and anti-forensics methods can be applied for this purpose.
- **Communication:** is the transfer of information to members both within and outside of the terrorist group (instructions and promotion of the movement). Social networking tools and anti-forensics methods can be used for this purpose.
- **Operations**: managing and controlling the execution of attacks and the organisation as a whole. Operational activities entail the use of web literature, anti-forensics and fundraising activities.
- **Propaganda:** a type of communication tactic that aims at influencing people towards supporting a specific cause. In some cases, propaganda is even referred to as mis-information, which can be seen as the spread of an altered type of information. Both web literature and social networking tools can be employed for this purpose.
- **Funding**: the generation of funds to support the activities of a terrorist organisation. Fundraising incentive schemes are applied for this purpose.
- **Psychological warfare**: the ability of spreading disinformation to instil fear and powerlessness within the enemy ranks. Web literature and social networking tools can be applied for this purpose.

The Internet ideally suits the tactics of terrorists in terms of their recruitment, training, communication, operational, propaganda, funding and psychological warfare needs. All of these functions can rapidly, remotely, conveniently and cheaply be carried out over the Internet. Brunst (2010) has stated that the Internet is a desirable tool as provides for many advantages like prime location, independence, speed, anonymity, internationality and a relatively low cost benefit ratio. Denning (2009) discusses the use of terrorist web sites to offer news reports, propaganda and directly distribute information to its members and supporters. Figure 18 represents the traditional use of the Internet by terrorists (communication and information gathering tool), as well as the emerging, innovative functions (at the time of writing these can be considered innovative). Examples of the Internet exploitation methods are shown in Figure 19. The Internet can be used to carry out both uni-directional and bi-directional communication. This means that the Internet can be used to target a specific individual for example communication and recruitment or it can be used to reach a wider audience like fund raising incentives or training.

This list is by no means exhaustive, but shows typical examples of how the Internet can be used to support terrorism as well as the evolution of ingenious new functions and methods. The next section takes a look at, specific methods that terrorist employ.

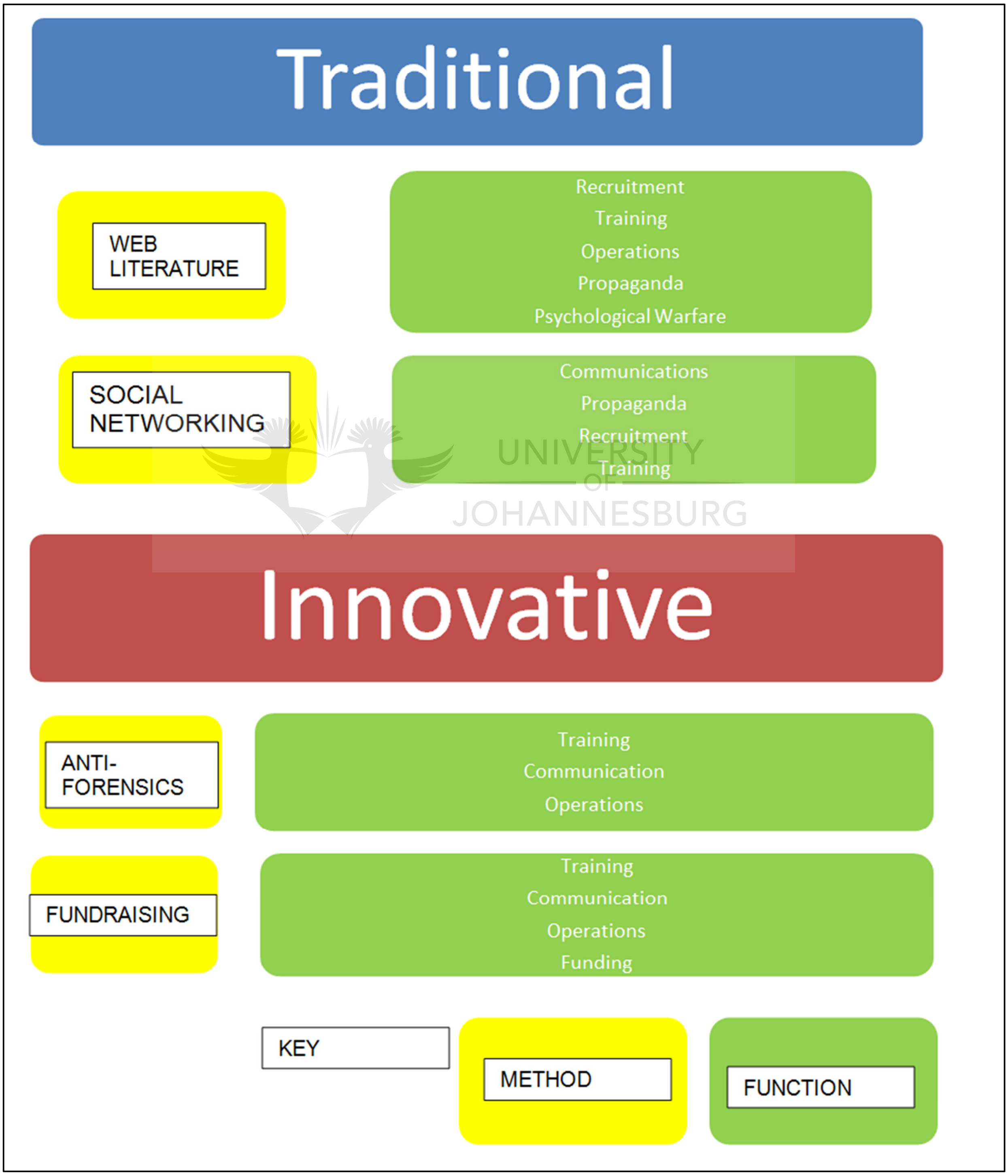


Figure 18: Terrorist Use of the Internet (Own Compilation)

6.4 Exploitation of ICT Infrastructure for Terrorist Support

In this chapter, Internet exploitation methods are classified into five main groups. Figure 18 showed four of the five groups of Internet exploitation methods but in Figure 19 another group entitled Other is introduced to provide additional examples of how terrorist groups are exploiting the Internet. The groups are:

- Web literature
- Social networking tools
- Anti-forensics
- Fundraising
- Other

Figure 19 shows this grouping of Internet exploitation methods, as well as a few examples of these methods. A discussion follows on each of these Internet exploitation groups.

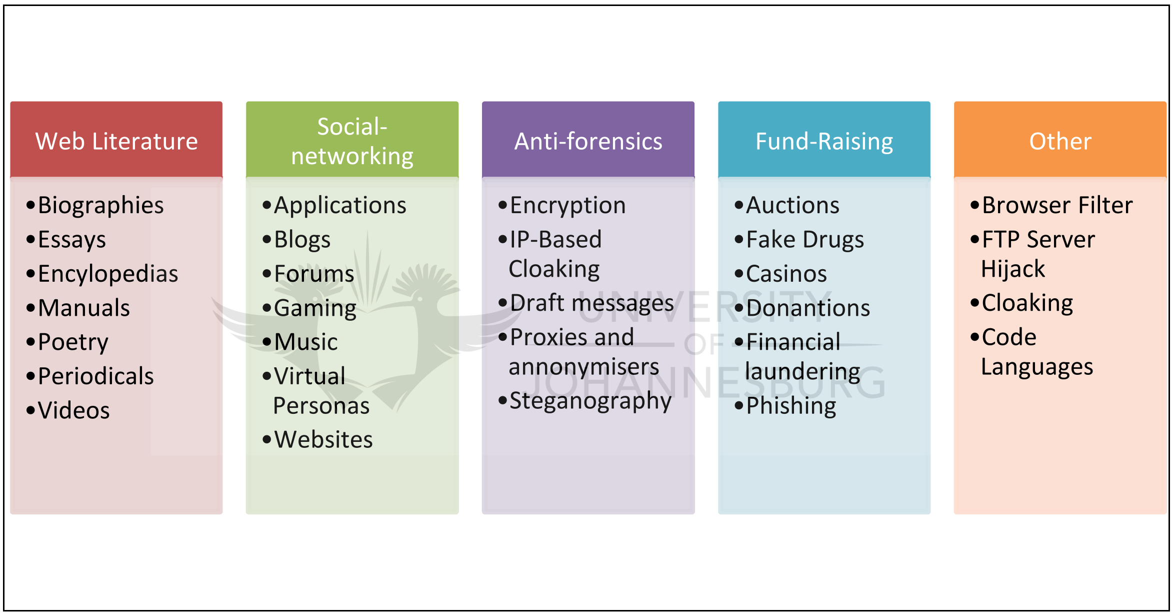


Figure 19: Internet Use Examples for Terrorism Support (Own Compilation)

6.4.1 Web Literature

Web literature consists of the online publication of a collection of material describing a specific subject. Web sites can host a variety of content relating to terrorist groups. These include: manuals, encyclopaedias, essays, poetry, biographies, video, music, statements and periodicals. Web literature utilises a mass uni-directional method of communication, which ideally suits terrorists' requirements of recruitment, training, propaganda and operations.

In a special report by Radio Free Europe/Radio Liberty, the manner in which Sunni Insurgents in Iraq and their worldwide supporters use the media is discussed. The report states that terrorist media campaigns produce a number of published items consisting of text, audio-visual and website content (Kimmage, Ridolfo 2007). The distribution of text and audio-visual media utilises the Internet in a traditional way, with little means of unconventional application. The text media industry consists of the release of press statements, operational statements, inspirational texts and martyr biographies. Denning (2009) explains that al Qaeda began with the web site alneda.com in the 1990's, and since 2002, this site containing audio and video of bin Laden, justification of the 9/11 attacks, poetry and messages has been on the run and regularly moved to different domains and service providers. Furthermore, online training material can describe in detail how to make letter bombs; deploy poisons and chemicals; car bomb detonation; shoot soldiers; use the stars to navigate (Coll, Glasser 2005) and the assembly of a suicide bomb vest (Lachow, Richardson 2007).

Dedicated websites within terrorist circles have become prominent. Weimann (2004) lists the following group web sites:

- Alneda.com, which was closed down in 2002, is claimed to have encrypted information between al Qaeda members.
- Assam.com provided jihad support for members in countries like Chechnya, Afghanistan and Palestine.
- Qassam.net is believed to be linked to al Qaeda, as well as Hamas.
- 7hj.7hj.com taught users hacking of networks and governmental and organisational website infection.

These dedicated websites tend to publish the vision and mission statement of the group, as well as news about current activities. Propaganda tactics may focus on gaining the sympathy of the public. Ulph (2010) mentions a number of sources like ideological materials, treatises, books, encyclopaedias that are available online to transform a reader into a soldier dedicated to a cause. Websites established by insurgent groups provide detailed tutorials to group members, like techniques to bypass a web server and hack a web site. Lappin (2010) discusses how new jihadis are recruited using videos on web sites containing quotes from the Koran and the message of the need to distance oneself from society.

An al Qaeda training manual claims that it is possible to gather at least 80% of all information required about the enemy through the use of open Internet sources without even having to resort to illegal means (Weimann 2005b). Since the 9/11, terror attacks over 1 million pages of historical government documents were removed from public view. This aimed to reduce the risk of information disclosure. One of the removed documents was a Federal Emergency Management Agency database which contained details describing various federal facilities, with approximately 200 000 pages of naval facility outlines and blueprints. Since the data was removed from public domain, individuals can still request to see sections based on stipulations made in the Freedom of Information Act (Bass, Ho 2007).

The wealth of information that can be collected over the web includes blueprints, site photos, maps, satellite images, transport routes, power plant designs, communication grid layouts, pipeline systems, dam designs, water supply routes, natural resource distribution locations and email lists. In the hands of a malicious terrorist, this information may not only be used for cyberterrorism, but also to plan a traditional terror attack without even having prior physical access to the target location. In addition, flight simulation software can be used by terrorist groups to train members. Recruitment campaigns are carried out using web literature. Terrorism is glorified through enticing media coverage. The web is thus aiding terrorist groups to recruit, attract, train and operationalise members.

6.4.2 Social Networking Tools

Social networks provide for social interaction and communication between like-minded people, contacts, family and associates. However, socialising and communication are not the only uses of social networks. Information, music, games, advertising and marketing are amongst the myriad of capabilities that social networks provide. Consequently, terrorist groups are also engaging in social networks, forums and blogs to identify recruit and train supporters, members and participants. Social networking tools enable both uni-directional and bi-directional communications, that can be used for recruitment, training, propaganda and communication.

New members to social networks and gaming sites often need to create a virtual persona and specify basic information like name, skills and interests. These virtual personas can be used by terrorist groups to identify potential recruits (Whelpton 2009). Potentially terrorists could discover individuals with a background in chemistry, engineering or weapons development and persuade them to join the movement. Social networks, forums and blogs provide access to information about people's interests, skills, beliefs and careers. Terrorists are keen to prey on this type of information and convince users that their support and skills are needed by terrorist groups. Furthermore, online gaming sites are also prime hunting grounds for terrorists (Whelpton 2009). Online players that have a strong shooting ability could be indicative that they have violent tendencies. Terrorist groups would profile, engage and interact with the potential recruitees, as violent temperaments may be suited for the terrorists operations.

Conway (2012) explains that since large numbers of people can gain cheap and easy access to the Internet, violent extremists are pushing their content across social networking sites like Facebook and Bebo, YouTube, dedicated blogs and Twitter. This gives these radicals access to a far larger and diverse audience. Social networking sites like Facebook and MySpace have traditional interfaces through which the public can engage with accepted contacts. However, this form of technological communication has evolved to become customisable. West and Latham (2010) explain that social networking creation sites have become a dream for online extremists – these platforms are affordable, easy-to-use, provide customisation and beneficial to online extremism. For example, Ning supports the creation of an individualised site where users can upload audio and video files, send and receive messages, make blog entries, update events and access RSS feeds. Similarly, a terrorist group could also set up a customised social site, which it controls and thus post messages, propaganda and fundraising announcements. Furthermore, Seib (2011) mentions that the pioneering use of platforms like YouTube, Facebook and web forums are making terrorist operations appear very attractive to the audience.

Music has also become a popular way of attracting members (Whelpton 2009). Islamic and white supremist groups have created appealing songs that have pop and hip-hop beats. The performance of this type of music helps attract young teenagers. The lyrics of the music endorse the movement's goals and the appealing rhythm of the music keep the youth enthralled. Seib (2011) mentions the use of videos in cyber cafes in Tangier or Amman showing American soldiers being killed while a thrilling martial soundtrack and appealing promises plays in the background to those who also join the fight.

Other social networking examples include chat rooms, discussion groups, bulletin boards, and micro blogging (such as Twitter). Charvat (2010) discusses the use of games, forums, chat rooms and links to webs sites to find susceptible supporters. These channels can also help aid terrorist groups in hiding their communication. Matusitz (2013) states that Internet chat rooms allow for the simultaneous dissemination and immediate co-ordination of cyberterrorism members. Furthermore, Lappin (2010) says that the virtual operation of terrorists consists of interconnected computers, chat rooms and servers. Lappin, also states that this cutting edge technology is being used to plot terrorist attacks and share blueprints.

6.4.3 Anti-Forensics

Anti-forensics entails the use of tools or methods that opposes the use of customary forensic tools and methods. In other words, anti-forensics is the attempt to disguise activities so well that even forensic techniques cannot detect the existence of the concealed activities. Examples of anti-forensic techniques include steganography, encryption, dead dropping, IP-based cloaking, proxies and anonymising. Anti-forensics techniques are mostly targeted at uni-directional communication and thus help support training, operations and communication within terrorist groups. The above-mentioned techniques will now be discussed in detail.

Steganography consists of covertly hiding messages inside another form of communication. This is carried out by embedding the hidden message into another innocuous form of communication like an image, sound clip or text file. The hidden message can be extracted from the original message through the application of the appropriate key. Other secure alternative means are used to deliver the password or passphrase to its intended recipient (Lau 2003). The message in which the hidden message is embedded does not display any visibly evident signs of concealment. Thus, while no obvious visual signs can be detected in the modified carrier; a statistical analysis may reveal that the carrier has been modified. The Technical Mujahid February 2007 edition encourages readers to search and download a copy of the encryption program *"Secrets of the Mujahideen"* (2007). This program is capable of hiding data in the pixels of the image and then compressing the file to avoid being detecting during steganalyis.

Virtual dead dropping, or draft message folders is another technique that would bypass messaging interception techniques. Bruce Hoffman from Rand Corp (in Noguchi, Goo 2006) explains that terrorists create free web based email accounts and then provide the login credential for the accounts so that the drafts messages can be read without ever sending them over the Internet. The email account name and password are communicated to the intended recipients in code using chat forums or secure message board. This technique is used especially for highly sensitive information (Nordeste, Carment 2006) and if electronic interception legislation may come into play.

Another anti-forensic technique that can be applied is the redirection of traffic through IP-based cloaking. Cottrell (in Carr 2007) at a seminar in FOSE 2006, stated that when the Web server receives a page request, a script is run that checks the user's IP address against a list of known governmental IP addresses. If a match is found, the server returns a Web page containing fake information. If no match is found, the requesting user is sent to a Web page with the correct information. Based on this principle a similar technique called IP-based blocking has developed which blocks users' access to a site instead of redirecting them to another site. Such practices are termed cloaking as the authentic site is masked.

Terrorists utilise a proxy as a secure channel to hide their activity on the Internet. The Search for International Terrorist Entities (SITE) Institute identified a posting that promotes the use of a proxy as it removes digital identifiers like web and IP addresses (Noguchi, Goo 2006). The basis of this approach is once a user connects to a proxy, the proxy requests an anonymising site to redirect the user to the requested site. When a user connects to the proxy, an encrypted channel secures the communication by hiding the originating user's details. Furthermore, the renowned cyber terrorist Irhabi 007 (Terrorist 007) provided security guidelines by sharing anonymising software that concealed an IP address (Labi 2006).

Spammic.com has developed an innovative use of the Internet. Spam is the unsolicited distribution of mass volumes of email. For the average netizen receiving random or unwelcomed marketing communication is a nuisance. Spam filters are set up to block these messages automatically but if they do reach recipients, the automatic response of users are to delete them. However, Spammimic.com now provides a novel functionality that conceals messages and hides information within the text of regular email. The approach is not a true form of encryption but rather the concealment of short messages in what appears to be spam. Due to the spam-like appearance of the email, few people will pay close attention to the message. Thus, only the intended recipients will be informed that the email contains a disguised message and decode it through the web interface (Tibbetts 2002).

6.4.4 Fundraising

Fundraising entails urging and gathering contributions by appealing for donations, especially monetary funding. Terrorists often use illicit means to gather funds. These include: donations, auctioneering fake items, hiding money in online casinos, credit card theft, drug trafficking, fake drug offering and phishing. Fundraising consists of targeted communication aimed at assisted activities and providing financial backing to keep the organisation operational.

The 9/11 terrorist attack sparked a reliance by terrorist groups to use the Internet to generate funds for their organisations. Websites of popular terrorist organisations publish links like *"What You Can Do"* or *"How Can I Help".* The request for funds on terrorist websites appeals to sympathetic users to contribute to the organisation by making donations that will help sustain the group. Such visitors can then be identified and further monitored and researched to determine the possibility of recruitment. Individuals repeatedly visiting the website or spending large amounts of time on the website are contacted (Piper 2008). Once contact is established, they are directed to secret chat rooms or given instruction to download software, which will enable communication on the Internet without the risk of being monitored (Nordeste, Carment 2006).

Gentle persuasion and appeal for legitimate financial support can be used to generate funds. However, terrorists also carry out disguised methods of fundraising or even employ malicious techniques to generate funds for their group. Terrorists may utilise electronic money transfer, laundering and support from front organisations (Goodman, Kirk & Kirk 2007). The Financial Action Task Force states that non-profit organisations mis-use funds to finance terrorism and this has become a crucial weakness and global struggle, (Jacobson 2009). Mercy International, Rabita Trust, Global Relief Fund, and Help the Needy are all examples of such exploitation (Conway 2006). Many charities are established solely to finance terrorism, while others are active entities that have been infiltrated by terrorist supporters from within the organisation itself (Jacobson 2009).

Online auctioneering is also used to move money around. The practice consists of two partners, known as smurfs, who arrange a fake transaction. One partner places a bid on an alleged item on auction and makes the payment to the auction house. The recipient smurf thereafter receives the payment for the fake item on auction. Another type of auctioneering scams entails user bidding on their own item to store money and hide their activity (Whelpton 2009). In one specific example, a set of second-hand video games were offered for $200. However, the same set of brand new video games retails for $39.99 (Tibbetts 2002). The absurdly high sales prices are not against the law, but will only attract the attention of those involved in the scheme. These types of tactics provide an easy mechanism for terrorists to move money around without actually selling or delivering any auctioned goods or services.

Terrorists also make use of online casinos to launder and store money. Large sums of money can easily be managed in online gambling sites. Terrorists will place small bids to keep the gambling accounts active and safely store and hide the rest of the money in the online casino (Whelpton 2009). Winnings could also be cashed in and electronically transferred to specifically designed bank accounts which can hide the originator and owner (Jacobson 2009).

Terrorist fundraising activities also include the use of stolen credit cards. For example; Irhabi 007, together with his accomplice were able to accumulate 37 000 stolen credit card numbers, and made over $3.5 million in charges (Jacobson 2009). Another incident involved a request, originating from Paris to purchase domain space in 2005. The credential for the payment came from stolen credit card details. Shortly afterwards a similar request from another name in Britain was sent through for nearby domain space. These incidents were flagged as being fraudulent .The backup files from the initial site were investigated. While the files were mostly in Arabic, video footage showed insurgent forces in conflict with American forces, (Labi 2006).

Terrorists also rely on drug trafficking as a large source of income. Tamil street gangs operate in Canada by sending the proceeds from bank and casino fraud, immigration fraud and drug smuggling to LTTE to support terrorist activities (Biersteker, Eckert 2007). Fake Internet drugs are put on offer, and often they contain harmful ingredients like arsenic, boric acid, talcum powder, brick dust, chalk, leaded road paint and polish. In these elaborate schemes, people are tricked into believing they are buying legitimate drugs (at sometimes low prices) but actually receive fake drugs. The money received for these drugs is used to support terrorism financially. According to the UK Medicine and Healthcare Regulatory Agency almost 62% of the prescription medicine on sale on the Internet, obtained without a prescription, are fake (Whelpton 2009).

6.5 Other ICT Infrastructure Exploitation Examples

Kovner (in Lachow, Richardson 2007) explains that one of al Qaeda's goals for using the Internet was to create resistance blockades to stop Western ideas from infiltrating Islamic institutions. Unsuspecting users are given Internet browsers so that content believed to stem from undesirable Western sources could be filtered out. Brachman (2006) mentions jihadi computer programmers that configure machines with browsing software, similar to the browser Internet Explorer but it only searches specific sites and thus limits the ability to access certain online destinations.

The infamous terrorist Irhabi 007 also used a technique to exploit vulnerabilities in File Transfer Protocol (FTP) servers, which reduced the risk of exposure and saved costs. Irabhi transferred files (including videos of Osama Bin Laden and the 9/11 hijackers) onto an FTP server at the Arkansan State Highway and

Transport Department and then posted links to users encouraging them to download the files but also warned them that there was a limited window of opportunity to access the files (Labi 2006).

SITE (in Brachman 2006) discovered a guide explaining to jihadis how they could use the Internet safely and anonymously. In the guide, descriptions are given of how governments identify users, infiltrate software chat programs (like Microsoft Messenger and Paltalk), and recommends readers not to make use of Saudi Arabian based email addresses (those ending with .sa) as they are considered insecure. Instead, readers are encouraged to make us of anonymous accounts provided by commercial vendors like Yahoo or Hotmail.

Another trend for terrorists is cloaking which looks at ways in which terrorists can hide their activities. Cottrell in 2006 (in Dizard 2006) explains the following cloaking trends, which have emerged in recent times:

- Terrorist organisations create fake websites that hide their covert information or publish mis-information to users so as to misguide visitors identified as federal employees or agents.
- Criminal and terrorist organisations are progressively blocking all traffic from North America or those originating from IP addresses from users in countries who depend on the English language.
- Another cloaking practice is the communication of fake passwords at covert meetings. If one of the fake passwords is used, the individual is marked as possibly being a federal intelligence agent. Subsequently, this identification increases their vulnerability of being kidnapped or unwitting becoming a carrier of false information.
- Hackers establish a set of criteria which are shared using the Linux operating system and the Netscape browser. If federal investigators operating on computers with Windows and Internet Explorer visit the hackers' shared site, the hackers' system immediately mounts a Distributed Denial-of-Service attack against the federal system.

Furthermore, terrorists also use a specially developed code to communicate. If inconspicuous words and phrases are used, messages can be sent in a public forum without drawing undue attention. For example, the final message from Mohammed Atta's to the eighteen terrorists who were involved in the 9/11 attacks is reported to be some form of a code. The message talks about the semester commencing in three weeks and the receipt of nineteen confirmations into the faculty of law, urban planning, fine arts and engineering. The reference to the various faculties is believed to be code for the buildings targeted in the attacks (Weimann 2005b).

Website defacement is also a popular way for terrorists to reveal their technical skills and generate public fear. Public alterations of visible websites to a large audience create the perception that critical systems governing these websites are not secure. Such an attack occurred in 2001, when a group known as the Pentaguard defaced various government and military websites in the United Kingdom, Australia, and the United States. Another incident occurred when pro-Palestinian hackers who coordinated an attack to infiltrate 80 Israel-related sites and deface them, including al Qaeda, inserted images on the hacked website of the Silicon Valley Landsurveying, Inc. of the murdered Paul Marshall Johnson, Jr (Brunst 2010).

6.6 Conclusion

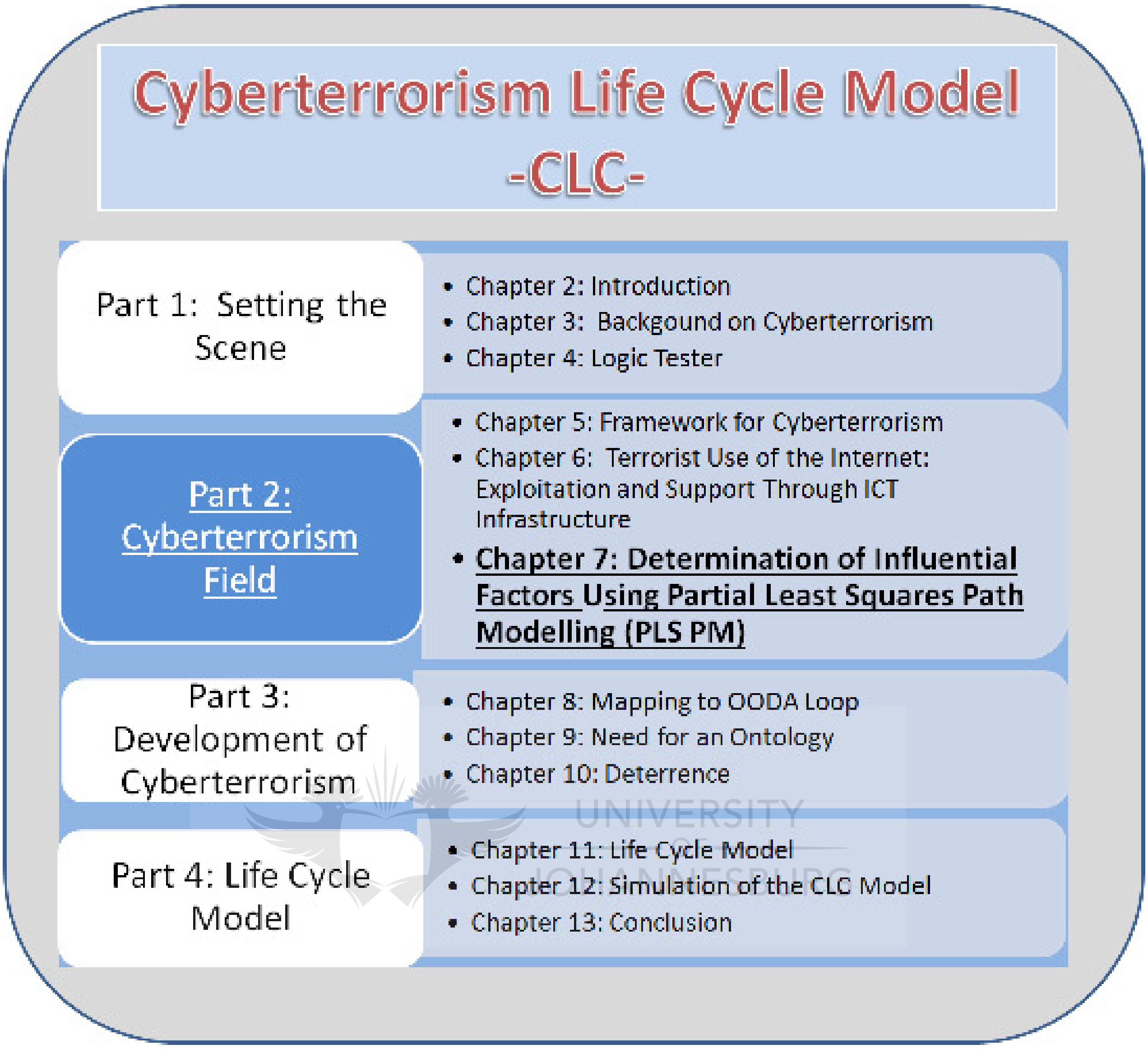
The Internet is now being used for both traditional, as well as innovative functions. Security features in ICT are also enabling the concealment of terrorist activities. Networked capabilities of cyberspace provide a vast landscape to attract members and identify targets. Terrorists can now embrace the anonymity, remoteness and accessibility offered by technology in order to support and carry out operations.

This chapter aims to create awareness of the capabilities that ICT infrastructure has in supporting terrorist groups in their operations and normal functions.

The main drivers derived from this chapter that will be captured in the CLC model are summarised as follows:

- The Internet has a very useful capability in that it can be used for traditional uses, as well as more innovative functions. The traditional and innovative uses of the Internet will be represented as malicious objectives and support functions in the CLC model respectively (Section 6.3).
- These support functions include recruitment, training, communication, operational planning and execution, propaganda distribution, fund raising and the execution of psychological warfare. These support functions will be captured in the CLC model (Section 6.3).
- The use of the Internet for cyberterrorist can also be grouped under the following classifications: web literature, social-networking tools, anti-forensics and fundraising. These classifications and detailed uses will form part of the practices in the CLC model (Section 6.4).
- Propaganda and knowledge creation is carried out using web literature. Examples of web literature include periodicals, essays, manuals, encyclopaedias, poetry, videos, statements and biographies. These concepts will form part of the explanation of practices in the CLC model (Section 6.4.1).
- Social-networking tools include forums, blogs, websites, gaming, virtual personas, music and applications. The effect that social-networking tools can have in recruitment, training and communications will be shown as part of the practices in the CLC model. These topics can also have significant further research in studying the recruitment, training and communication practices in order to develop ways of interception and prevention. (Section 6.4.2)
- Terrorists are constantly trying to utilise ICT to their advantage without leaving a trace of their actions. Some of the identified anti-forensics methods that are being used include: steganography, draft message folders, encryption, IP-based cloaking, proxies and anonymises. The CLC model will indicate these anti-forensic techniques in order to show the ingenious practices that are being carried out in order to hide their activity and also highlight that new and innovative methods will most likely also be developed (Section 6.5).
- Fund-raising is carried out using various scams including auctioneering fake items, online- casinos, drug trafficking, fake drugs, donations, credit card theft and phishing. The CLC model will incorporate these fund-raising schemes 6.4.4.

The research in this chapter demonstrated that international terrorist groups can make use of the Internet for many of its traditional functions to stimulate growth and facilitate operations. This chapter demonstrates that terrorist groups can utilise the functionality of ICT infrastructure in order to advance their groups purpose and operation. This chapter discussed various examples of Internet exploitation. As attackers evolve to discover new forms of threats, so too will other innovative terrorist methods of ICT exploitation arise.This chapter also discussed the various practices and support functions that terrorists may rely on ICT. The next chapter also looks at investigating more influential factors. It focusses on a using Partial Least Squares Path Modelling to analyse survey data.



Cyberterrorism Life Cycle Model -CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- **Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)**

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

7 Determination of Influential Factors using Partial Least Squares Path Modelling (PLS PM)

““Stuxnet was the first virus to create physical damage – it was purely electronic in its origin but caused actual explosions and meltdown, which hadn’t been seen before. Now terrorists don’t need to board planes and put bombs in location, but can use the internet to get into critical infrastructure or nuclear facilities and cause explosions. This is a new type of risk.””

- Laila Khudairi, Underwriter – Enterprise Risk at Lloyd’s underwriter RJ Kiln & Co.

7.1 Introduction

Part 2 focuses on the influential factors and techniques of cyberterrorism. In Chapter 4, a framework of cyberterrorism is proposed which discusses various influential factors. Chapter 6 further elaborates on the framework by explaining more examples of practices and support functions. Chapter 7 will further elaborate on the influential factors by investigating the potential impact of a few social factors. In this chapter, Partial Least Squares Path Modelling (PLS PM) is used to determine whether a few factors have a significant effect on the development of a cyberterrorist.

PLS PM is a statistical technique and the benefit of this modelling technique is that is serves to prove mathematically whether a few factors have an influence on cyberterrorism. In previous chapters, philosophical reasoning was used to identify influential factors, whereas In this chapter, the reader will be introduced to various statistical calculations.

Figure 20 shows that this chapter further elaborates on influential factors relevant to the field of cyberterrorism and thus mainly addresses Sub-Objective 2, Influential Factors (originally presented in Figure 3).

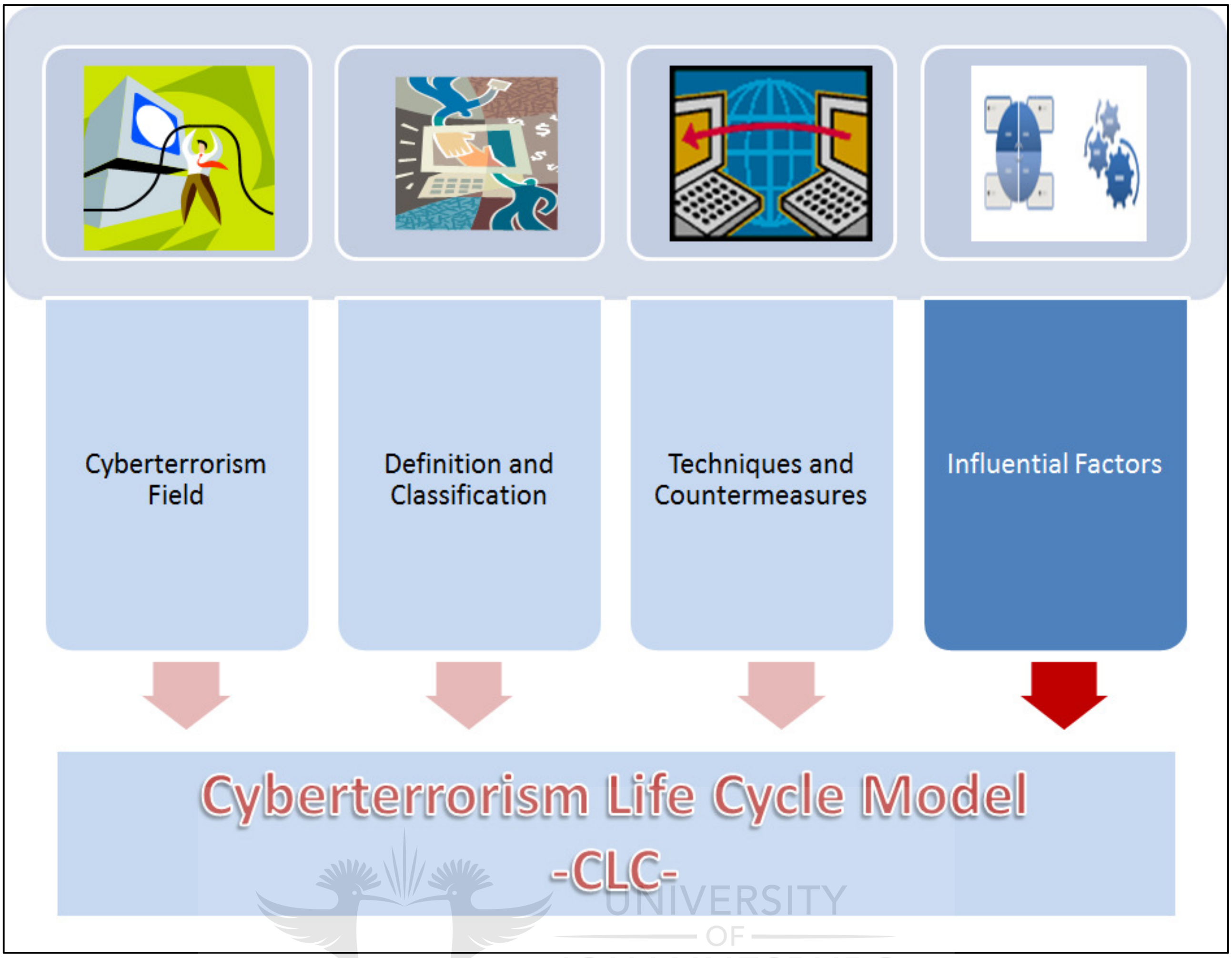

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 20: CLC Model Focus Chapter 7 - More Influential Factors (Own Compilation)

Technologies are continually being adopted, which has resulted in a strong dependence on critical infrastructures that may utilise networked resources. Civilians with hostile views, political strategies and other ideologically motivated reasons may attack these critical infrastructures. This chapter addresses the willingness of individuals to attack critical infrastructure using technological methods based on certain political and ideological viewpoints. The findings look at the possibility of virtual attacks based on nationalism, antagonism, group equality, group dynamics and technical outlooks. The implications of this research will be the determination whether certain social factors have a strong influence on cyberterrorist behaviour.

7.2 PLS Modelling Introduction

Initially, a brief description of PLS Modelling is given in order to familiarise the reader with the basic constructs and motivation for using this technique.

Figure 21 shows a summary of the functionality of PLS as proposed by Sanchez (2013a). Overall, the technique provides for useful approach to exploring, describing, explaining, predicting, classifying, discrimination and showing causality in systems.

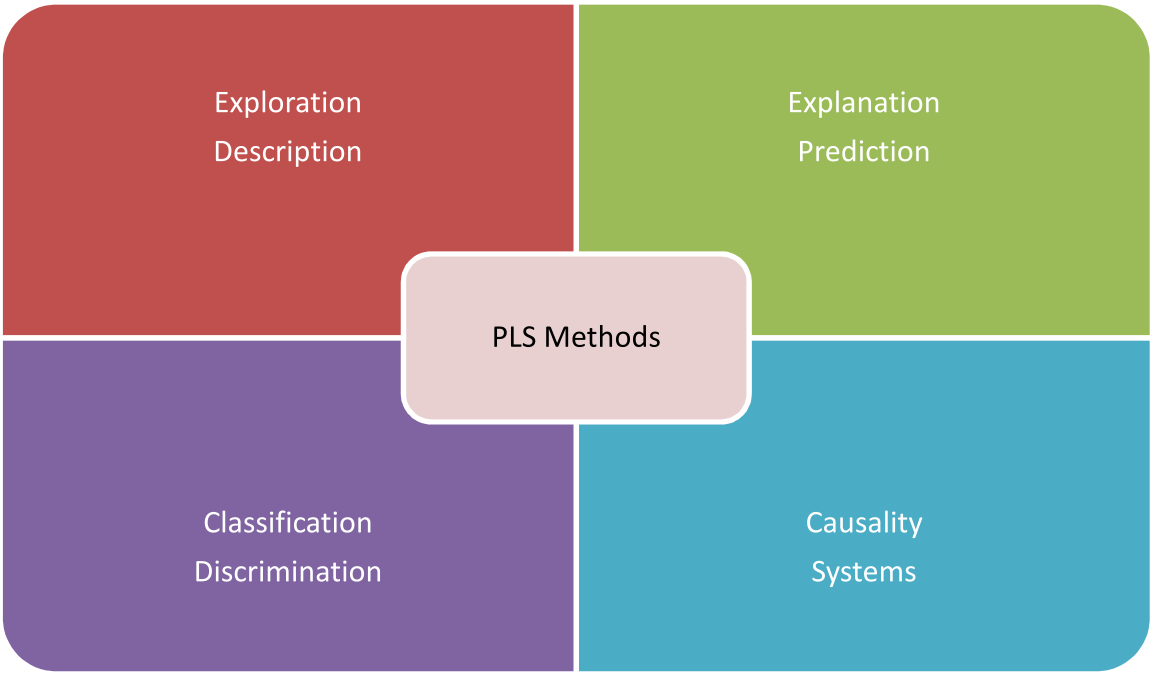


Figure 21: PLS Methods (Sanchez 2013a)

Partial Least Squares Path Modelling is a form of Structured Equational Modelling (SEM). SEM was first introduced by Jőreskog in 1973 and since then various other statistical analysis methodologies have emerged. According to Haenlein (2004), SEM allows for the simultaneous modelling of relationships between independent and dependant constructs. PLS PM is classified as variance based SEM which means it is based on the study of relationships between observed and unobserved (also called latent or intangible) variables. With PLS PM, the data analysis methodology consists of studying a block of observed variables representing the latent (intangible) variables.

Structural Equation Modelling and Path Modelling are used interchangeably but Path Modelling is preferred to show the distinction that PLS PM analyses multiple relationships between blocks of variables. Originally founded by Herman Wold in 1975, PLS was called Nonlinear Iterative Partial Least Squares (NIPALS) (Haenlein, Kaplan 2004) and looked at the variance of the dependant variables explained by the independent variables.

Overall, SEM allows the researcher the ability to construct unobservable or latent variables based on indicators (also referred to as items, manifest variables or observed measures) (Haenlein, Kaplan 2004). This helps to test a theoretical hypothesis against empirical data. Garthwaite (1994) also explains that PLS forms a relationship between the *Y* variables and explanatory variables (*X1…..Xm*) often called, latent variables or components.

Hulland (1999) states that the advances in causal modelling techniques have now made it possible to incorporate theory and measures simultaneously. However, in 1982, Fornell and Bookstein (1982) stated that LISREL could be poorly suited to small data samples as it produces inaccurate results that do not reflect a fair representation of the situation or environment. LISREL proposed by Jőreskog in 1975 is one of the most popular programs for SEM (Haenlein, Kaplan 2004). PLS was thus developed to address some of these limitations like improper solutions.

To summarise, PLS proposes that observed data is generated by a system or process driven by a number of latent (not directly observed or measured) variables (Rosipal, Krämer 2006). Furthermore, Rosipal and Kramer explain that PLS comprises of regression and classification tasks together with dimension reduction techniques and modelling tools.

PLS is essentially a method of statistical analysis that can help investigate the relationship of dependant and independent factors. Thus, this method was ideal in this context for identifying influential factors in the field of cyberterrorism. PLS could thus be used to study how unobserved factors could be caused by observed factors in order to assess the overall influence on the cyberterrorism life cycle development. The assessment of social factors using PLS PM is helpful in mathematically determining whether they have a strong influence on cyberterrorism. In general, the compilation of a PLS PM model has a number of steps which are shown in Figure 22.

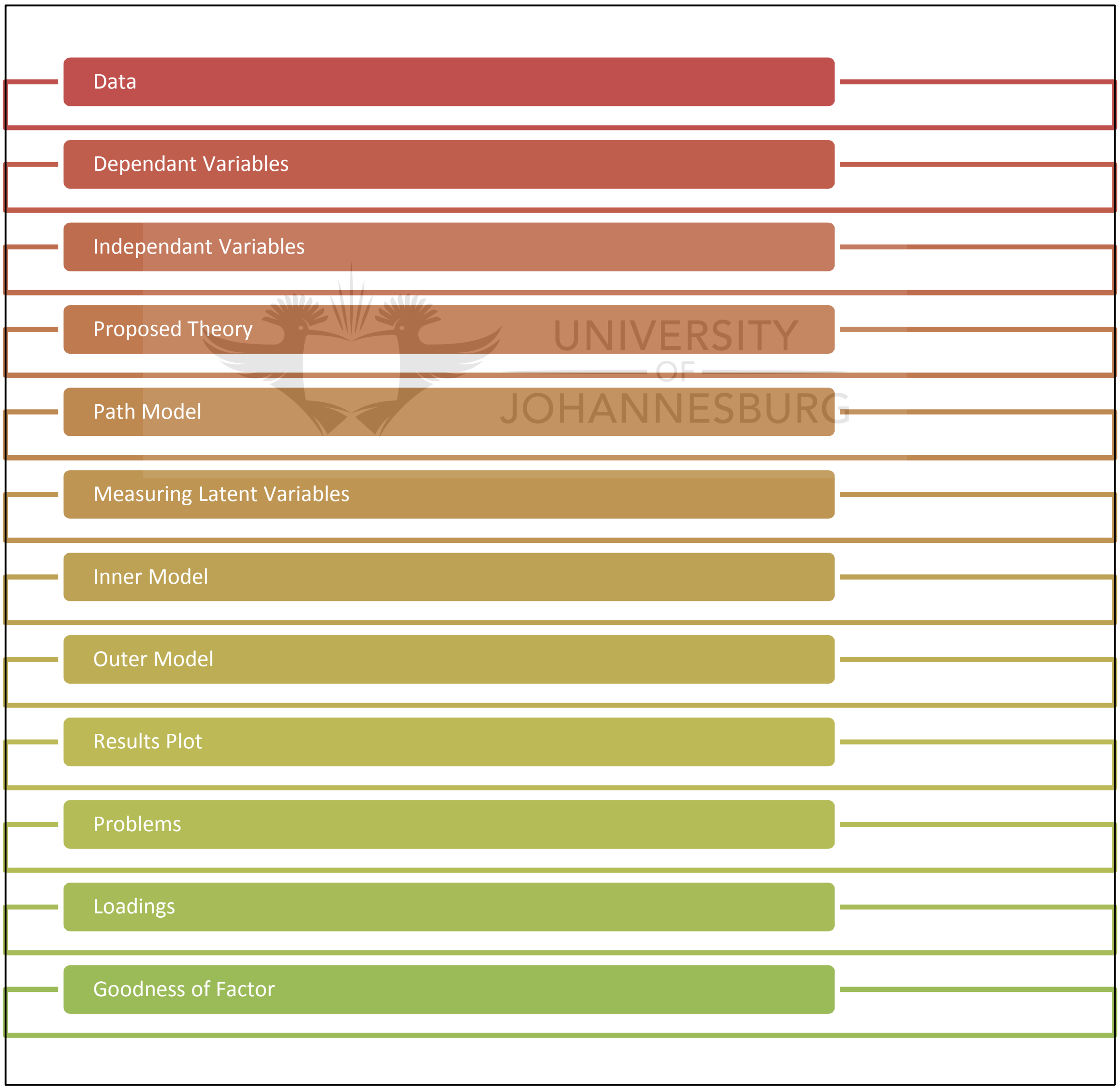


Figure 22: PLS PM Model Steps (Own Compilation)

Each of these steps will be explained in upcoming sections. The next section addresses the first step that focuses on the collection of the data that was used for the PLS PM modelling.

7.3 Survey Data

7.3.1 Context

A small data set was collected from a survey carried out together with researcher Dr Tom Holt from the University of Michigan. Dillman's Tailored Design Method was used to create the survey. Thereafter, volunteers were requested to complete the online survey. The large majority of respondents stemmed from academic institutions around the country. During security awareness training carried out at South African tertiary institutions, participants were requested to fill in the survey. In addition, fellow students and contacts of the author were also requested to complete the survey. Furthermore, lecturers at South African tertiary institutions aided with the collection process by distributing the survey to their students. A total of 286 responses were received from the South African survey with 60% being male and an average age of 27 (somewhat higher than average student age but the survey was also distributed to non-students). It should be noted that the data will have some limitations. The survey related to participants' willingness to engage in cyber attacks and thus the subjects themselves may not have been cyber deviant. This focus of the study is therefore influenced by the perception of cyber deviance by the participants. Furthermore, while the goal was to get a representative sample, the main subset of participants were university students.

The survey posed questions relating to their willingness to engage in online and offline attacks on critical infrastructure. (This study only examined the tendency for online cyber deviant behaviour, which is more closely aligned to cyberterrorism). While the scope of the survey covered a wide range of topics, the focus of this study was related to the influence of nationalism, antagonism, group inequality, group dynamics and technical outlooks. Therefore, the survey also contained a large number of questions that were grouped into categories. The answers from the survey questions formed the dependant and independent variables of the PLS PM model which are discussed next.

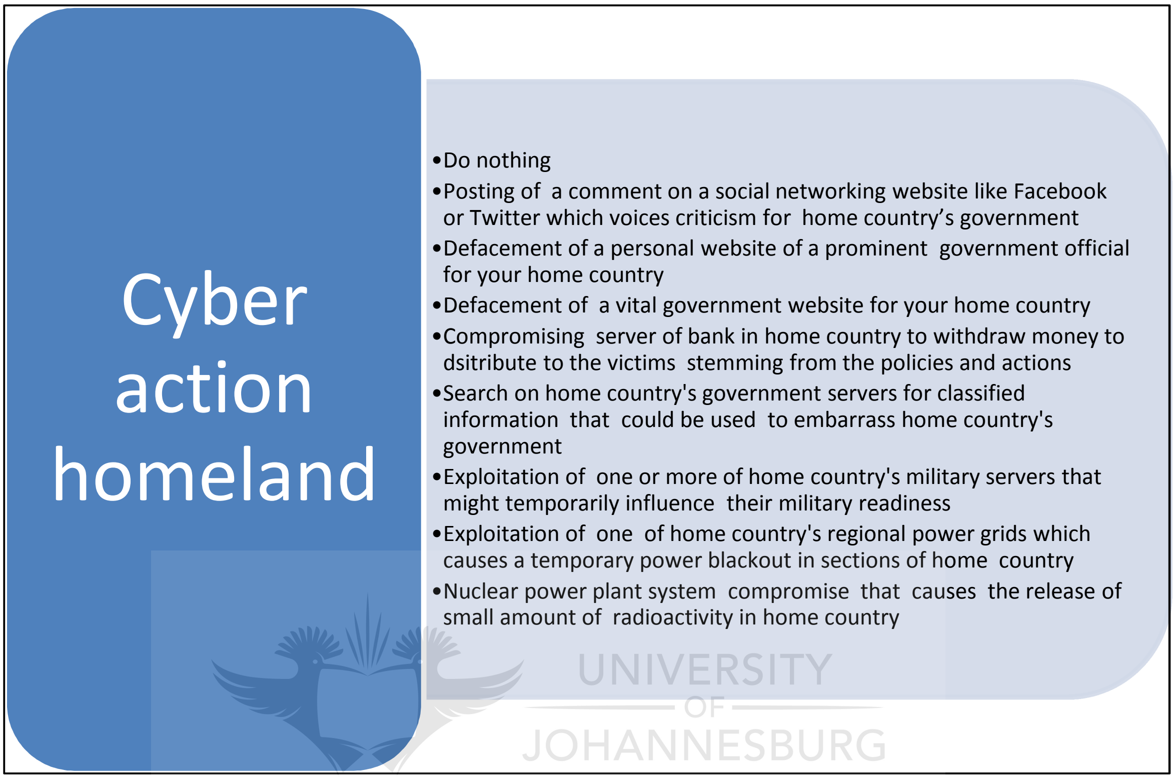
7.3.2 Dependant Variables

Figure 22 shows that after the data collection, the focus turns to the compilation of the dependant variables, which were based on the scenarios from the survey. The scenarios in the survey pertained to a nation state harming citizens of their home country and a hypothetical country called Bagaria. The two dependant variables in this study are the cyber actions against their homeland and cyber actions against Bagaria. As mentioned earlier in this chapter, PLS PM consists of studying the relationships between observed (dependant) variables and unobserved (latent) variables. Therefore, in order to compile the PLS PM model it is important to firstly establish the dependant variables.

For the first scenario (cyber actions against homeland), respondents were asked their reactions under the following conditions:

- Imagine that your home country has introduced policies and executed actions that negatively affect the country. The results of these policies and actions have created tremendous hardships for the people in the country.
- Hypothetically speaking, what type of actions would be deemed appropriate in the light of these policies and actions (the respondent could select as many of the proposed actions as they deemed fit).

Together with physical responses (which fall outside of the scope of this study), respondents were requested to indicate which online activities would be appropriate to take. Respondents were asked which of the actions in Figure 23 would be appropriate to take against their home country. As many actions as the respondent deemed necessary, could be chosen. In the scenario, it was assumed that the respondents had the skills necessary to execute the proposed actions.


Cyber action homeland

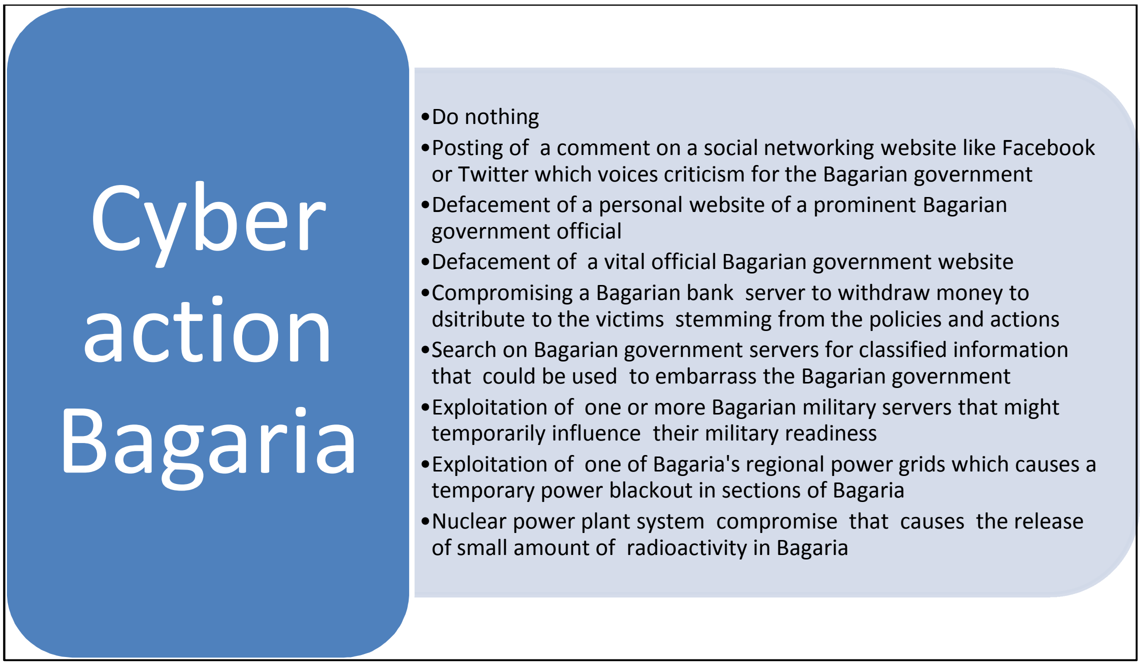
- Do nothing
- Posting of a comment on a social networking website like Facebook or Twitter which voices criticism for home country's government
- Defacement of a personal website of a prominent government official for your home country
- Defacement of a vital government website for your home country
- Compromising server of bank in home country to withdraw money to dsitribute to the victims stemming from the policies and actions
- Search on home country's government servers for classified information that could be used to embarrass home country's government
- Exploitation of one or more of home country's military servers that might temporarily influence their military readiness
- Exploitation of one of home country's regional power grids which causes a temporary power blackout in sections of home country
- Nuclear power plant system compromise that causes the release of small amount of radioactivity in home country

Figure 23: Cyber Actions Against Homeland (Dependant Variables)

For the second scenario (cyber actions against Bagaria), respondents were asked their reactions under the following conditions:

- Imagine that the country Bagaria has introduced policies and executed actions that negatively affect your home country. The results of these policies and actions have created tremendous hardships for the people in your home country.
- Hypothetically speaking, what type of actions would be deemed appropriate in light of these policies and actions (the respondent could select as many of the proposed actions as they deemed fit).

Once more respondents were requested to indicate which of the on-line activities shown in Figure 24 would to appropriate to take against Bagaria. As many actions as the respondent deemed necessary, could be chosen. In the scenario, it was assumed that the respondents had the skills necessary to carry out the actions.



- Do nothing
- Posting of a comment on a social networking website like Facebook or Twitter which voices criticism for the Bagarian government
- Defacement of a personal website of a prominent Bagarian government official
- Defacement of a vital official Bagarian government website
- Compromising a Bagarian bank server to withdraw money to dsitribute to the victims stemming from the policies and actions
- Search on Bagarian government servers for classified information that could be used to embarrass the Bagarian government
- Exploitation of one or more Bagarian military servers that might temporarily influence their military readiness
- Exploitation of one of Bagaria's regional power grids which causes a temporary power blackout in sections of Bagaria
- Nuclear power plant system compromise that causes the release of small amount of radioactivity in Bagaria

Figure 24: Cyber Actions Against Bagaria

Thus, the scenarios and proposed actions (in Figure 23 and Figure 24) posed to the respondents in the survey questions, formed the dependant variables. In the next section, the compilation of the independent variables will be discussed.

7.3.3 Independent Variables

Now that the dependant variables have been explained, the discussion moves on to the independent variables (see Figure 22). Once again, the independent variables are formed from the questions posed to the respondents in the survey. In this study, eight independent variables are proposed to influence willingness for cyber deviance. They are: *Patriotism, Group Inequality, Nationalism, Antagonism, Technicality and Piracy, Marital, Gender and Age.* Each of the independent variables will be discussed next.

7.3.3.1 Patriotism

According to Holt and Kilger (2012), patriotism refers to national identity and nationalism is the willingness to engage in attacks. Holt's findings are based on a study from Kosterman and Feshbach (1989) that hypothesised factors that would reflect these attitudes. According to Kosterman and Feshbach (1989), patriotism is feelings of attachment to the homeland and patriotism is the view that the home is superior and should be dominant. To judge a respondent's emotional connection to their homeland, respondents were asked to rate their agreement (1= strongly disagree; 4=strongly agree) with the following six statements (which have been summarised):

a) Proud to be a citizen of my home country

b) I am emotionally attached to my home country and get emotionally affected by actions that influence it

c) Even though I may not always agree with the government in my home country, I still have a strong commitment

d) I have great pride in my home country

e) I feel great, when I see my home country's flag displayed

f) An important part of my identity is being a citizen of my home country

7.3.3.2 Nationalism

The role of nationalism or the willingness to engage in attacks was assessed through a three-item scale adapted from Kosterman and Feshbach (1989). These items look at the viewpoint that a person believed that their home country is superior to other countries. Respondents were asked to rate their agreement with the following statements (which have been summarised):

a) Other countries should strive to make their government like my home country's government

b) In general, the more influence my home country has on other countries, the better it will be for them

c) Foreign nations may have good achievements, but my home country does things best of all

7.3.3.3 Group Equality

Another potential influential factor is the viewpoint of group equality. Six items were adapted from Sidanius and Pratto (2001). The (summarised) statements posed to respondents pertaining to group equality were:

a) If groups could be equal, this would be good

b) Group equality should be an ideal

c) All groups should be allowed an equal chance in life

d) Everyone should do what they can to equalise conditions for different groups

e) There would be less problems if we treated people more equally

f) Equalising incomes should be strived for

g) Society should not be dominated by any one group

7.3.3.4 Antagonism

In order to assess antagonism, five measures were adopted from Sidanius and Pratto (2001). These measures included the following (summarised) statements:

a) Some groups are merely inferior to other groups

b) If certain groups stayed in their place, there would be fewer problems

c) It is probably better that certain groups lie at the top and other groups fall down to the bottom

d) Inferior groups should remain in their place

e) In some cases, groups must be kept in their place

7.3.3.5 Technicality

Hackers possess certain levels of technical skills, and thus their technical capability could be a contributing factor to cyber deviant behaviour. To assess technological skills, three measures were used to gauge ease of use of ICT. These measures included more evolved technical skills and included:

a) Is capable of using an operating system like Unix or Linux

b) Is capable of using a standard computer programming or scripting language like C++, Perl, or Java

c) Can install an operating system like Unix or Linux

Reponses could range from 1 (not at all comfortable) to 5 (very comfortable).

7.3.3.6 Piracy

Respondents' involvement in cybercrime was assessed through measures relating to participation in piracy in the past twelve months. The two-item assessment queried how many times the respondents had engaged in the following two actions:

a) Consciously utilise, create, or provide another person a "pirated" copy of commercially sold computer software

b) Consciously utilise, create, or provide another person "pirated" media (music, movie or television series)

7.3.3.7 Marital Status, Gender and Age

Three demographic variables are also included in this analysis: gender, age and marital status. The measures were converted to a binary measure (female= 0, male= 1). Marital status options were single, married or divorced. The age categories were 20 and under, 21-30 and over 30.

7.3.3.8 Willingness to Engage in Cyber Attacks

An additive scale was use to study the relationship between political and social activism and the on-line environment. Figure 23 shows the nine actions that respondents were requested to select concerning on-line protest against their own homeland. However, two of the responses (Do nothing and Post a comment on a Social Networking Site) do not apply to being cyber deviant behaviour as this is a more passive form of protest. Therefore, the other seven actions reflect behaviour that is more malicious and an active form of resistance. Thus, the other seven actions were combined to create a binary measure for cyber actions against their homeland and Bagaria.

Table 6 shows the reported willingness of the respondents to engage in cyber actions. The willingness to engage in on-line protest actions was 67% against their own homeland and Bagaria. The most common act that users responded to was the posting of messages on Facebook and social media for both the homeland and Bagarian scenarios - interestingly both correlated to 54% of respondents.

Table 6: Willingness to Engage in Cyber Actions (Own Compilation)

Response	**Homeland (n=286)**	**Bagaria (n=286)**
Posting of a comment on a social networking website like Facebook or Twitter with criticism	152 (53,14%)	153 (53,5%)
Defacement of the personal website of an prominent government official	32 (11,9%)	41(14,34%)

Response	Homeland (n=286)	Bagaria (n=286)
Defacement of a vital government website	45 (15,73%)	39(13,63%)
Compromising the server of a bank server to withdraw money to distribute to the victims of their policies and action	24 (8,39%)	26 (9,09%)
Search government servers for classified documents that could be used to embarrass government	41 (14,34%)	45(15,73%)
Exploitation of one or more of the military servers that might temporarily influence their military readiness	19 (6,64%)	25 (8,74%)
Exploitation of one of the regional power grids which causes temporary power blackout in parts of the country	16 (5,59 %)	17 (5,94%)
Nuclear power plant system compromise that causes a small release of radioactivity	9 (3,15%)	11 (3,84%)

7.4 PLS PM Implementation

The PLS PM Implementation was carried out with the guidance of the book PLS Path Modelling with R (Sanchez 2013b). The theoretical sections provided in this section thus stem from Sanchez (2013b). The design of the data inputs for the PLS PM model is also based on the work by Holt and Kilger (2012). Holt and Kilger carried out regression analysis on their dataset whereas in this study, the author focussed on PLS PM techniques.

In order to set up the PLS PM models the free open source software R was used. R is a statistical data analysis program and unlike many other statistical programs, it is capable of producing graphical results. Within R, the package ***plspm*** provides the functionality for carrying out PLS PM analysis and computing.

Typically, with structural models, some type of theory needs to be proposed in order to build the model (see Figure 22). In this case, the proposed theory was:

The stronger the tendency towards ***Patriotism, Group Inequality, Nationalism, Antagonism, Technicality and Piracy*** *as well as a stronger disposition in terms of* ***Marriage, Gender and Age****, the higher the* ***Willingness t****o be* ***Cyber Deviant.***

The theory can also be expressed in a more abstract format using functional notation like:

```
Will_Cyber_Deviant=  f(Patriotism,  Group_Inequality  Nationalism,  Antagonism,
Technical, Piracy, Gender_Marriage, Age)
```

This theory can be further expressed in a linear function using the following equation:

```
Will_Cyber_Deviant=  Patriotism  +  Group_Inequality  +  Nationalism  +  Antagonism
Technical + Piracy + Gender_Marriage + Age
```

Haenlein and Kaplan (2004) explain that the research model representing the theory can be shown graphically by a path diagram (see Figure 22), hence the name PLS path modelling which shows how the various elements relate to each other. Sanchez (2013b) describes PLS PM as a flow chart where the process flows in one direction with the goal of quantifying the relationships between the variables. Interestingly, the connected variables are dependent on the combination of the set of other variables. The graphical models help to represent the concepts proposed in a visually appealing format. In this case, Figure 25 shows the relation of Will_Cyber_Deviant based on the concepts of patriotism, group inequality, antagonism, nationalism, technical skill, piracy, age, gender and marital status. The overall goal of this chapter is to determine whether the variables depicted in Figure 25 have a strong influence on the willingness to engage in cyber deviance (cyberterrorist behaviour).

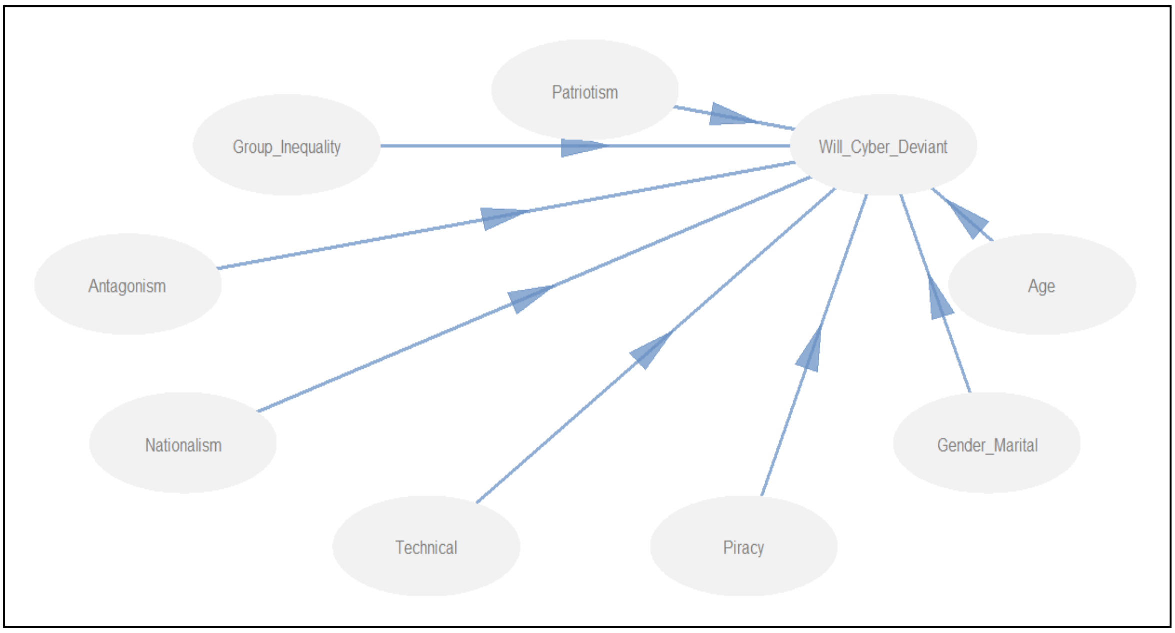


Figure 25: Path Model for Willingness for Cyber Deviation (Own Compilation)

7.4.1 Latent Variables Deeper Analysis

Section 7.3.3 introduced the independent (latent) variables. In this section, the latent variables are explored in more detail. One of the assumptions in PLS PM is that the latent variables can be measured using *manifest variables*. The variables can be measured in two ways:

- Effects reflected on their indicators (observed measures). This is known as the *reflective* way and is seen as being *caused* by the latent variables.
- Different indicators that reflect on the indicators. The second case is called the *formative* way in that the latent construct is *formed* by its indicators

Mainly, the two ways differ in their causal-effect relationships. Figure 26 shows the formative and reflective approaches for a simple example of a soccer attack. This example demonstrates a practical application of the formative and reflective approaches. In order to measure the quality of the Attack, the following questions should be asked:

- What will reflect the attack?
- What will affect the attack?

In the example shown in Figure 26, the formative indicators like the hours trained look at what contributes to the quality of an attack. The reflective indicators like the shots on goal measure the attack effects.

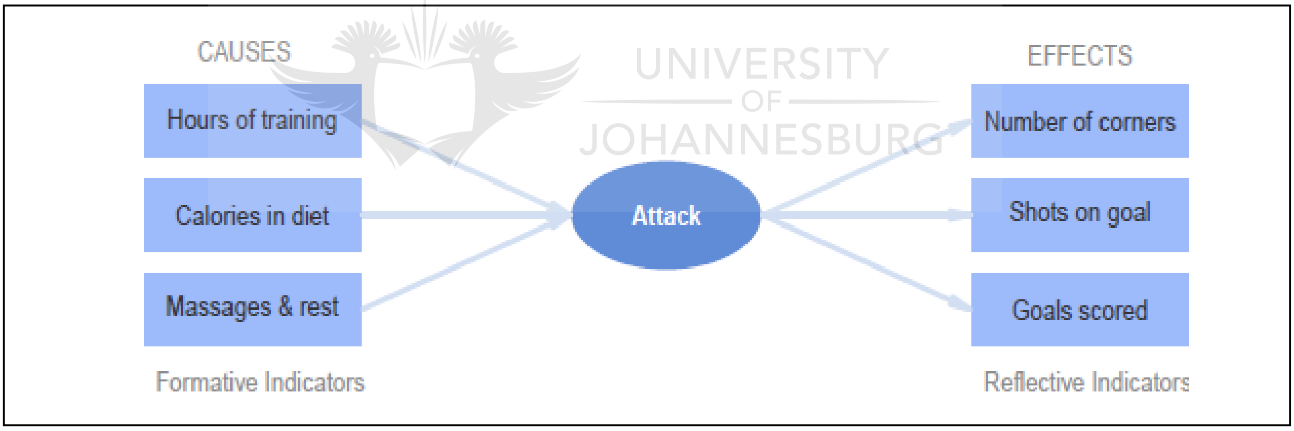


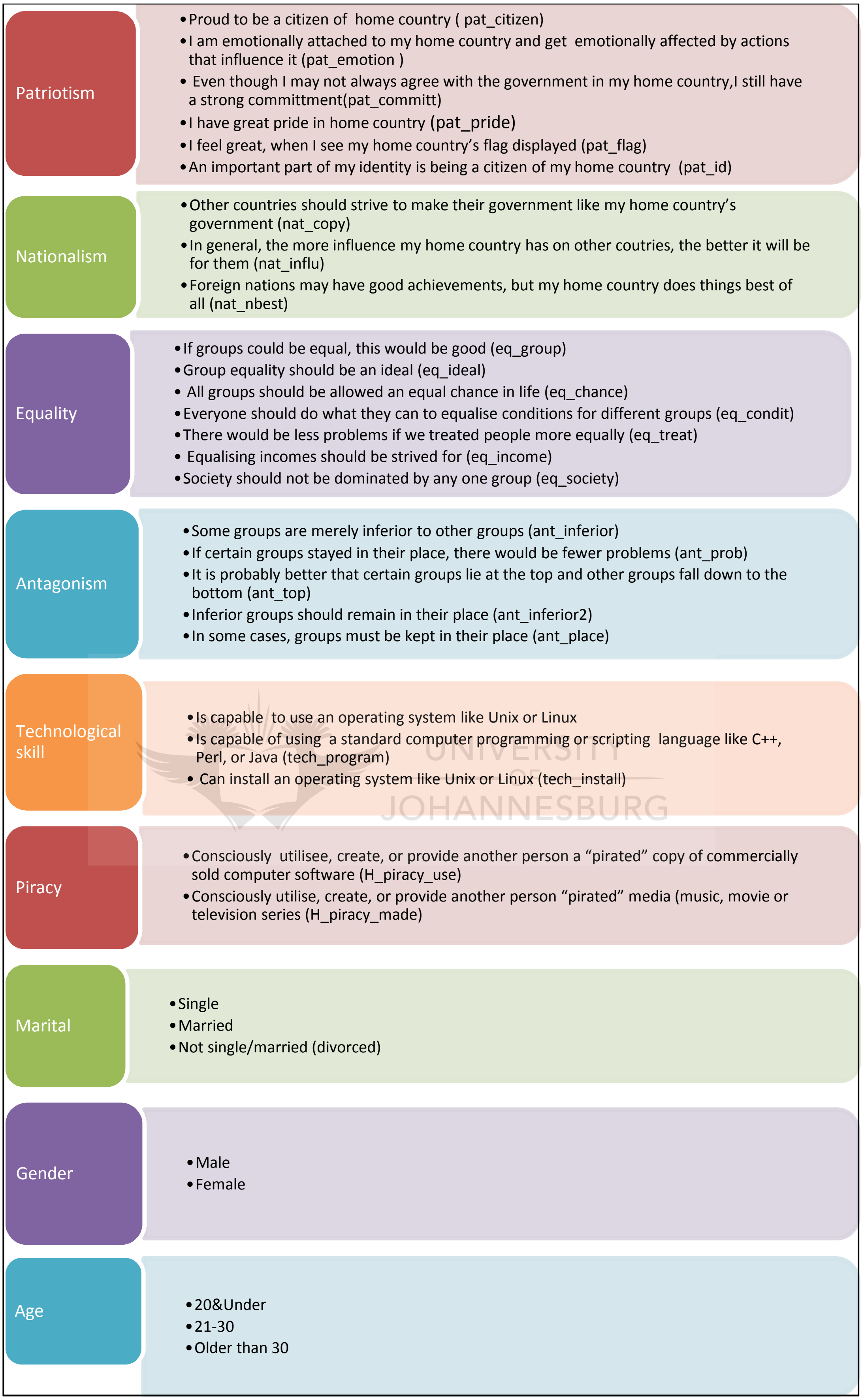
Figure 26: Formative and Reflective Relationships (Sanchez 2013b)

The reflective indicators measure the effects of the attack. In this example, the effects that can be measured are the number of corners, shots on goal and goals scored. On the other hand, the formative indicators cause the attack. For example, the number of hours spent in training, the diet calories, massages and rest can all cause a soccer attack.

7.4.2 Measuring Latent Variables

The reader should recall that in order to create a PLS PM model, the dependant and latent (independent) variables should be set up. The previous section discussed the dependant variables and introduced the latent variables. Both the dependent and latent variables are based on the questions posed to the respondents in the survey. The previous sections indicated which survey questions are associated with each variable. In this section, the latent variables are discussed in more detail (see Figure 22).

For the PLS PM model there are nine latent variables- *Patriotism, Group_Inequality Nationalism, Antagonism, Technical, Piracy, Gender_Marriage and Will_Cyber_Deviant.* The next step is to establish a set of indicators for each of these variables. Figure 27 shows the indicators for each latent variable. Each of the indicators corresponds to the survey questions that were posed to respondents. The abbreviated word at the end of each statement in Figure 27 will be used in the data analysis in the next section. Each abbreviation will represent the longer statement in the data analysis table (Figure 30).



Patriotism

- Proud to be a citizen of home country (pat_citizen)
- I am emotionally attached to my home country and get emotionally affected by actions that influence it (pat_emotion)
- Even though I may not always agree with the government in my home country,I still have a strong committment(pat_committ)
- I have great pride in home country (pat_pride)
- I feel great, when I see my home country's flag displayed (pat_flag)
- An important part of my identity is being a citizen of my home country (pat_id)

Nationalism

- Other countries should strive to make their government like my home country's government (nat_copy)
- In general, the more influence my home country has on other coutries, the better it will be for them (nat_influ)
- Foreign nations may have good achievements, but my home country does things best of all (nat_nbest)

Equality

- If groups could be equal, this would be good (eq_group)
- Group equality should be an ideal (eq_ideal)
- All groups should be allowed an equal chance in life (eq_chance)
- Everyone should do what they can to equalise conditions for different groups (eq_condit)
- There would be less problems if we treated people more equally (eq_treat)
- Equalising incomes should be strived for (eq_income)
- Society should not be dominated by any one group (eq_society)

Antagonism

- Some groups are merely inferior to other groups (ant_inferior)
- If certain groups stayed in their place, there would be fewer problems (ant_prob)
- It is probably better that certain groups lie at the top and other groups fall down to the bottom (ant_top)
- Inferior groups should remain in their place (ant_inferior2)
- In some cases, groups must be kept in their place (ant_place)

Technological skill

- Is capable to use an operating system like Unix or Linux
- Is capable of using a standard computer programming or scripting language like C++, Perl, or Java (tech_program)
- Can install an operating system like Unix or Linux (tech_install)

Piracy

- Consciously utilisee, create, or provide another person a "pirated" copy of commercially sold computer software (H_piracy_use)
- Consciously utilise, create, or provide another person "pirated" media (music, movie or television series (H_piracy_made)

Marital

- Single
- Married
- Not single/married (divorced)

Gender

- Male
- Female

Age

- 20&Under
- 21-30
- Older than 30

Figure 27: Latent Variables' Indicators (Own Compilation)

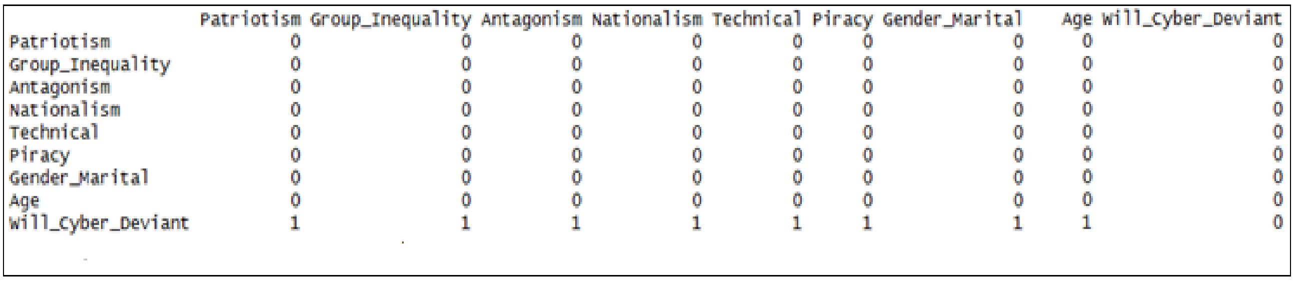
Figure 25 shows the simple path diagram depicting the relationships between the latent variables. To establish the full path model two sub models are constructed first. Two sets of linear equations are formally defined: the inner model and the outer model. In the inner model, the relationships between the unobserved or latent variables are specified and in the outer model, the relationships between a latent variable and its observed or manifest variables are established (Henseler, Ringle & Sinkovics 2009). According to Sanchez (2013b), latent variables are also known as constructs, composites, hypothetical variables, theoretical concepts, intangibles and factors. These types of variables are typical in social sciences and behavioural sciences (e.g., psychology, sociology, economy). Cyberterrorism spans these fields as well and thus, these unobserved entities could be found in cyberterrorism. In order to create a PLS PM model in R, several commands need to be run. The next few sections contain the commands and explanations of how the Willingness for Cyber Deviance PLS PM model were created. The inner model is discussed next.

7.4.2.1 Inner Model

Now that the dependant and independent variables have been specified and measured, the discussion moves on the compilation of the inner model (see Figure 22). The inner or structural model encapsulates the relationships between the latent variables. In R, it can be captured as a matrix. The matrix must be square (same number of rows and columns) and is known as a lower triangular Boolean matrix. The elements in the diagonal and above it must be zeroes and the elements below the diagonal can be zeroes or ones. The inner matrix is defined as follows:

```
Patriotism = c(0,0,0,0,0,0,0,0,0)
Group_Inequality= c(0,0,0,0,0,0,0,0,0)
Antagonism= c(0,0,0,0,0,0,0,0,0)
Nationalism= c(0,0,0,0,0,0,0,0,0)
Technical= c(0,0,0,0,0,0,0,0,0)
Piracy= c(0,0,0,0,0,0,0,0,0)
Gender_Marital = c(0,0,0,0,0,0,0,0,0)
Age= c(0,0,0,0,0,0,0,0,0)
Will_Cyber_Deviant= c(1,1,1,1,1,1,1,1,0)
#matrix (by row binding)
terror_inner= rbind (Patriotism, Group_Inequality, Antagonism, Nationalism,
Technical, Piracy,Gender_Marital,Age, Will_Cyber_Deviant)
#add column names
colnames (terror_inner)= rownames (terror_inner)
```

This creates three vectors that will be rows of the argument inner_matrix. The matrix is read by looking at how the columns affect the rows. A number one in the cell *i,j* (*i-th* row,*j-th* row) indicates that column *j* affects row *i*. The zeroes in the diagonal indicate that a latent variable cannot affect itself. The inner model matrix is shown in Figure 28.



```
                   Patriotism Group_Inequality Antagonism Nationalism Technical Piracy Gender_Marital   Age Will_Cyber_Deviant
Patriotism                  0                0          0           0         0      0              0     0                  0
Group_Inequality            0                0          0           0         0      0              0     0                  0
Antagonism                  0                0          0           0         0      0              0     0                  0
Nationalism                 0                0          0           0         0      0              0     0                  0
Technical                   0                0          0           0         0      0              0     0                  0
Piracy                      0                0          0           0         0      0              0     0                  0
Gender_Marital              0                0          0           0         0      0              0     0                  0
Age                         0                0          0           0         0      0              0     0                  0
Will_Cyber_Deviant          1                1          1           1         1      1              1     1                  0
```

Figure 28: Inner Model Matrix (Own Compilation)

7.4.2.2 Outer Model

The inner model has been completed and so the discussion turns to the outer model (See Figure 22). The outer model is defined using a list and a vector, which indicates what variables of the data are associated with what latent variables. Using the example,

```
#define list of indicators:what variables are associated with
#what latent variables
terror_outer=  list(1:6,  10:16,  17:21,7:9,  40:42,  43:44,  c(45,46,47,48),
c(49,50,51), 52:53)
```

The list contains nine elements, one for each latent variable - *Patriotism, Group_Inequality Nationalism, Antagonism, Technical, Piracy, Gender_Marriage and Will_Cyber_Deviant.* The number ranges indicate the column numbers from the data set (Excel spreadsheet containing the data). Thus, the first latent variable *Patriotism* is linked to the first six columns from the data set, the second latent variable *Group_Inequality* is linked to columns 10 until 16 and so forth for the rest of the latent variables. (The columns numbers may not be chronological due to the data being captured from different questions that appear in a different order in the survey).

The latent variables are measured in a reflective way (Section 7.4.1 discusses the reflective way), which can be explicitly defined using a vector of modes.

```
#modes(reflective blocks)
terror_modes= rep("A",9)
#Running PLS PM
#Now that the basic components of the model have been defined, the PLS path
#model can be run.
#apply plspm
terror_pls=plspm(terrorism, terror_inner, terror_outer, terror_modes)
terror_pls
```

7.4.3 Plotting Results

Now that the variables and inner and outer models have been established, the results can be plotted (see Figure 22).

7.4.3.1 Reflective Indicators

Formative blocks can be rather straightforward to interpret, whereas reflective may not be. Reflective indicators are based on Test Theory developed in psychology or more specifically in psychometrics. Psychometrics is commonly known as the design of tests with many tricky questions, multiple choices and random exercises. The tests are filled with vocabulary words to check for reliability, validity, consistency and accuracy, which are then used extensively in Structural Equation Modelling. It is therefore important to understand the key ideas behind the reflective measurement model. Reflective indicators need to have strong ties (strong mutual association) and get along with its latent variable (loyal to its construct). This will help prevent traitor indicators (higher loading on another construct). In simple terms, a few variables measuring an aspect of some component (the same latent variable), should roughly point in the same direction. This is what uni-dimensionability means.

7.4.3.2 Problem

The results of the inner model are displayed in Figure 29.

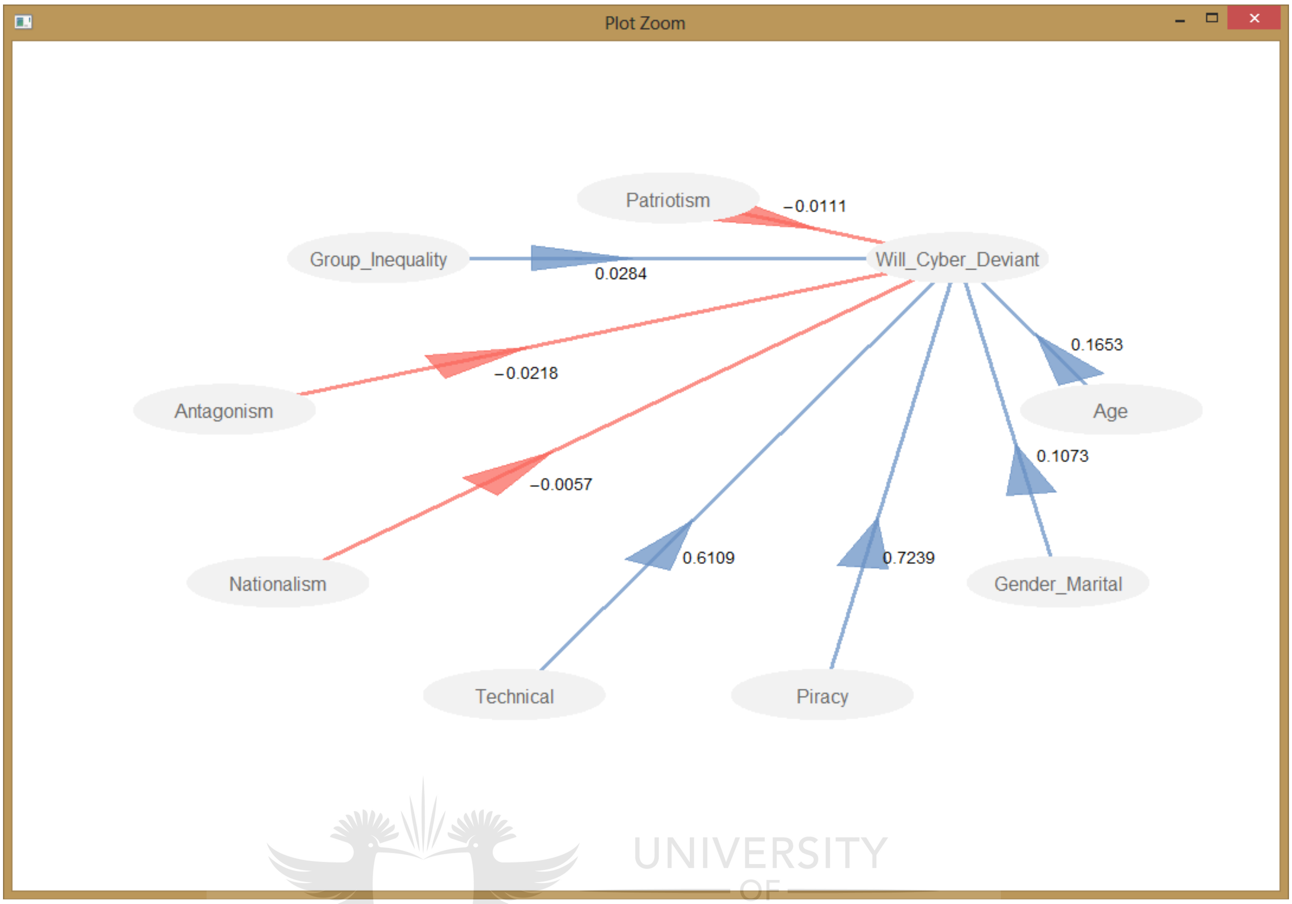


Figure 29: Inner PLS PM Model (Own Compilation)

Figure 29 shows that there are issues with *Patriotism, Antagonism* and *Nationalism* as they have negative values. Furthermore, a few more issues arise in the outer model. In this section, identified problems are addressed (see Figure 22). The outer model is checked in the following way (called the loadings):

```
#plot the loadings
plot(terror_pls, what="loadings")
```

Figure 30 shows the results of the loadings diagrammatically. As mentioned previously, the abbreviation pat_id correlates to the indicator and survey question “An important part of my identity is being a citizen of my home country”. Likewise, the abbreviation pat-flag represents the indicator and survey question “I feel great, when I see my home country’s flag displayed”. In the same way, the other abbreviations used in Figure 29 correlate to their associated indicator and survey question.

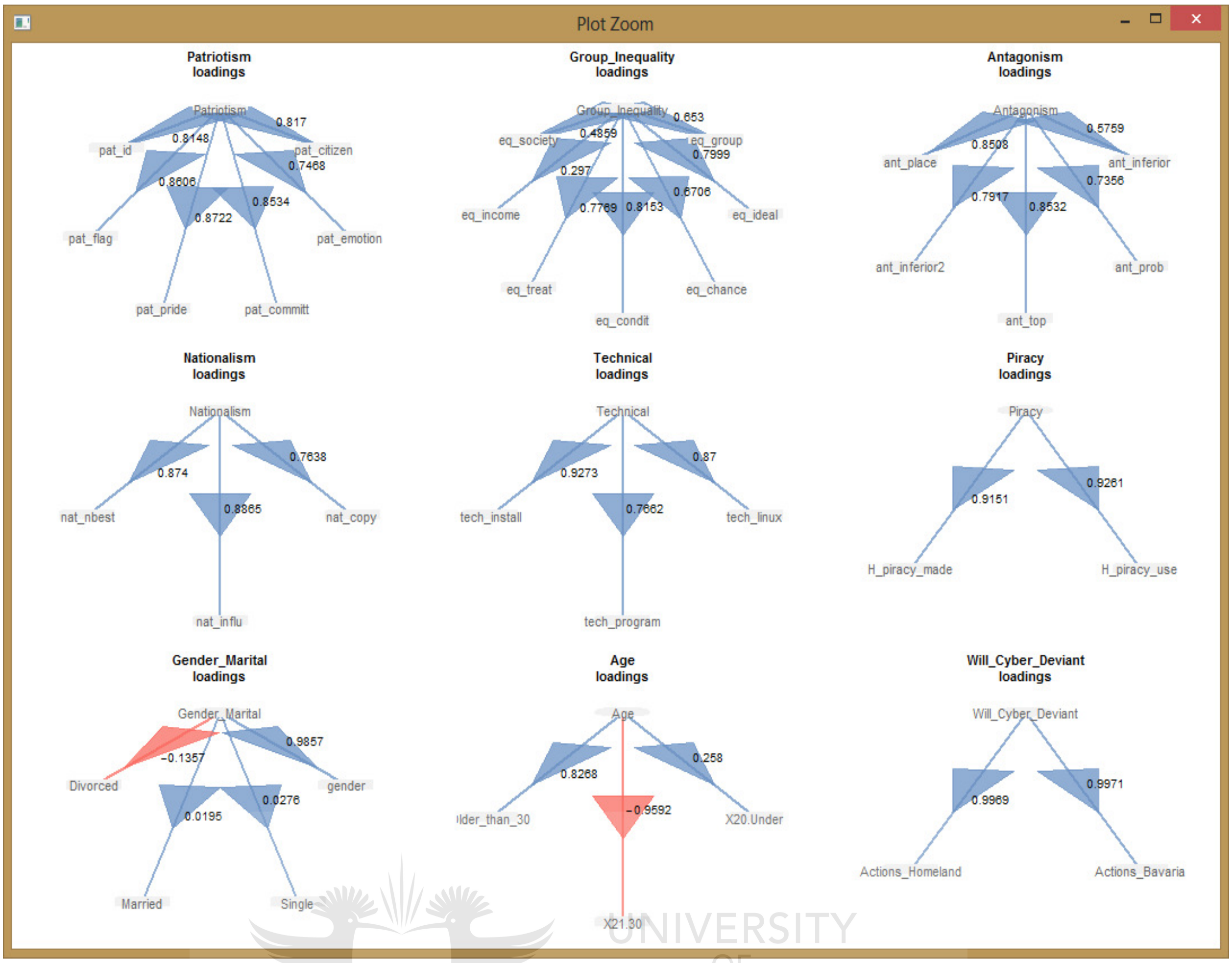


Figure 30: PLS PM Loadings (Own Compilation)

The loadings plot (Figure 30) shows that *Divorced* in the variable *Gender_Maritial* and *X21-30* in the variable *Age* have negative arrows, which indicate that they have negative loadings. As explained in the previous section, indicators measuring an aspect of a variable should roughly point in the same direction as an indication of unidimensionality. In this case (see Figure 30), all the indicators of a variable do not correlate and therefore a problem has arisen.

This anomaly of mixed signs of indicators is rather common and can be addressed by making changes to the data columns. There are four options in the survey questions (strongly disagree, disagree, agree, strongly agree) which correlate to the values 1, 2, 3 and 4 in the dataset. To reverse the data, if a user answered 1 and the answer should be 4 then, subtract 1 from 5 to get an answer of 4. Conversely, if the original value was 4, it will now be 1. In this way, the number 5 is used to subtract the original values each time. Thus, the data was corrected using the following commands in R:

```
# Modify patriotism, nationalism and antagonism
#modify negative age and marital

#Patriotism
terrorism$unpat_citizen = 5- terrorism$pat_citizen
terrorism$unpat_emotion = 5- terrorism$pat_emotion
terrorism$unpat_committ = 5- terrorism$pat_committ
terrorism$unpat_pride = 5- terrorism$pat_pride
terrorism$unpat_flad = 5- terrorism$pat_flag
```

```
terrorism$unpat_id = 5- terrorism$pat_id

#Nationalism
terrorism$unNat_copy = 5- terrorism$nat_copy
terrorism$unNat_influ = 5- terrorism$nat_influ
terrorism$unNat_best = 5- terrorism$nat_nbest

#Antagonism
terrorism$unAnt_inferior = 5- terrorism$ant_inferior
terrorism$unAnt_prob = 5- terrorism$ant_prob
terrorism$unAnt_top = 5- terrorism$ant_top
terrorism$unAnt_inferior2 = 5- terrorism$ant_inferior2
terrorism$unAnt_place = 5- terrorism$ant_place

#Divorced and X21.30
terrorism$over20=1-terrorism$X21.30
terrorism$not_marriedNorSingle=1-terrorism$Divorced
```

The data has now been updated and the outer model lists must be modified with the new column indices. The following commands were executed in R to update the loadings:

```
terror_outer= list(54:59, 10:16, 63:67,60:62, 40:42, 43:44, c(45,69,46,47),
c(49,51,68), 52:53)
#plot the loadings
plot(terror_pls, what="loadings")
```

Figure 31 shows the updated loadings, which now contain the modified indicators.

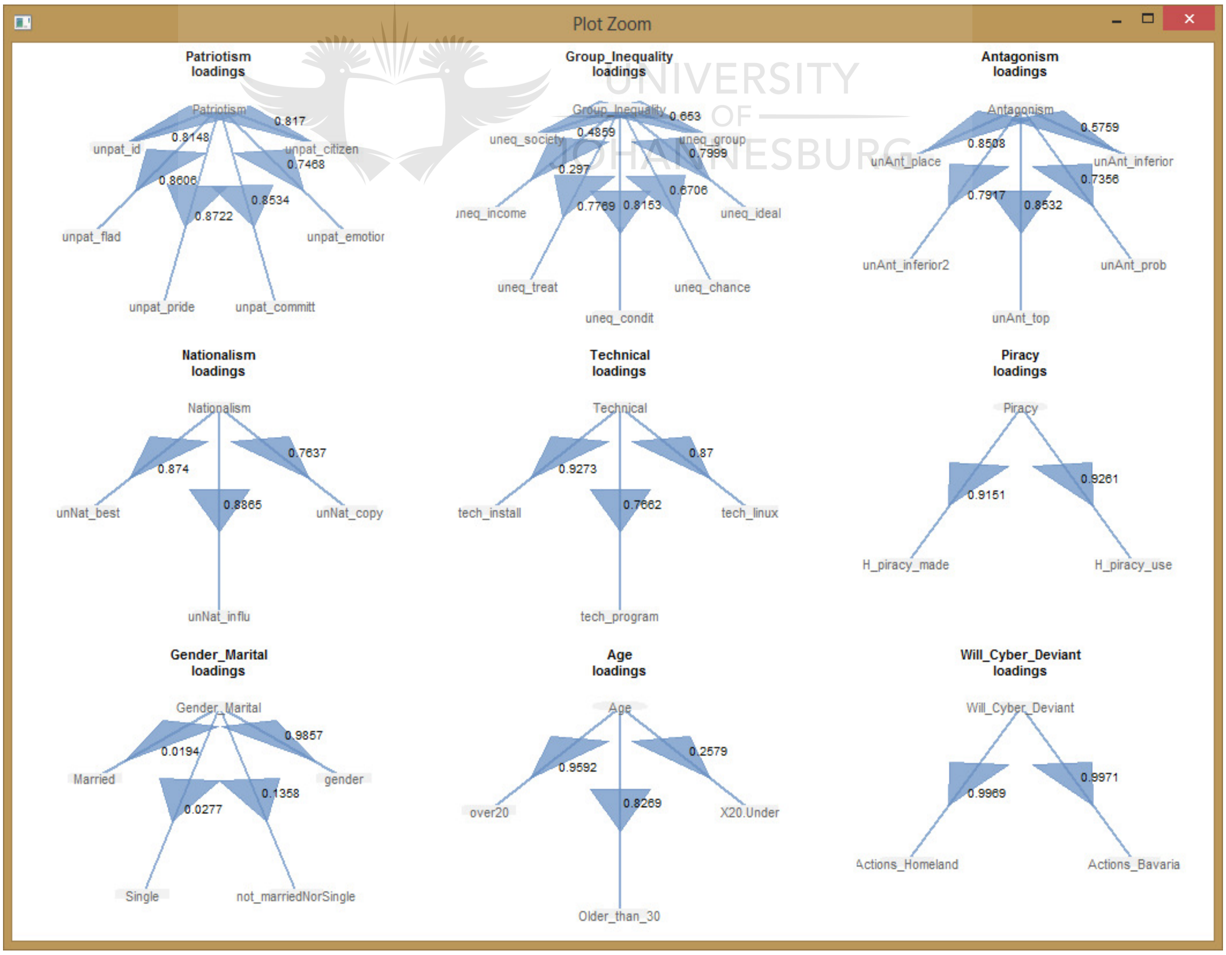


Figure 31: Updated Loadings (Own Compilation)

The outstanding issues have been addressed in the PLS PM Model and the inner model can be redrawn. The updated inner model loadings are shown in Figure 32.

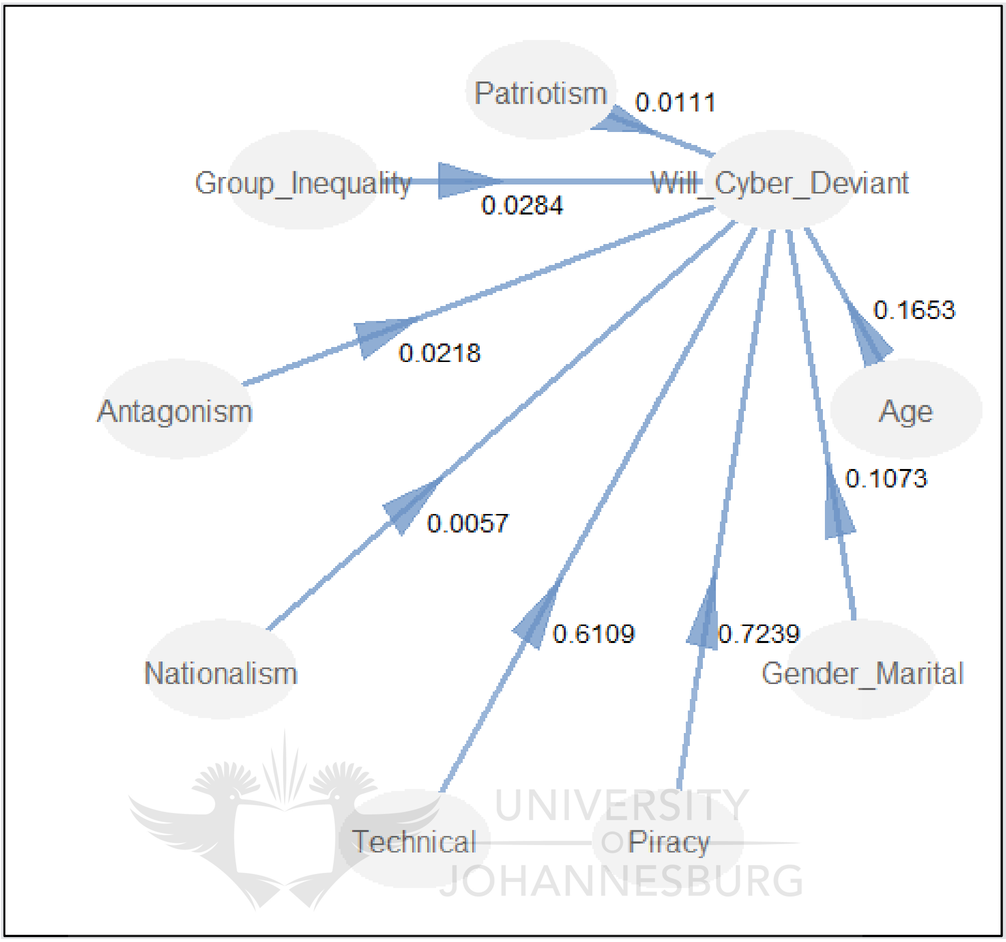


Figure 32: Updated Inner Model (Own Compilation)

The updated data now indicates the following effects on Willingness_Cyber_Deviance:

```
> #inner model written summary of image
> terror_pls$inner.mod
$Will_Cyber_Deviant
                 concept  value
1                     R2 0.9555
2              Intercept 0.0000
3        path_Patriotism 0.0111
4  path_Group_Inequality 0.0284
5        path_Antagonism 0.0218
6       path_Nationalism 0.0057
7         path_Technical 0.6109
8            path_Piracy 0.7239
9    path_Gender_Marital 0.1073
10              path_Age 0.1653
```

These values can be interpreted as follows:

- **Technical skills** and the **willingness to commit piracy** strongly influence people’s willingness to engage in cyber deviance

- People who are more likely to commit cyberterrorism can sway to a certain **gender, age group and marital status**
- **Patriotism, Nationalism, Antagonism and Group Inequality did not** strongly influence people's willingness to engage in cyber deviance

7.4.3.3 GOF

The Goodness of Factor (GoF) index accounts for the quality of both the measurement and structural models. It is more applicable to reflective indicators as is calculated in the following way:

GoF is considered a global criterion that can be used to assess the performance of the inner and outer models. Acceptable values in the PLS PM community are **GoF >0.7**. The GoF of the PLS PM model was calculated as follows:

```
#goodness of fit index - gof
terror_pls$gof

0.7546555
```

The results of the GOF index in this model is a value of **0.755** which is an acceptable level of data quality.

7.5 Conclusion

This chapter focussed on using PLS PM to identify social factors that may influence cyberterrorism. PLS PM is a statistical analysis methodology. It is essentially a method of statistical analysis that can help investigate the relationship of dependant and independent factors. The use of PLS PM requires data to analyse. A survey was carried out in order to determine civilians' willingness to engage in on-line attacks. The PLS PM model was then set up to determine the influence of a few social factors including: *Patriotism, Group Inequality, Nationalism, Antagonism, Technicality and Piracy, Marital, Gender and Age.* The results of the analysis showed that Nationalism, Patriotism, Antagonism and Group Equality did not a play a strong role in influencing cyber deviance.

The main drivers derived from this chapter that will be captured in the CLC model are summarised as follows:

- **Technical skills and the willingness to commit piracy** strongly influence people's willingness to engage in cyber deviance (Section 7.4.3.2).
- People who more likely to commit cyberterrorism can sway to a certain **gender, age group and marital status** (Section 7.4.3.2).

Overall, PLS PM is a useful technique for carrying out statistical analysis. Other data sets can also be analysed using PLS PM to reveal further influential factors in cyberterrorism.

Now that the introductory concepts, background information and some of the main driving forces have been discussed, the discussion moves on to a mapping of cyberterrorism to a pre-existing model- the Observe, Orient, Decide and Act Loop. This model has various phases and describes a process of execution. Therefore, the OODA loop was deemed an appropriate model in order to create the basis of the CLC model as the phased style of execution could also be appled to cyberterrorism. The next chapter therefore describes the mapping of cyberterrorism to the OODA loop.

Part 3 Development of Cyberterrorism

This study, CLC- Cyberterrorism Life Cycle model is made up of four parts- originally shown in Figure 2. Figure 33 shows the status of the CLC model development study. Part 1 and 2 have been completed.

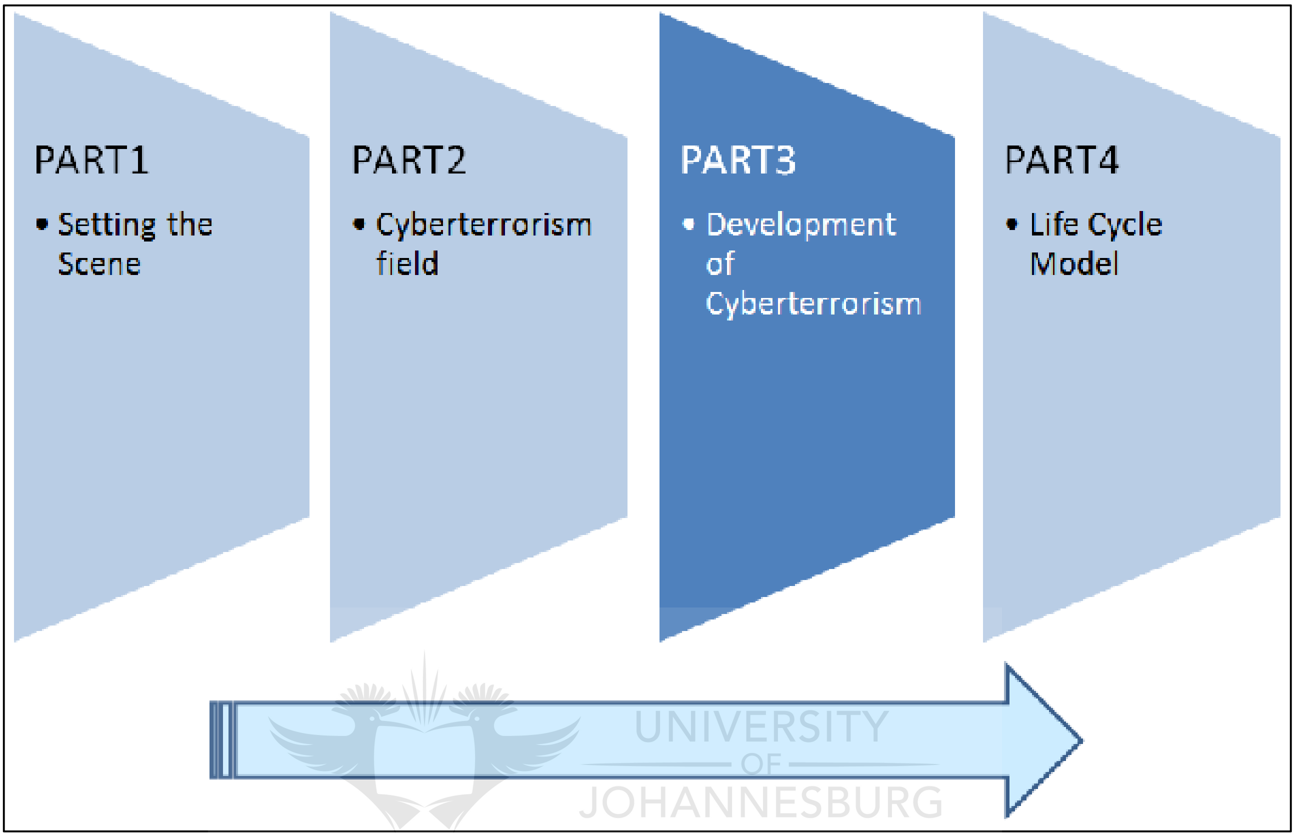
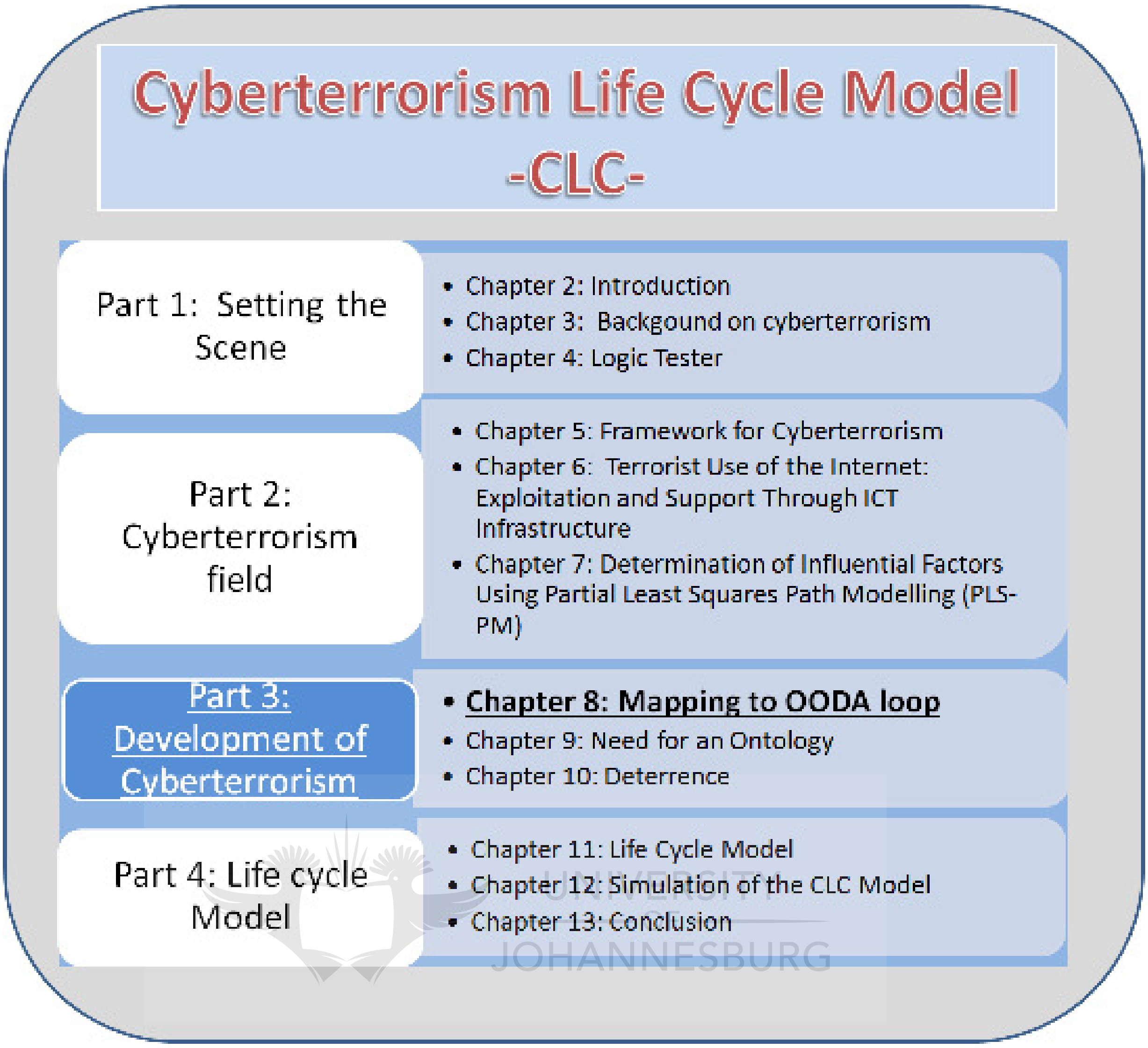


Figure 33: Part 3 of CLC Model Development (Own Compilation)

Part 3, Development of Cyberterrorism looks in detail at the growth of cyberterrorism, as well as deterrence methods. It consists of three chapters.

- Chapter 8: High-level Mapping of Cyberterrorism to the Observe-Orient-Decide-Act (OODA) Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence of Cyberterrorism



Cyberterrorism Life Cycle Model -CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS-PM)

Part 3: Development of Cyberterrorism

- **Chapter 8: Mapping to OODA loop**
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

8 High-level Mapping of Cyberterrorism to the Observe-Orient-Decide-Act (OODA) Loop

> *"Everybody knows that their iPhone can do, everybody knows what their computer can do, but I think there are too few people out there who understand the potential for the kind of attack that could cripple this country. It is the kind of capability that can basically take down a power grid, take down a water system, take down a transportation system, take down a financial system. We are in a world in which countries are developing the capability to engage in the kind of attacks that can virtually paralyze a country."*
>
> *- Leon Panetta US Defence Secretary*

Part 1 and Part 2 provided the background to the field of cyberterrorism by defining the field and introducing various influential factors. Another objective of this study is to represent the various influential factors. Part 3 addresses this objective, by representing these influential factors in a model that aims to show their dynamic interaction.

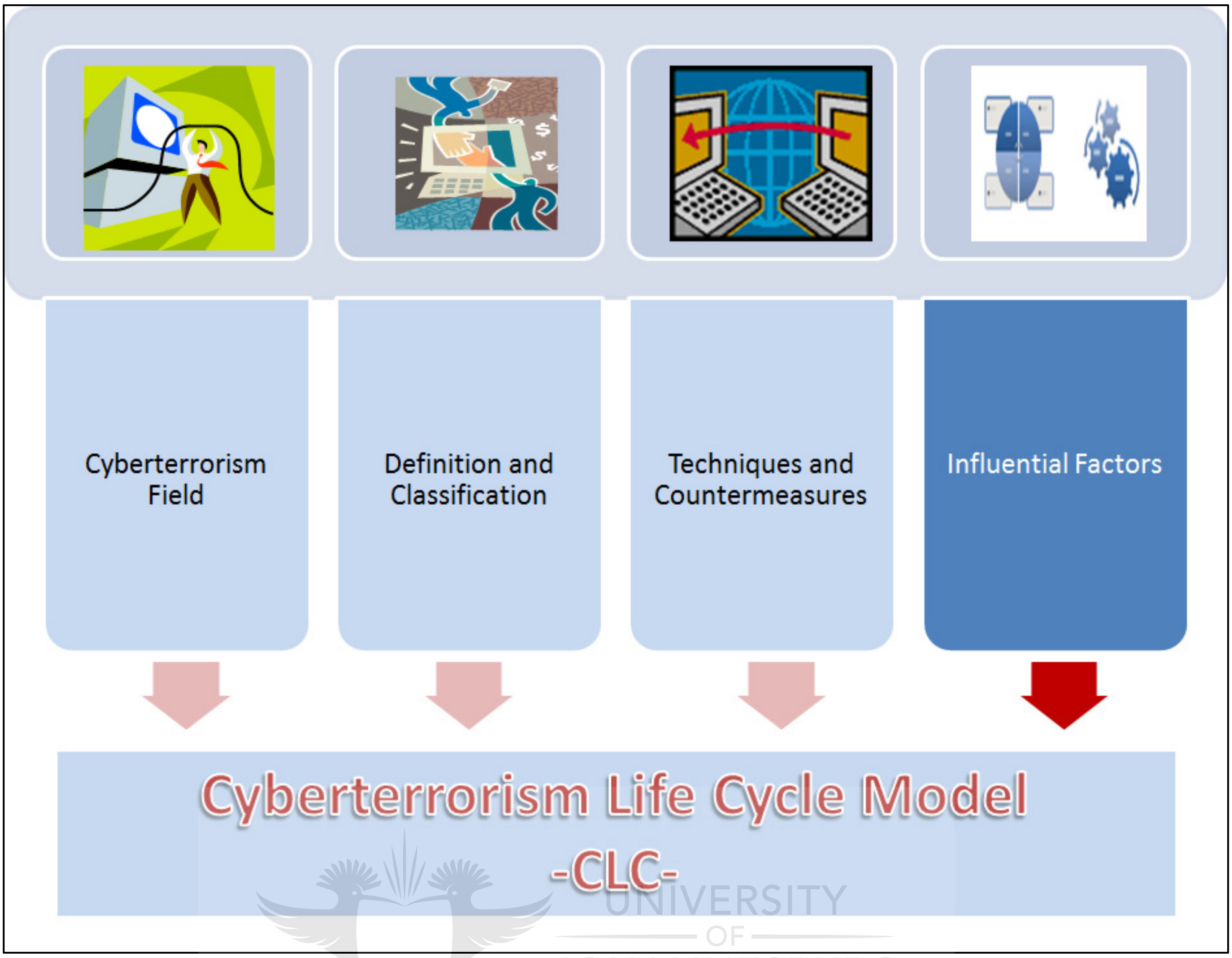

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 34: CLC model focus Chapter 8 - Cyberterrorism Representation of Influential Factors (Own Compilation)

Figure 34 shows that the focus of the chapter will be on integrating the influential factors that will form the basis of the CLC mode.

Part 3 moves on to an initial study on the development of a cyberterrorist, which is one of the core research problem statements of this dissertation. This chapter is largely based on the Observe-Orient-Decide-Act (OODA) loop by Col J Boyd as the loop shows the process of decision-making, which is a fundamental factor in the life of a cyberterrorist. Therefore, this chapter will expand on the research to show how cyberterrorism can develop by providing a high-level mapping to the Observe-Orient-Decide-Act (OODA) loop. The chapter commences with a discussion motivating the mapping to the OODA loop. The OODA loop consists of a number of phases for decision-making and thus it was found to be an appropriate model in order to formulate some of the foundation concepts of the CLC model.

8.1 Background

Citizens can be influenced by group behaviour. People can also be swayed into supporting certain ideals, values, political agendas or religious beliefs. The previous chapter discussed various influential factors. Therefore, it is imperative to understand how environmental issues, culture, social standing, tribal relations, loyalties, power and self-fulfilment drive cyberterrorism. There arises a need to represent the interaction of motivational and technical drivers of cyberterrorism succinctly.

A semiotic model and Red Teaming model were evaluated to assess how the influential factors of cyberterrorism can initially be represented. Desouza and Hensgen (2003) presented a semiotic framework to address the reality of cyberterrorism. This framework is summarised in the next section. Thereafter, the following section investigates Red Teaming to analyse cyberterrorism.

8.1.1 Semiotic Framework

8.1.1.1 Semiotic Framework Overview

Desouza and Hensgen (2003) proposed a semiotic emergent framework for cyberterrorism. This section summarises their findings. They state that there is much debate over the precise definition of cyberterrorism but many studies look at how cyber attacks can be categorised. According to Desouza and Hensgen attacks can be seen as conventional (overt) or unique (covert):

- **Conventional attacks** are disruptive to information infrastructure and include worms, viruses, Easter eggs, Trojan horses, or distributed Denial-of-Service attacks.
- **Unique attacks** are considered a variant of cyberterrorism and entail the use of valid electric devices to enable communication between terrorist groups. These include messages on discussion boards and steganography.

Due to different views, the issue of cyberterrorism and the use of cyberspace also arise. Insight into large-scale attacks on national information infrastructures like energy and defence is often the focus. This may lead to overlooking vital threats to security in general. Attacks may be masking in disguise. Attacks come in various waves or levels as familiarity with the target is gained.

A semiotic model is proposed to frame the levels of attacks that may be recognised. Semiotics is the formal doctrine of signs (Lyons 1977). Semiotics can be used to provide background to a field, its meanings, associations and evolution. Semiotics can be studied as follows (Desouza and Hensgen 2003):

- **Syntactics**: entails the relationships or links between various components.
- **Semantics**: placing relationships in context and perspective.
- **Pragmatic**s: gaining meaning and insight from relationships within the context of syntactics and semantics.

A variation of the traditional semiotic ladder segments threat phases into five levels: morphological, empirical, syntactical, semantic and pragmatic. These levels are explained as follows (Desouza and Hensgen 2003):

- **Morphological/Physical**
  - Concerned with objects and agents at the basic stage.
  - Cyberterrorism at this level consists of individual acts carried out by an agent. Examples include a cracker or hacking agent trying to bring down a web site.

- **Empirical**
  - Observable in nature, grouping of common acts and agents.
  - Grouping of perpetrations with similar origins and attacks. For example identifying a group of attacks on a domain name server or a Denial-of-Service attack could be traced back to a group of IP addresses.
- **Syntactical**
  - Derive high- order information linking objects and agents from the morphological and empirical levels.
  - The aim is to assimilate the data into meaningful sets. Data at the morphological and empirical levels may be interdependent and interrelated. By identifying patterns and relationships cyberterrorism activities can be better predicted. For example, using cause-effect diagrams, association rules and network analysis to couple agents and objects. At this level, it is important to deduce syntactical connections.
- **Semantic**
  - Consists of detailed analysis of the components in the relationship in the appropriate system context.
  - This entails studying the relationships, associations and role of objects in the high-level system. Most cyberterrorism literature can be considered in this level.
  - Attacks at this level are aimed at national information infrastructures with large-scale impact. The environment for these types of attacks is national and global. To carry out the attacks the perpetrators are usually skilled and knowledgeable about the systems. Insider knowledge can be used to exploit systems.
- **Pragmatic**
  - At this level, the information gained throughout the model can be used to aid decision-making.
  - This level synthesises everything that was learned in the earlier levels and involves a response. Processing the information for a second time in the semiotic model is likely to be advantageous. For example, a power grid failure on the West Coast is run through the model to determine whether it is related to terrorist activity. On the second cycle, if a similar incident happens elsewhere in the country, much of the refining work of finding the suspect will already have been carried out in the first cycle.

This section provided an overview of the semiotic framework for cyberterrorism. In the next section, the semiotic framework is compared to the CLC model drivers to determine its shortcomings.

8.1.1.2 Comparison of Semiotic Framework to CLC Model Drivers

The use of the semiotic framework helps to analyse the levels of the cyber-attack. Classifications can be carried out based on risk, possibility of occurrence and impact or rate of damage. A cyberterrorism act could also emerge from the semiotic levels. It is important to first limit issues at the morphological layer before trying to prevent attacks of an empirical or semantic nature. Terrorist attacks increase in sophistication through the various semiotic layers. It is therefore important to study cyberterrorism not only at the various semiotic layers but also at the emergence of these acts across the layers.

Since the conclusion of every chapter contains a list of drivers, which are important to incorporate into the CLC model, it would be helpful to compare the semiotic model to some of these drivers that will contribute to the CLC model. Now that a summary of the semiotic model has been provided, a comparison is provided to some of the CLC model drivers as identified and explained at the end of every chapter (not all drivers are applicable to the semiotic framework and therefore this comparison is meant to indicate the main aspects where the semiotic framework falls short of representing the cyberterrorism field). Table 7 shows the selected CLC model requirements, the comparable stance in the semiotic model and the associated shortcoming.

Table 7: Comparison of Semiotic Model to CLC Model Drivers (Own Compilation)

CLC Model Drivers	Semiotic Model	Shortcoming
The CLC model will incorporate the different motivating reasons (political, social or religious). (In Section 3.10).	The semiotic model describes cyber attacks and may list originating group.	The motivation behind every group is not explicitly identified.
A formal definition of cyberterrorism establishes the foundation knowledge. The definition also contributes to the CLC model by providing a basic explanation of the field. (In Section 3.10).	There is much debate over the precise definition of cyberterrorism but this study looks at how cyber attacks can be categorised as cyberterrorism.	Cyberterrorism attacks are analysed but no definition for cyberterrorism is provided.
ICT infrastructure can serve as both a weapon to support an attack or as the target. This idea is important in differentiating between support and attack goals. (In Section 3.10).	The semiotic model considers cyberterrorism as conventional attacks, as well as unique activities like those supporting communication.	Support functions are not only limited to communication and fails to include other functions like recruitment and propaganda.
Preparation, means and target can be a combination of digital and physical aspects. (In Section 4.7)	Cyber attacks occurring in cyberspace are classified.	Does not address the use of a combination of physical and digital preparation, means and targets.
ICT has various advantages for cyberterrorism, which includes: affordability, anonymity, variation, enormity, remote control, direct effect, automation, replication and speed. Identification of these characteristics will be shown in the CLC model. (In Section 5.7).	The semiotic model analyses attacks and relationships surrounding the attacks.	The characteristics that make cyberterrorism advantageous are not covered.
Social factors that influence the development of cyberterrorism will be	The model will study relationships to identify the	Social factors are not represented in the semiotic model.

CLC Model Drivers	Semiotic Model	Shortcoming
shown to be a significant influential force in the CLC model. (In Section 5.7).	perpetrators and sophistication of the attack.	

Overall, the semiotic model looks at the analysis of attacks to determine who and how it was carried out. The semiotic model mainly addresses the development of attacks from an execution point of view. However, the CLC model needs to cover technical, motivational and strategic issues. The CLC model will cover a wider range of aspects than the Semiotic Model and not just the technical progression of attacks.

Next, another method of modelling cyber terrorist behaviour is assessed to determine its functionality in representing cyberterrorism appropriately.

8.1.2 Red Teaming

Schudel, Wood and Parks (1999) in their paper on Modelling Behaviour of Cyberterrorists propose studying the adversary process through Red Teaming.

In addition, Wood and Duggan (2000) states that the approach of a Red Team stems from the premise of an analyst modelling an adversary. Also, Palmer (2001) mentions that organisations have come to the realisation that one of the best ways to assess the intruder threat would be to hire an independent computer security professional to try and compromise the security of computer systems. Red Teams are often used to show how an attacker can execute an exploit on a system and thus, using this approach Schudel et al. modelled cyberterrorism. The remainder of this section provides a summary of their work (Schudel, Wood & Parks 1999).

Shudel et al. (1999) propose a few hypotheses taken from literature. The hypotheses include:

- Information systems managing a nation's defences and critical infrastructures can be vulnerable to cyber attacks.
- Terrorists can advance their agenda by carrying out an attack on a nation's critical infrastructure.
- Cyber attack costs (when considered in proportion to their perceived effectiveness) asymmetrically favour cyberterrorism.

The adversary is modelled by the Information Design Assurance Red Team (IDART) and makes the following assumptions (Schudel, Wood & Parks 1999):

- **Sophistication:** the cyberterrorist has a high level of sophistication that is comparable to the skill level of a hacker and a member of a foreign intelligence organisation.
- **Resources:** the adversary has access to commercial resources that are generally available. These may include consultants, commercial technology, expertise, developers, information on tools, attacks and target.
- **Intelligence**: the adversary has intelligence support and can thus gain design information of the target.

- **Life cycle**: the adversary can affect the life cycle of a product by influencing individuals with access or the product development. By influencing these critical role players, the target's product could be altered.
- **Risk aversion**: the risk profile of the adversary is risk averse. This means that even though the adversary is hostile, there is still some level of care to prevent detection.
- **Specific target**: there is a specific target or goal in mind. To carry out an attack, it is important to identify a target and goal for the attack. This helps determine the success of the attack.

IDART served as a model of cyberterrorism. It led to reviews to determine whether any patterns emerged. A summary of the significant patters follows (Schudel, Wood & Parks 1999):

- The Red Team spends the majority of the time gathering intelligence on the target
- The outcome is that the Red Team can successfully attack the system or exhaust the available resources
- The Red Team will give up before embarking on a path that is above their risk threshold
- The Red Team follows the same approach each time and this could make it vulnerable to countermeasures.

Previously, the conclusion of every chapter contains a list of drivers, which are important to incorporate into the CLC model. Now that a summary of the Red Team model has been provided, a comparison is provided to some of the CLC model drivers as identified and explained at the end of every chapter. (Similar to the semiotic framework comparison, certain drivers have been selected to indicate the main shortcomings of the Red Team model of a cyberterrorism adversary). Table 8 shows the selected CLC model requirements, the comparable stance in the Red Team model and the associated shortcoming.

Table 8: Comparison of Red Team to CLC Model Drivers (Own Compilation)

CLC Model Drivers	Red Team	Shortcoming
The CLC model will incorporate the different motivating reasons (political, social or religious). (In Section 3.10).	The Red Team approach shows how the attack is carried out technically.	The motivation behind every group is not explicitly identified.
A formal definition of cyberterrorism establishes the foundation knowledge. The definition also contributes to the CLC model by providing a basic explanation of the field. (In Section 3.10).	This Red Team research addresses the execution of attacks.	The process of an attack is analysed but no definition for cyberterrorism is provided.
ICT infrastructure can serve as both a weapon to support an attack or as the target. This idea is important in differentiating between support and attack goals. (In Section 3.10).	The Red Team assumes that resources are available and that intelligence can be gathered.	Support functions are not only limited to intelligence but can also include recruitment and propaganda.

CLC Model Drivers	Red Team	Shortcoming
Cyberterrorism attacks will most likely be carried out against high-profile targets. Typical targets include transportation, utilities, finance, communication, emergency, public health and agriculture. The CLC model will cover the different types of targets.(In Section 5.7).	The initial results of the Red Team model show the attack process.	Attacks on high-profile or critical infrastructure are not differentiated.
Preparation, means and target can be a combination of digital and physical aspects. (In Section 4.7).	The Red Team Model shows the digital preparation and execution of attacks.	Red Team Model does not address the use of a combination of physical and digital preparation, means and targets.
Social factors that influence the development of cyberterrorism will be shown to be a significant influential force in the CLC model. (In Section 5.7).	The model will study technical execution of attacks.	Social factors are not represented in the Red Team Model.

The Red Team Model largely looks at the observed adversary attack process and does not consider the motivation behind the attacks. In addition, the Red Team Model does not cover the differentiation of cybercrime or support functions. The CLC model will address a wider range of factors that include the technical execution and motivation. The CLC model will aim to integrate the various concepts that span the field of cyberterrorism.

The previous chapters show that cyberterrorism consists of a wide range of influential factors and therefore to represent these influential forces it is important to study other methods of information representation for cyberterrorism.

8.2 Observe-Orient-Decide-Act

Further research was carried out to find an apt framework to represent the influential factors of cyberterrorism. The Human Social and Cultural Board (HSCB) program in the United States developed a simple framework entitled the Socio-Cultural Behaviour Capability Areas Framework (Schmorrow 2011) based on the Observe-Orient-Decide-Act loop from Lt. Col John Boyd (Joint Chief of Staff 1996). The Socio-Cultural Behaviour Capability Areas Framework is shown in Figure 35.

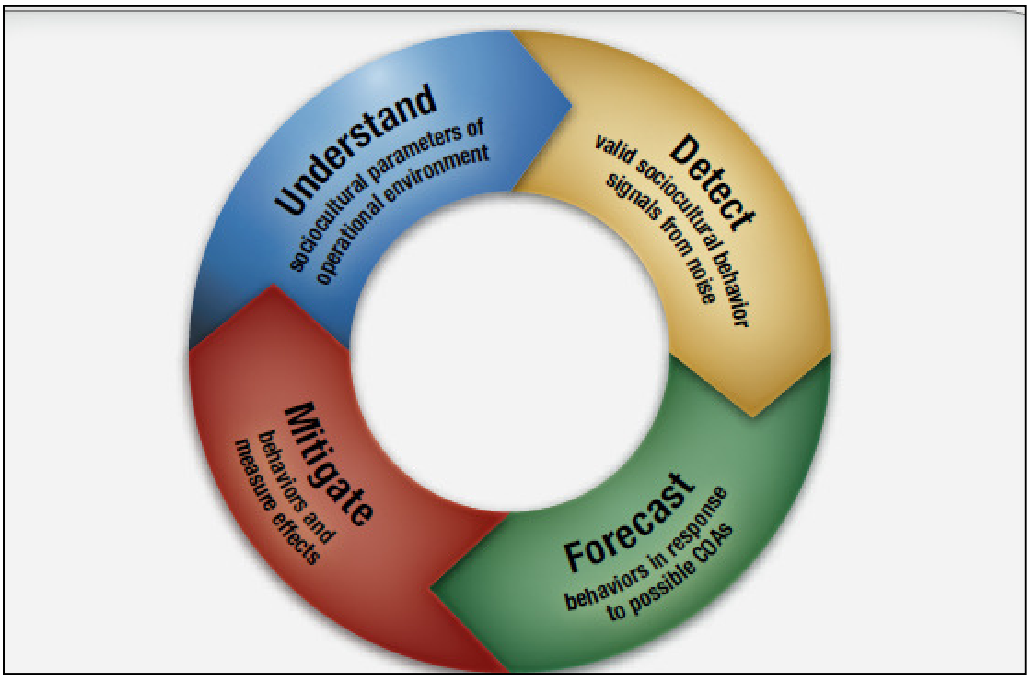

Understand
sociocultural parameters of operational environment
Detect
valid sociocultural behavior signals from noise
Forecast
behaviors in response to possible COAs
Mitigate
behaviors and measure effects

Figure 35: Sociocultural Behaviour Capability Areas Framework (Schmorrow 2011)

The OODA loop has been used extensively in various service doctrines of the United States Defence Force including the Joint Publication 3-13-1 Joint Doctrine for Command and Control Warfare (Joint Chief of Staff 1996). Originally proposed by Boyd in 1987, the outline capabilities of the Observe-Orient-Decide-Act loop show the transition of activities feeding into each other and forming a cycle. Similarly, Williers (2007) provides a mapping of the Information Hierarchy, OODA loop and various other factors to describe integrated Information Warfare. Mapping out factors can help provide clarity and gain better insight into the various issues in question. Therefore, this chapter addresses a mapping of the various influential cyberterrorism factors to the OODA loop. This helps to visualise the conceptual knowledge of the various influential factors, as well as the dynamism of decision-making.

The OODA loop is versatile in that is it able to span all the various levels of factors influencing cyberterrorism. The OODA loop is initially used in this chapter to form a structured framework to represent the factors that contribute to the development and functioning of a cyberterrorist. Later on, the mapping to the OODA loop will be adapted to show the life cycle development of a cyberterrorist. The next section therefore addresses the initial mapping to the OODA loop that forms the basis for the CLC model.

8.2.1 Introduction to Mapping

The previous chapters indicated that various factors can influence cyberterrorism. In order to analyse the influence of these factors on the development of a cyberterrorist, this chapter proposes a mapping to the Observe, Orient, Decide, Act (OODA) loop.

The mapping will take into account how information is received, transformed and can be used by cyberterrorists, through the consideration of the evolution of information in the Information Hierarchy. The mapping will capture the main interactions between the OODA loop, Information Hierarchy and the influential factors identified in the framework in Chapter 5. Overall, the mapping will integrate the various influential factors of cyberterrorism to show a more holistic interaction between the various operating forces.

At a technical level, cyberterrorism can target critical services like emergency departments, banks, fuel supply or air traffic control. While it is difficult to determine why terrorists pick a target, it would be useful to understand the development, transformation and operation of cyberterrorists.

Studying how insurgent groups arise, can provide insight into environments that incubate and promote the advancement of terrorist conduct. However, due to the large number of factors influencing cyberterrorism ranging from the social circumstances to capabilities and objectives, it would be useful to represent all these psychological, technical and counter-terrorism issues succinctly.

Col John Boyd proposed the theory encapsulated in Observe, Orient, Decide and Act (OODA) loop (shown in Figure 36) (1987). Subsequently, this idea has been applied in various ways (such as OODA loops within each phase of the loop). Conceptually, this principle provides an ideal foundation to demonstrate the transformation of data and information into tacit and explicit knowledge and thereafter establish additional content relating to the development and execution of cyberterrorism.

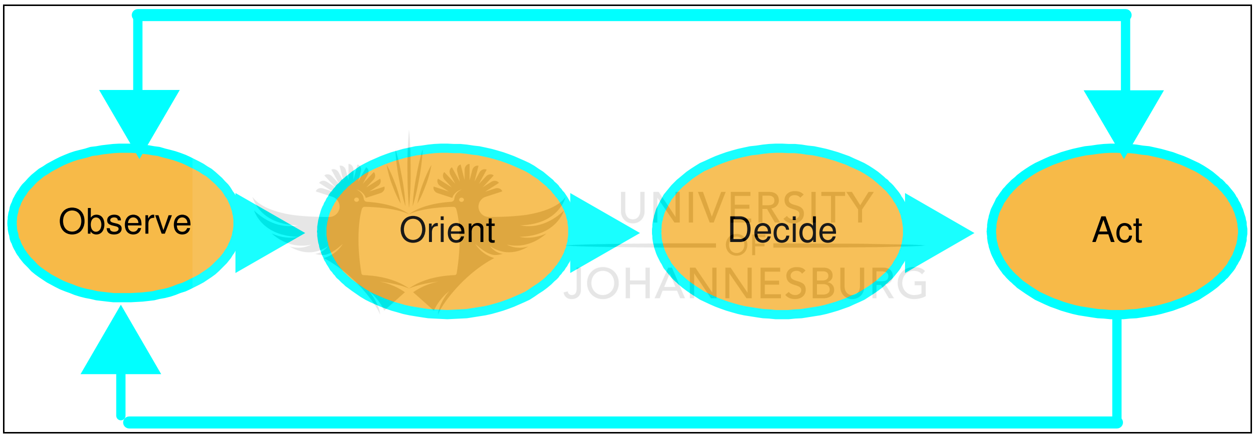


Figure 36: OODA Loop (Joint Chief of Staff 1996)

The next section looks at the hierarchy of information, which provides the context for the development of a cyberterrorist. The different classifications of information in the hierarchy are used as an additional layer in the mapping of the cyberterrorism framework to the OODA loop to show the transformation into a cyberterrorist.

8.2.2 Hierarchy of Information

To show more detail in the OODA loop, information classification is considered. This serves to show how information develops hierarchically and thus helps classify the information type that may be involved in the different aspects of the OODA loop mapping. Williers et al. (2005/06) explores the hierarchy of information in more detail. A graphical representation is given in Figure 37. An overview of the Information Hierarchy concepts is presented thereafter.

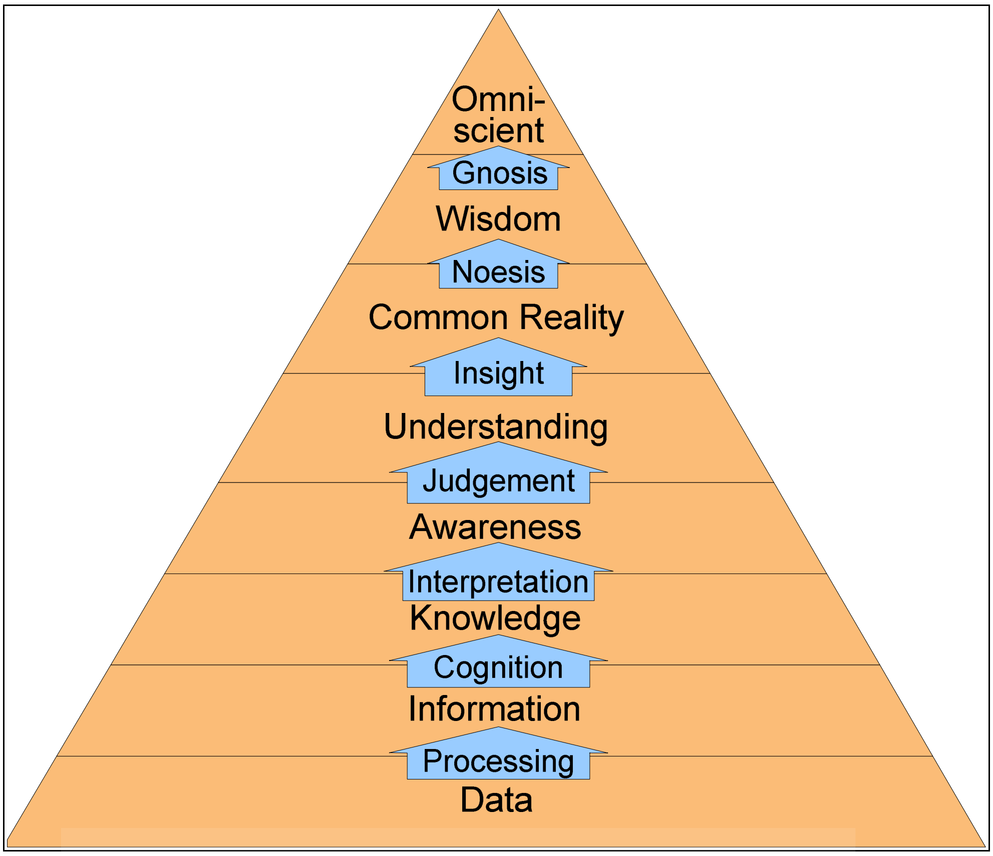


Figure 37: Hierarchy of Information (Rowley 1998)

According to Rowley (1998), data is information that should undergo some processing so that the results of the processing can be communicated for a particular purpose. Data at the most basic level represents information in a raw format that can undergo some processing and can be stored on computer systems.

Definitions of information from the online dictionary Answers.com include (2013):

- A collection of facts or data
- The action of informing
- The state of being informed
- Data that has undergone some form of processing, storage or transmission
- Knowledge gained from studying, experience or instruction
- Knowledge of specific event or situations that have been gathered or obtained from communications, intelligence updates or news reporting

Data, information and knowledge are intertwined concepts that represent content that is received and thereafter perceived by humans. Knowledge, according to the Oxford dictionary (2008) is defined as:

- Information and skills that is gained from experience or education
- The sum of what is known
- Awareness or familiarity

Therefore, to summarise data, information and knowledge, Hutchinson and Warren (2001) states that data describes attributes of things; information is data that has been collated; and knowledge is information that has been interpreted based on experience. Data and information therefore represent the most basic form through which sensory input is received. Data once processed becomes information. When information is cognised, knowledge grows.

From knowledge comes awareness. Awareness has a wider scope than knowledge in that awareness involves linking concepts together to make broader conclusions. Knowledge, once interpreted, can bring about a greater sense of awareness. Awareness leads to understanding through the process of judgement and inference. Understanding involves cognitive and analytic development. Understanding can lead to new knowledge and thus new synthesis of thought can take place.

With insight from a broader sector, understanding can form a common reality. Common reality is representative at a wider level and tries to incorporate many perspectives. From common reality, we move on to wisdom, which can be subjective in nature. Established principles and human codes, like morality and ethics, guide behaviour. Wisdom can be philosophical in nature and deals with the judgement between right and wrong or good and bad. Decisions that are considered wise are not easily determined or predicted and require discernment, reflection and contemplation.

At the highest level comes omniscience, which is highly matured wisdom that evolves from gnosis (intuition and knowledge of truths). Acting with omniscience implies infinite knowledge.

This discussion summarised the transformation of data into wisdom and thus the development of implicit and tacit knowledge that facilitates the execution of activities. This theory will be used in the mapping of cyberterrorism to the OODA loop in the next section.

8.3 Mapping to the OODA Loop

8.3.1 Introduction

Williers (2007) developed a mapping of the Information Hierarchy, OODA loop and various other factors to describe Integrated Information Warfare. Similarly, this approach has been applied to show an integrated picture of cyberterrorism and create the foundation of the CLC model. In Figure 38, a high-level mapping is given of the OODA loop to the Information Hierarchy, as well as to various aspects in the field of cyberterrorism. This representation serves to show the synergistic effect of all the relevant aspects. The integrated picture thus captures a more holistic representation of all the currently identified influential factors. Later on when more influential factors are identified and refined, the complete CLC model will be presented. However, the mapping to the OODA loop at this stage provides an apt representation of how the influential factors interact with each other.

The mapping is not exactly one-to-one in that some overlaps of the factors do occur. However, the map tries to provide an indication of the main relationships and influential factors in the field of cyberterrorism. A more detailed discussion follows on the various factors in the mapping.

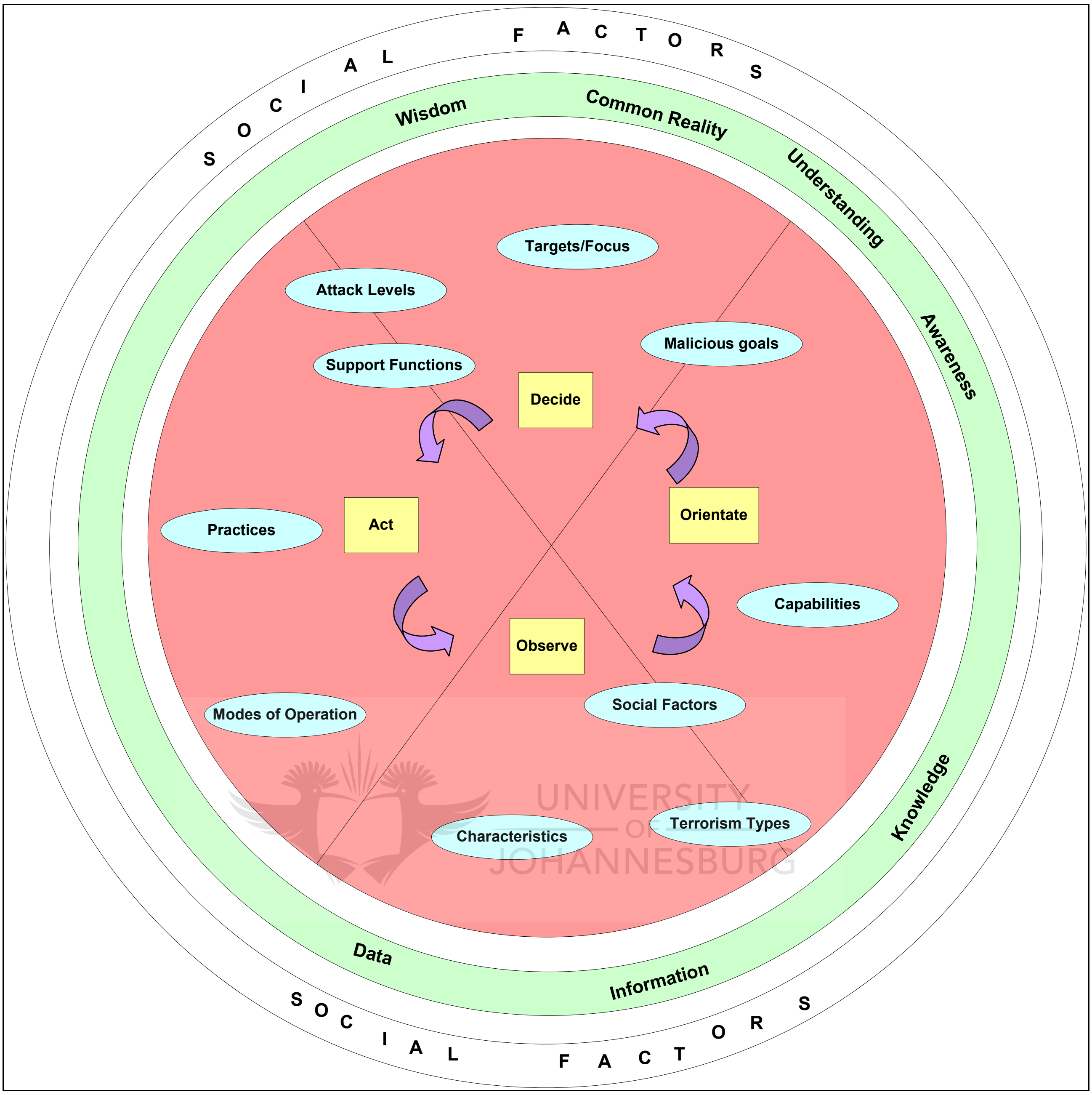


Figure 38: Mapping of Cyberterrorism to Information Hierarchy and OODA loop (Own Compilation)

At the centre of the mapping (Figure 38) is the OODA loop with the four blocks representing Observe, Orient, Decide and Act. Moving outwards, the various factors described in the conceptual framework (in Chapter 5) are shown (captured as ovals in Figure 38). Initially, social factors will strongly influence the formation of a cyberterrorist and are therefore shown under the Observe aspect of the model. However, social factors also span the outermost ring to show that they will influence the mind-set of a cyberterrorist throughout their lives. The second ring represents the various levels in the Information Hierarchy (as discussed in Section 8.2.2).

The four aspects of the OODA loop are divided into sections (separated by the large X through the centre of Figure 35). As mentioned previously, the mapping is not one-to-one and some overlap occurs. Therefore, some factors span over the different OODA loop sections in Figure 38. The Observe and Orient aspect of the

OODA loop looks at the various forms of data and information that are communicated. At a cyberterrorism perspective, this can deal with the observations that cyberspace has several advantages such as anonymity, variation, replication, enormity, remoteness, directness, automation and speed (Denning 2000, Weimann 2004). Furthermore, Webb (2009) mentions that low entry costs, problems with identifying an attack and its source and the potential for extreme chaos are all selling points for this form of terrorism.

It should be noted that the mapping to the OODA loop (Figure 38) forms the basis of the CLC model. However, in upcoming chapters, further analysis and research are carried out to determine additional drivers for the CLC model. Therefore, the mapping to the OODA loop in Figure 38 is a first-order attempt at establishing the CLC model. Upcoming chapters will provide additional drivers and refine concepts introduced in this mapping. The complete CLC model is depicted in Figure 60 on page 186 and presents the overall findings.

The mapping consists of a number of factors that were introduced in Chapter 5. Each of these factors are described in more detail in the next few sections. The first factor to be discussed is Social Factors.

8.3.2 Social Factors

Social factors are captured in the Observe and Orient sections of Figure 38. Section 5.4.3 first introduced the influence of social factors on cyberterrorism. Social factors entail the collective, shared environment, behaviour or conditions that may influence a person. Various social factors mainly influence the initial observations that a person makes. Jenkins (2006) explains that terrorism usually develops out of the ideas of law, morality, and the rules of war, together with the influence of concepts like culture, ideology and politics. Furthermore, Wilson, Wilcox and Richards (2005) show that culture, genetics, experience and new information is fundamental to orientation.

To elaborate further on the social factors that influence the development of a cyberterrorist, the findings of Daly and Gerwehr (in Kamien 2006) are given. Daly and Gerwehr (in Kamien 2006) author a chapter in the McGraw Hill Security Handbook and mention a few variables that are conducive for extremist recruitment. Social factors can be summarised as distress or dissatisfaction, cultural bombardment (disillusion), family dis-functionality and dependant personality tendencies. Thus, the conditions that affect a person’s upbringing can also influence the way in which data and information is perceived and thus the development of certain viewpoints. It was mentioned earlier that overlaps do occur and the various aspects do not strictly map to a single aspect of the OODA loop or the Information Hierarchy only. When considering social factors, aspects, like culture, beliefs, political views, upbringing and personality traits will play a supportive role throughout all phases of a cyberterrorist life. In this way, social factors are also shown in a central ring encompassing the entire model to indicate its influence throughout all stages. The discussion moves on to the other aspects of the mapping to the OODA loop.

8.3.3 Terrorist Types

Terrorist types correlate to the causes being promoted. It is linked to the religious, philosophical, social or ideological viewpoints and is thus linked to various initial observations and orientation of a person (See Figure 38). For example, terrorist types can include religious, New Age, ethno-nationalist separatist, revolutionary and far-right extremism (Weimann 2004). A cyberterrorist will proceed to act in support of a particular viewpoint or favourable cause. The reader is reminded that the types of terrorism include:

- **Religious**: strong religious ideas which can include the justification for the taking of lives
- **New Age thinking**: manipulation tactics and impact of unconventional attacks
- **Ethno-nationalist separatist**- promote establishing a new political order based on ethnicity
- **Revolutionary**: inadequacy of the government or state and need to overthrow social order
- **Far–right extremist**: justification for seizing power due to superiority belief system

8.3.4 Further Analysis of OODA Loop Mapping

Figure 38 shows the interaction of various influential factors. In this section, these factors are further analysed. Information due to social circumstances, psychological development and exposure to the environment all form part of the baseline observations that are made. During observation and orientation, identification with family, tribes, religion and social loyalties plays a huge role. The social environment that a youngster is exposed to influences later decisions and activities in life. For example, in impoverished war-torn African countries, young children are forced to join guerrilla groups and fight indiscriminately. Arabic scholars are taught in madrassas whereby the pillars of Islam are instilled at a very young age. This type of exposure promotes loyalty to a cause for the purposes of survival, acceptance and social norms. In cultural groups, there is the tendency for a common set of principles to be established and followed. Behaviour that is compliant with this common set of principles is often encouraged. Whilst personality and relationships are immense driving forces, culture, customs and society does affect an individual's development. Culture is the cornerstone for encouraging new members and provides an avenue to direct and influence existing members. Values, impressions and loyalties are developed through culture as well as provide the sense of belonging.

Once inherent tendencies are stimulated or loyalty to a cause is established, the potential to become a cyberterrorist exists. Thereafter, during the orientation stage capabilities and malicious goals can be formed which will aid with the decision-making and execution of cyberterror activities in the future. Capabilities include education, training, skills, expertise, financial support, resources, intelligence or insider knowledge. Some of the capabilities like education, intelligence and training lead to the establishment of higher knowledge. Knowledge contributes to the skill set, expertise and experience. Thus, the various forms of data and information that are received and interpreted into knowledge are interrelated. Whilst familiarising oneself with systems, networks, techniques and learning the appropriate skills, awareness is created. Awareness requires some analytical development, which is facilitated through the interaction on ICT systems, as well as interfacing with support members who are providing intelligence or funding. Thus, the capabilities of a cyberterrorist are developed.

At the decision phase of the OODA loop, the cyberterrorist operates at Common Reality, as the impact of the broader environment is the focus. The Common Reality may seem skewed due to the malicious goals, which objectively do not promote greater good. However, at the subjective level the cyberterrorism characteristics, social factors, capabilities and terrorist type thinking is the driving force behind subsequent decisions and will continue to influence future actions. During the decision phase, a target will be selected based on the underlying goals that are trying to be achieved. Cyberterrorist targets include (Collin 1997) (Desouza, Hensgen 2003) (Foltz 2004) (Lewis 2002):

- **Transportation**: air, rail, road
- **Utilities**: water, energy
- **Financial**: banks, foreign exchange agencies
- **Communication**: telephone, radio
- **Emergency**: health, fire, police
- **Public Health**: hospitals, health department
- **Agriculture**: feed suppliers, processing and packaging plants

8.3.5 Objectives

Section 5.6 initially discussed the objectives of malicious goals and support functions. Overall, the cyberterrorist seeks to protest, disrupt, kill, maim, terrify, intimidate, demand, affect sensitive information or crucial services, gain publicity or solicit money (see Figure 16 in Chapter 5). ICT can also play a supportive role to terrorism in general. These objectives will have an impact across the OODA loop (see Figure 38). Examples in which ICT plays a supportive role include recruitment, training, intelligence, reconnaissance, planning, logistics, finance, propaganda, and social services. Such activities utilise the capability provided by ICT to enable communication, marketing and funding. Thus, computers and networks also enable terrorism by providing supporting functionality.

8.3.6 Levels of Attack

Furthermore, decisions concerning the levels of attack will be made. The level of attack will be determined in the Decide section of the OODA loop (see Figure 38). This relates to whether simple exploits will be executed or complex co-ordination over a number of years will take place. At a high level, cyberterrorism can have different modes of operation to carry out a number of practices. Arquilla and Ronfeldt (2001) talk of the three broad offensive categories, which include perception management and propaganda; disruptive attacks to immobilise a site/service/system temporarily and; destructive attacks that ruin physical or virtual systems/networks. This correlates to the modes of operation, which determines the type of action that will be unleashed. Typical examples of practices used to carry out cyberterrorism are web defacement, disinformation, propaganda, Denial-of-Service with malware, crucial service disruption, data corruption and credit card information theft. Whilst operating in the virtual world of cyberspace and networks, execution of cyberterrorism practices will require physical interaction with ICT equipment. Thus, whilst cyberterrorism does mainly involve virtual connections, there are some associated physical connotations.

8.3.7 Summary of Mapping to OODA Loop

Overall, the mapping in Figure 38 captures the transformation of information that influences the mind-set of an individual into a cyberterrorist. Thus, it shows how information at a certain level is received and used. The mapping also captures the development of a cyberterrorist by showing how various factors affect observation, orientation and decision-making to eventually lead to the execution of cyberterrorist acts.

In general, the model can be practically applied when studying certain insurgent/clandestine groups and documenting how the terrorist tendencies and behaviour developed. It is often difficult to infiltrate an ethnic/religious/cultural group, as a limiting factor will lie in the physical appearance of the operative. Members who are part of the cultural or belief system can be convinced to provide information and thus contribute to intelligence gathering. In this way, insight can be gained into the different personality differences, inherent tendencies, values and morals that contribute to the initial psychological seeds that are planted which then promote the struggle for a certain political or social cause. This model is helpful in profiling a terrorist group and understanding how the capabilities are developed, how targets are selected, the supportive functionality that ICT plays in the organisation and how they operate. In this way, the life cycle of a cyberterrorist can be established as a person moves from the initiation stages through to immersed operation in a terrorist organisation. This mapping will further be used in the compilation of the life cycle model that shows how a cyberterrorist develops.

8.4 Conclusion

Various facets ranging from technological to motivational reasons drive cyberterrorism. This chapter shows a mapping of these various components to the OODA loop in an attempt to capture a more dynamic representation of these influential considerations. This chapter provides insight into the growth and execution of cyberterrorism activities by capturing various interacting aspects in the field. Aspects in the mapping include the Information hierarchy (to show the transformation of information), as well as factors like characteristics, social factors, terrorist types, capabilities, goals, targets, attack levels, support functions, practices and modes of operation.

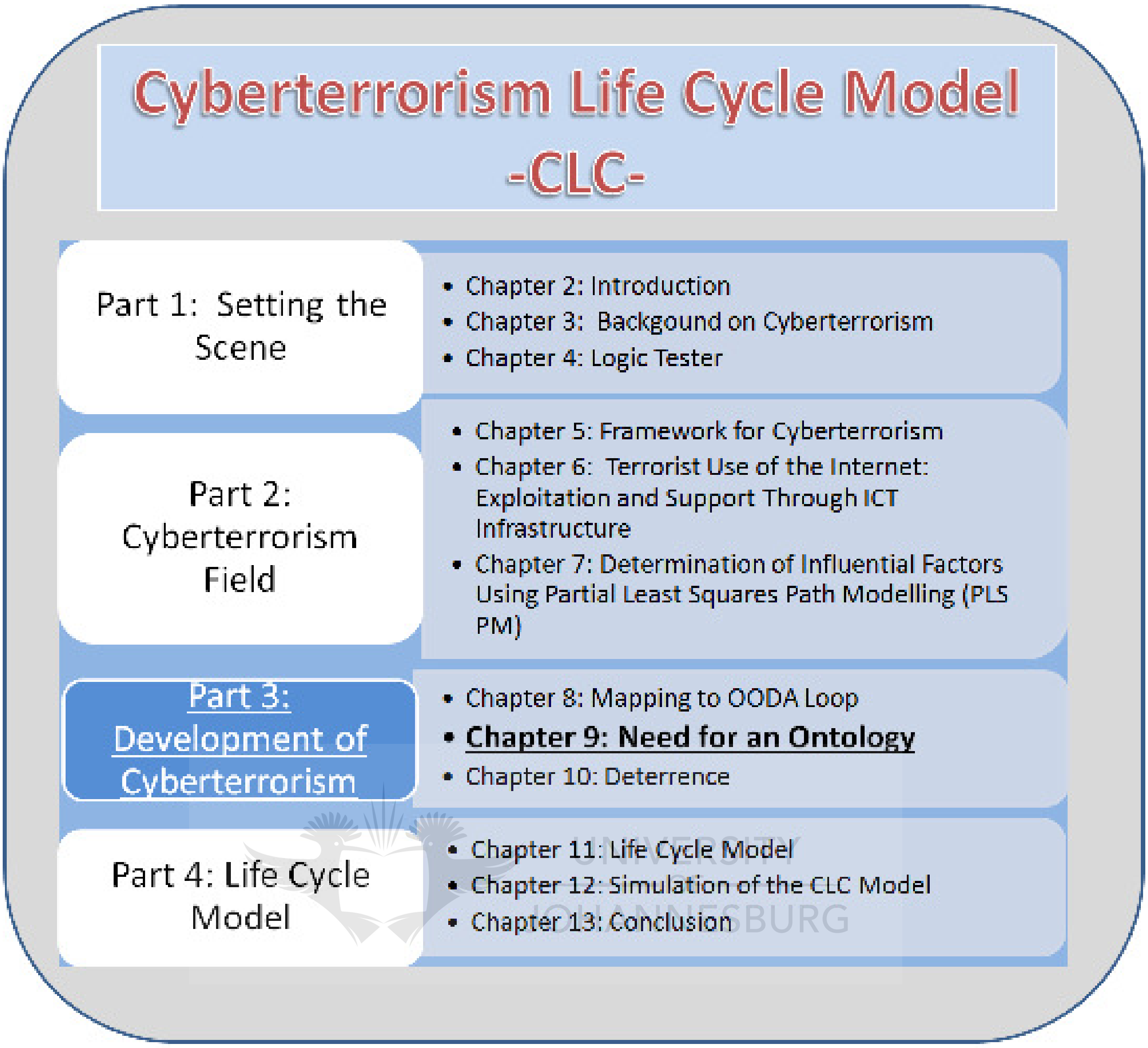
In summary, the vital drivers that are derived from this chapter that will contribute to the CLC model are as follows:

- Social factors are an influential factor throughout the life cycle of cyberterrorism. This critical concept will be reflected in the CLC model (Section 8.3).
- During the initial observation phase, the important influential factors are the characteristics of ICT that make it a viable target or weapon, together with initial motivational forces that stems from the classification of terrorism types. This idea will be represented in the CLC model (Section 8.3).
- Critical to the orientation of a potential cyberterrorist is the capabilities that they possess. In addition, key to driving the development of a cyberterrorist is the social factors and motivation forces that stems from terrorism types, together with the formulation of initial malicious goals (Section 8.3).

- The decision phase consists of the target selection, which is based on the malicious goal or support function to be achieved. This will contribute to the development of the CLC model to show the formulation of objectives and targets (Section 8.3).
- When carrying out a cyberterrorism act, certain practices will be employed. The CLC model will show the various practices that can be utilised as part of a cyberterror attack or support function (Section 8.3).

In summary, the OODA loop provides a well-suited baseline to show the synergistic effect of all these aspects. Overall, this chapter aims to place the field of cyberterrorism in context against various developmental and technical issues.

Now that the initial CLC model has been formulated with the aid of mapping the critical concepts to the OODA loop, the discussion moves on to the development of an ontology. The ontology was used as a means of structuring the field and showing relationships in an ordered manner. In previous chapters, the use of ICT for support functions and malicious objectives were discussed. Furthermore, earlier chapters also introduced the ideas that cyberterrorism is confused with cybercrime in general. Therefore, in order to provide deeper input to the CLC model, an ontology was developed in order to identity the core aspects that contribute to cyberterrorism and the different life cycle phases, as well as to define a cyberterrorism attack, a support function and an undefined cyber event. The next chapter therefore presents an ontology for cyberterrorism.



Cyberterrorism Life Cycle Model

-CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- **Chapter 9: Need for an Ontology**
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

9 Need for an Ontology

"While Bin Laden may have had his finger on the trigger, his grandchildren may have their fingers on the computer mouse."

- Frank Cilluffo formerly of the Department of Homeland Security

Part 1 and Part 2 place the field of cyberterrorism in context by providing background information relating to the driving forces, contributing factors and overall influential issues in the field. Part 3 builds on Part 2 by introducing the use of ontologies, which further shows the interaction and relationships between the factors initially introduced in Chapter 5 and Chapter 8. In this chapter, the factors initially described in Chapter 5 and Chapter 8 are refined using an ontology. This chapter therefore addresses the need and application of an ontology for the field of cyberterrorism.

Figure 39 shows the current focus in this chapter to building a life cycle model for Cyberterrorism. Chapter 9 further addresses the Sub-objective 3, definition, and classification (originally indicated in Figure 3).

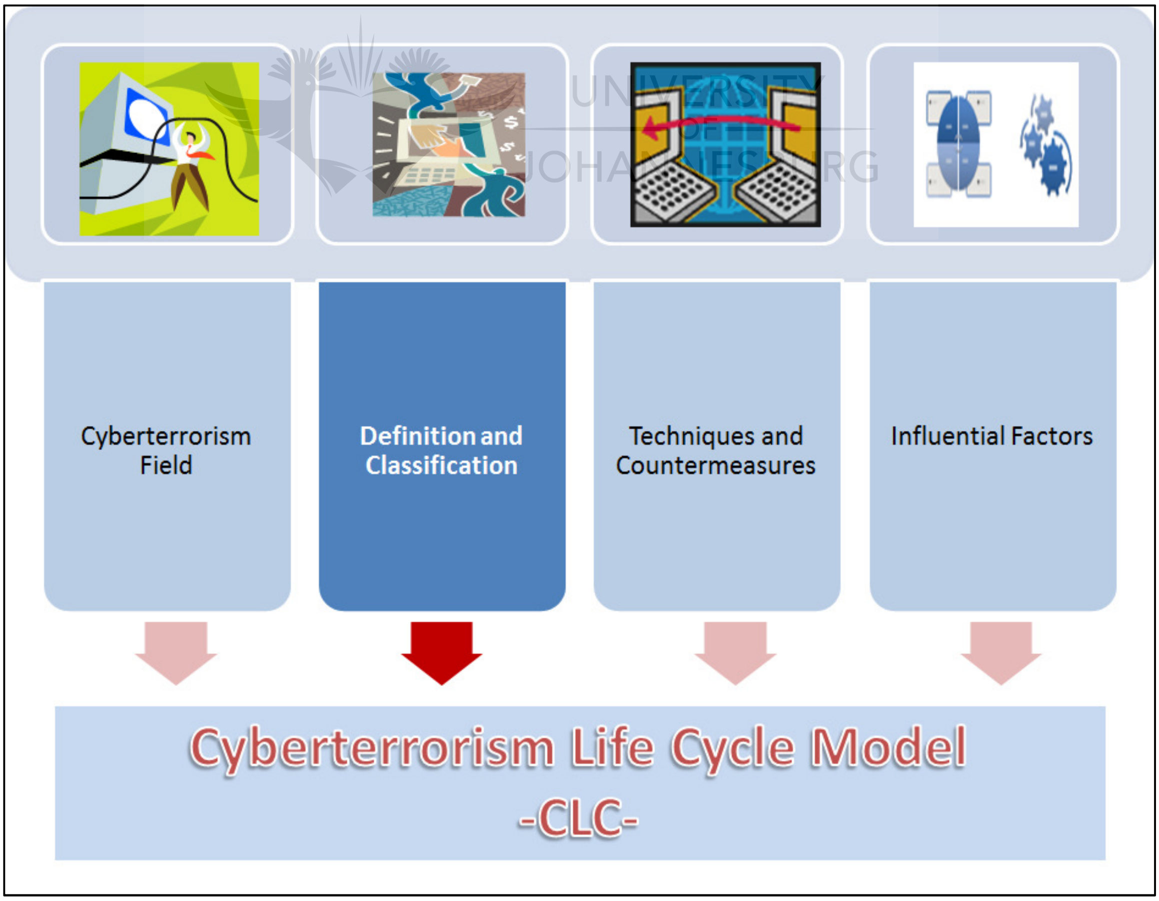

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 39: CLC Model Focus Chapter 9 - Cyberterrorism Definition and Classification Continuation (Own Compilation)

9.1 Introduction

The investigations carried out in previous chapters aimed at placing the field of cyberterrorism in context by describing the operating forces, techniques, motivations for carrying out cyberterrorism, as well as the function of the Internet to support cyberterrorism in general. This chapter discusses the modelling of cyberterrorism using ontologies.

Section 4.2 and 4.3 discussed the blur between cyberterrorism, cybercrime and traditional hacking and ICT infrastructure compromise. The misunderstanding of defining and differentiating attributes of cyberterrorism was discussed. In many instances, there are defining characteristics that separate traditional criminal cyber attacks from cyberterrorism. So how does one specify the attributes of a cyberterrorist attack in order to identify the defining concepts? This chapter proposes the use of ontologies to define whether a cyber event can be characterised as cyberterror, a support to terrorism or an unclassified other cyber event. Chapter 9 builds on the cyberterrorism OODA loop mapping in Chapter 8 in order to assess whether all the discussed factors make a significant contribution to defining a cyberterrorism event. This chapter thus helps to refine the compilation of the CLC model presented in Chapter 11.

This chapter first looks at the background of ontologies and the motivation for building a cyberterrorism specific ontology. Thereafter, the classes of the proposed ontological model are discussed: actors, effects, motivation, objectives, practices, targets and cyber events. The application of the model is practically demonstrated with examples. The chapter concludes with a discussion on future work.The main contribution of this research is the supplementation of the existing knowledge base of both cyberterrorism and cyber attacks, by enabling the convenient classification of an attack facilitated by ICT through a cyberterrorism specific ontological model. During the compilation of the ontology, the previously identified factors are applied. Therefore, the ontology helps to identify which of the influential factors can be refined for representation in the final CLC model.

The next section focuses on providing a motivation for the use of ontologies. This section aims to argue the usefulness of ontologies in the field of cyberterrorism. Thereafter, the ontological model is introduced. This is followed by a discussion on the specification of instances in the model.

9.2 Discussion on Ontologies

Gruber (1993), defines an ontology as a formal and explicit representation of a shared conceptualisation. Frantz and Franco (2005) argue that ontologies enable a shared and common understanding of a domain so that it can be communicated between people and computers to aid knowledge sharing and reuse. Furthermore, Frantz and Franco explain that ontologies offer a formal explicit conceptualization (which includes meta-information) to describe the semantics of information and contribute to the domain knowledge of knowledge based systems. Moreover, Curts and Cambell (2005) state that one of the most important uses of an ontology is the ability to define the boundaries, both internal and external to analyse the relationships within and across them.

In addition, Noy and McGuiness (2001) provide the following purposes for developing an ontology:

- To provide a shared common understanding of the structure of information between people or software agents
- Enable domain knowledge reuse
- Explicit specification of domain assumptions
- Separation of domain and operational knowledge
- To analyse domain knowledge

Jones, Bench-Cappon and Visser (1998) explain that the advantages of building an ontology or a domain model include the sharing of knowledge, as well as the re-use of knowledge. Therefore, ontologies can make a significant contribution towards knowledge capturing and sharing.

Uschold and King (1995) proposed a four-step methodology for developing ontologies: identify the purpose of the ontology, build the ontology, evaluate and document. The steps for building an ontology consists of three iterative sub-steps: capture the ontology, coding of the ontology and integration of existing ontologies. The capturing of an ontology entails identifying the key concepts and relationships from the studied field by producing precise unambiguous text definitions for these concepts and relationships. Ontology coding is the explicit representation of the conceptualisation in some formal language. Ontology integration refers to using other ontologies during the capture and coding process (Uschold, King 1995).

Overall, the usefulness of an ontology is summarised as follows:

- Formal representation
- Common conceptualisation
- Common understanding
- Knowledge sharing and reuse
- Shared structural understanding between people and software
- Reuse of domain knowledge
- Explicit specification of domain assumptions
- Analyse domain knowledge

It is envisaged that the ontology proposed in this chapter will provide important input to the development of the CLC model by identifying the critical concepts and eliminating redundant terminology. The next section will explain these steps in more detail in terms of the cyberterrorism ontology.

9.3 Background to Building an Ontology

9.3.1 Steps

Ontologies provide a common framework to share conceptual models. Through the use of an ontology, the internal and external environment of a field can be captured together with the relationships between them. This chapter proposes that an ontology can be used to identify and capture the content and boundaries in the field of cyberterrorism. The role of the ontology will be to provide a better structure and representation of relationships, interactions and influencing factors, as suggested by Noy and McGuiness (2001) in Section 9.2.

The initial step of building an ontology is to determine the purpose thereof. The aim of the proposed ontology is to determine whether a cyber event can be classified as cyberterror or a support to terror. The next step is to build the ontology by capturing key concepts and relationships, coding the explicit representation of the conceptualisation in the ontology language (in this case, Protégé), and integrating it with other ontologies. Ontologies provide the ability to form a knowledge base for a specified field. This step enables the formal capturing of domain knowledge to promote sharing and exchange.

Protégé is ontology specific software that serves as a knowledge base editor and thus facilitates the capturing of an ontology. It was developed at the Stanford University for both the Windows and Linux environments. Protégé provides the ability to define classes, relationships and properties. It is openly available and can be downloaded from http://protégé.stanford.edu. Horridge, Knublauch, Rector, Stevens and Wroe (2004) also explain that Protégé also comes with visualisation packages such as GraphWiz that allows the asserted and inferred classification hierarchies to be visualised. The visualisations help provide succinct images of the deductions drawn from the inserted data and specifications.

The next step is the evaluation of the built ontology. The reasoning capabilities within Protégé are used to infer new information from the asserted ontology as part of the evaluation process. Protégé has a number of built-in reasoners or inference engines that can be used to make deductions and queries based on the input specifications (the asserted statements and definitions).

In this research project, different reasoners drew the same conclusions and therefore did not influence the evaluation results. An ontology can contain information in an asserted form (stated as a fact) and thus it is valuable to operate on inferred relationships (derived as conclusion from given facts) rather than on the asserted relationships. Knublauch, Horridge, Musen, Rector, Stevens, Drummond, Lord, Noy, Seidenberg, and Wang (2005) explain this process minimises the loss of information about what has been explicitly asserted by the users. An important consideration is therefore the background logic that is used for reasoning certain arguments.

The final step is the documentation of the ontology. According to Prieto-Diaz (2003), ontologies are created in a very ad-hoc manner with the initial development of a controlled vocabulary for the subject area of interest. This is then organised into a taxonomy whereby key contents are identified and the concepts defined and related to create an ontology. Therefore, to initially develop the cyberterror ontology, a taxonomy was developed to identify the core concepts in the field of cyberterrorism. The process of building a taxonomy and ontology is very much intertwined. The various steps of building an ontology is iterative

(Capture, Code and Integrate). The next section looks at the development of the cyberterrorism taxonomy and ontology using Protégé.

9.3.2 Types of Ontologies

Figure 40 shows a framework of the different types of ontologies.

- **Upper**: focus on high-level ontologies with general-level descriptions
- **Core:** also known as mid-level ontologies and contain terms relevant across multiple domains
- **Domain** ontologies: cover terminology specific to that domain

Figure 41, Figure 42 and Figure 43 show examples of upper, core and domain ontologies. As one moves down the levels, the concepts become more refined and domain-specific. The type of ontology that cyberterrorism would best fit into is domain ontology. This is due to the detailed specification of terms that are relevant in the cyberterrorism field. Consequently moving upwards in the ontology hierarchy, cyberterrorism could fit into other mid-level domains like cybercrime and then high-level domains like cyber law.

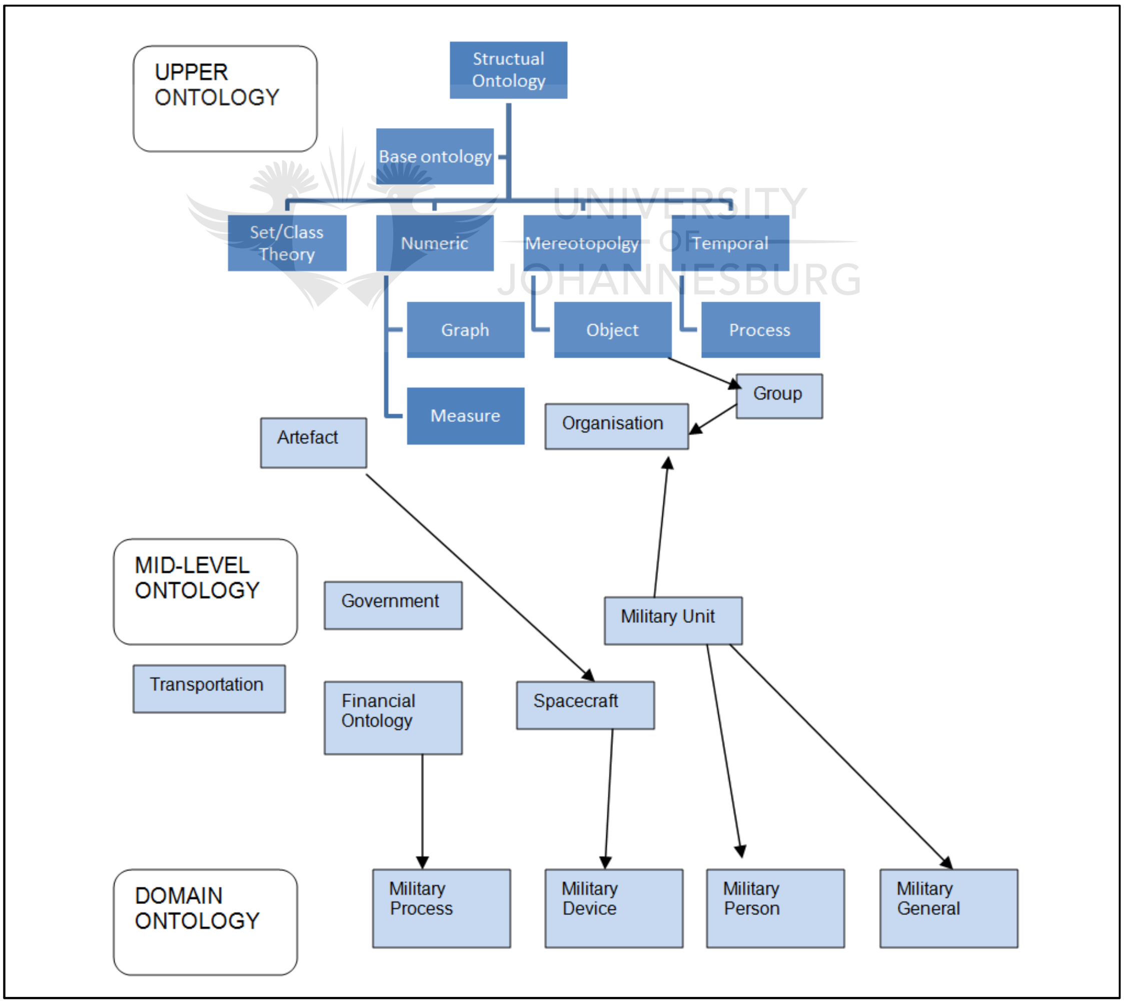


Figure 40: Example Ontology Hierarchy (Song, Ryu & Kim 2010)

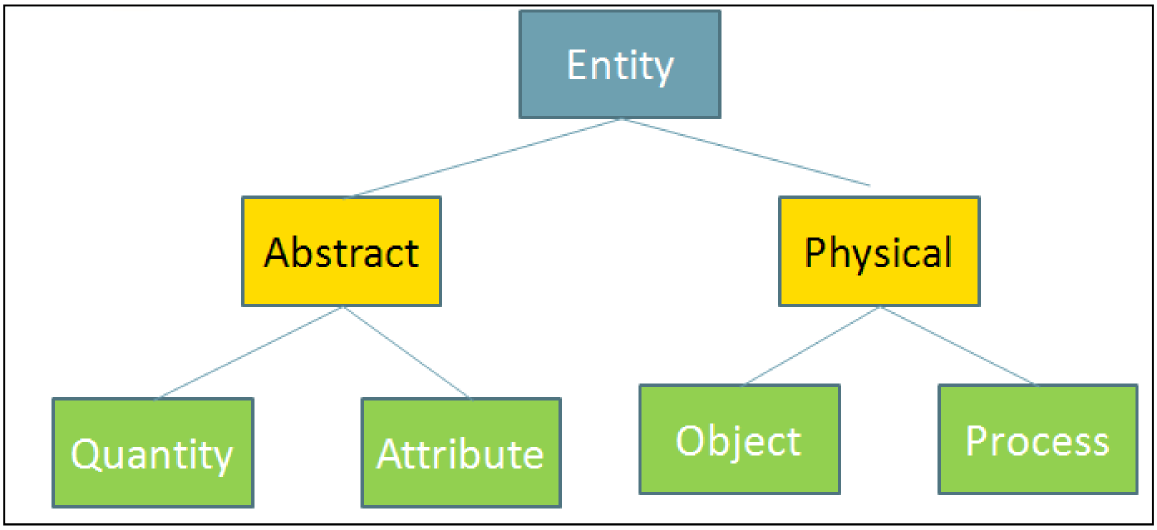


Figure 41: Example Upper Ontology (Sevcenko 2003)

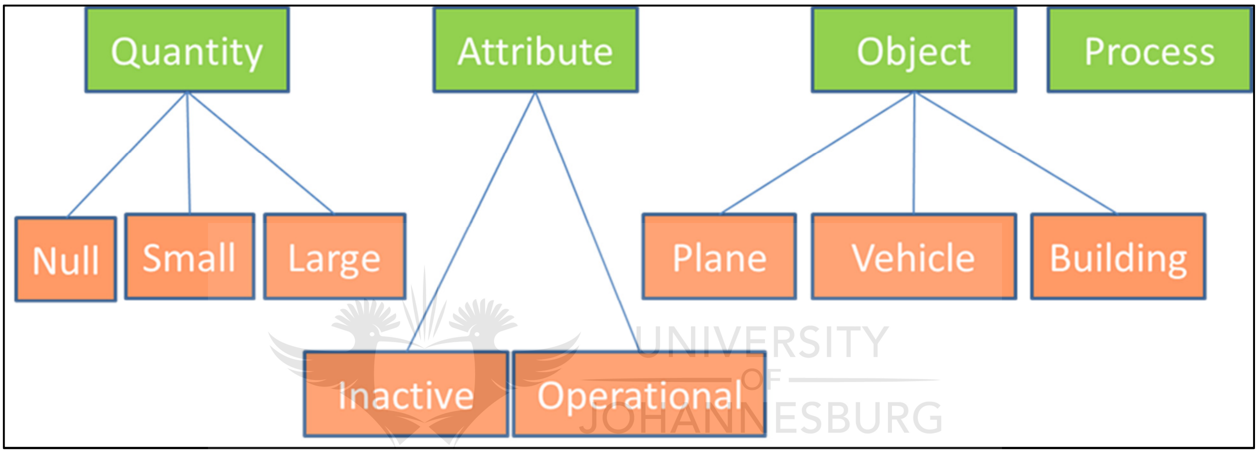


Figure 42: Example Core Ontology (Sevcenko 2003)

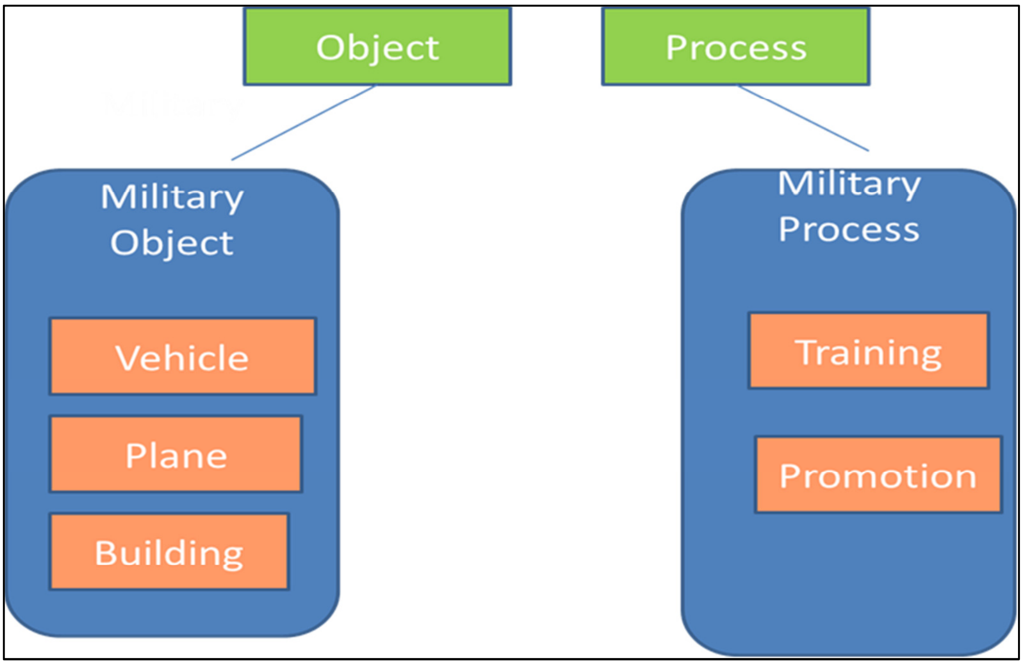


Figure 43: Example Domain Ontology (Sevcenko 2003)

Now that the type of ontology that cyberterrorism belongs to has been examined, the discussion moves on to the actual development of the ontology.

9.4 Classes in Cyberterrorism Ontology

Previous research by Van Heerden, Irwin and Burke (2012) was used as the basis for some of the underlying classes of the proposed cyberterrorism ontology. Van Heerden et al. proposed a Network Attack Ontology to classify computer-based attacks. Furthermore, Gordon and Ford (2002) in their terrorism matrix also classify attacks using a number of categories including Perpetrator, Action, Tool, Target and Motivation For the cyberterrorism ontology, the core classes of Actor, Effect and Motivation were adopted and modifications were made to address specific requirements within the field of cyberterrorism.

The main classes in the proposed cyberterrorism ontology are the Actor, Cyber Event, Objective, Motivation, Practice, Effect and Target. For example, every Cyber Event would have an Actor entity, Objective, Motivation, Practice, Effect and Target. The goal of the ontology (based on the initial taxonomy whereby the main concepts are defined) was to determine whether a CyberEvent could be classified as a Cyberterror or a SupportTerror, based on its specified attributes in the other classes. Before explaining the functioning of the main class CyberEvent, a discussion on the development of each of the classes follows. An outline of the Actor class is given next.

9.4.1.1 Actor

Due to the world of globalisation, different types of actors interact with each other, both malicious and harmless. From a cyberterrorist point of view, the types of actors in this ontology are the different types of attackers. While Gordon and Ford (2002) use the term Perpetrator, Van Heerden, Irwin and Burke (2012) refer to the term Actor. The term Actor was selected for the ontology as it is more neutral and does not assume guilt.

Van Heerden, Irwin and Burke (2012) formed the Actor Class for their Attack Classification Ontology as follows:

- Commercial competitor
- Hacker
  - Script kiddie hacker
  - Skilled hacker
- Insider
  - Admin insider
  - Normal insider
- Organised criminal group
- Protest group

Figure 44 shows the actor classes and sub-classes that were carried over from the Network Attack ontology (Van Heerden, Irwin & Burke 2012) to the Cyberterror ontology. In ontologies, classes and sub-classes have an “is a” relationship. For example, every class in Protégé is defined as being a “Thing” and thereafter sub-classes are assigned to classes.

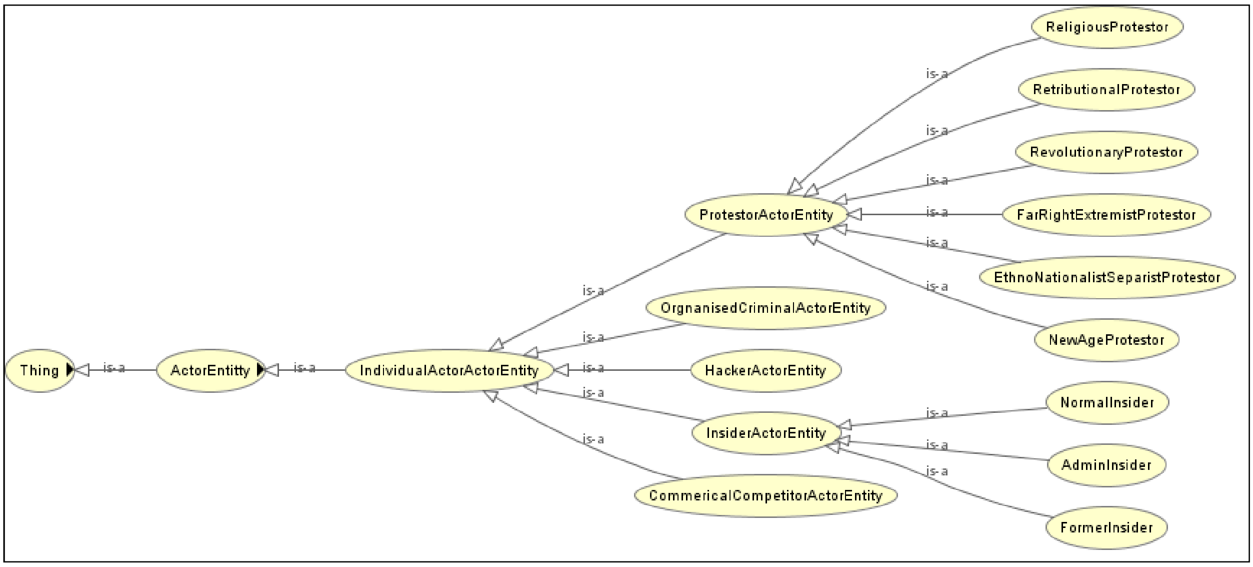


Figure 44: ActorEntity Class (Own Compilation)

The original class Protest Group was extended to include examples of the type of groups that correspond to terrorist activities and included Religious, Ethno-nationalist separatist, Revolutionary, Far-right extremist, New Age and Retributional (Veerasamy 2009b). The original Actor class was also adapted to cater for individual and group activities by defining the core actor entity as an individual and a group entity as consisting of a number of individuals. The importance of the hacker group is that hackers may not be as violent as serious cyberterrorists and just cause damage to computer systems (Matusitz, Breen 2011). In the next section, the possible effects are discussed.

9.4.2 Effects

Schudel, Wood and Parks (1999) in their paper on Modelling Behaviour of Cyberterrorists show that once an attack occurs, the damage is assessed. This will indicate whether the attack was successful or if more resources are available to take over after an attack. Assessing the damage will show the effect of a cyberterrorism attack. With reference to the definition established by the author (Section 3.3), cyberterrorism aims to create fear/shock, influence the government, intimidate the public or promote an ideological issue. In order to accomplish these objectives, the outcome of the attack needs to draw some attention and gain publicity. Therefore, attacks that have a significant result can only be considered as cyberterrorism.

Van Heerden, Irwin and Burke (2012) make use of the sub-classes Null, Minor, Major and Catastrophic in their Effects class of their Network Attack Ontology (see Figure 45).

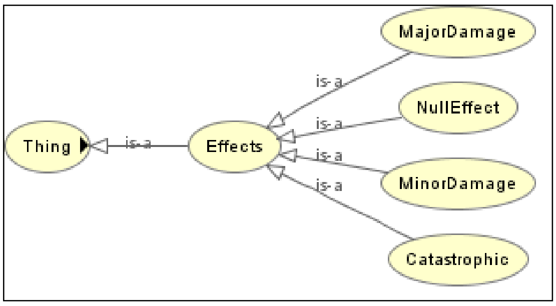


Figure 45: Effects Class (Own Compilation)

Explanations taken from Mirkovic and Reiher (2004) define "Null" as being no effect on the target, "Minor" refers to recoverable damage, "Major" indicates non-recoverable damage and “Catastrophic” entails damage of such a nature that the target can no longer operate as an entity, and potentially result in the declaration of bankruptcy. For this specific cyberterrorism ontology taxonomy, while the sub-classes were carried over, the definitions are adapted slightly:

- Null: no effect on target.
- Minor: recoverable damage to target (minimal financial implications and technical recovery required).
- Major: extensive financial or loss of reputation (more complex technical recovery required).
- Catastrophic: extensive damage such that the target failed to operate (massive damages - financial, technical and possibly life).

Now that the possible effects have been explored, the discussion moves on to an explanation of possible motivations.

9.4.3 Motivation

The Motivation class pertains to the high-level motivation or driving force of the actor. Often determining the motivation is subjective. However, a few high-level objectives have been identified from literature. Van Heerden, Irwin and Burke’s (2012) sub-classes for Motivation were Criminal, Ethical, Financial, Military and Recreational. Similarly, Gordon and Ford’s (2002) terms for motivation included Social and Political.

Denning (in Gordon, Ford 2002) talks about cyberterrorism being carried out to intimidate or coerce a government or its people to further political or social objectives. In addition, various terrorist groups are also strongly driven by religious beliefs, for example, Al Qaeda prescribes to the principles of Islam. Therefore, while ordinary criminals or attackers may not have political, religious or social motivations, cyberterrorists do have these types of driving forces. Additional sub-classes that were added to the Cyberterrorism ontology included Political, Social and Religious. (As mentioned in Section 3, the definition of cyberterrorism, the motivation may stem from political or ideological issues like religious, social or ethical beliefs.)

A summary of the motivation class is given in Figure 46. However, an actor may have a more specific objection that stems from the high-level motivation. The different types of objectives are discussed next.

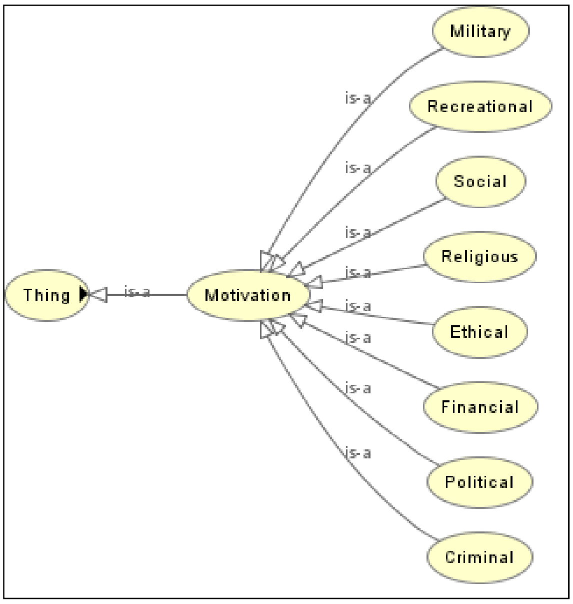


Figure 46: Motivation Class (Own Compilation)

9.4.4 Objectives

The Objectives class refers to the low-level purposes of the attack and is sub-divided into Malicious Objectives (correspond to cyberterror cyber events) and SupportTerror cyber events (correspond to a support activity). Based on previous research by Veerasamy (2009b) and Jenkins (2006), the Objectives class is divided as follows:

- Malicious or attack objective
  - Destroy
  - Disrupt
  - Force demands
  - Interfere
  - Intimidate
  - Kill or maim
  - Protest
  - Publicity
  - Steal
  - Terrify
- Support Objective
  - Finance
  - Intelligence
  - Logistics
  - Planning
  - Propaganda

  - Recruitment
  - Social services (provision of support to families of suicide attackers)
  - Training

Objectives are not mutually exclusive. For example, a religious terrorist could be trying to interfere in operations, as well as finance the terrorist organisation. Therefore, a terrorist could have multiple objectives. The classification of a Cyberterror Event or SupportTerror Event will also be influenced by the effect, practice and motivation. The defining requirements for a Cyberterror CyberEvent and SupportTerror CyberEvent are given in more detail in Section 9.4.7. The discussion now moves on to typical practices applicable to the cyberterrorist field.

9.4.5 Practices

Veerasamy (2009b) introduced some of the typical cyberterrorist practices as part of a framework covering influential factors in the field of cyberterrorism. These include the defacing of web sites, distribution of disinformation, spreading propaganda, Denial-of-Services using worms and viruses, disrupting of crucial services, corrupting of essential data, and stealing credit card information for funds. Furthermore, some of the uses of the Internet for cyberterrorism were classified as web literature, social-networking tools, anti-forensics and fundraising (Veerasamy, Grobler 2011). Based on the practices in literature, the Practices sub-class is structured as follows:

- Anti-forensics
  - Draft message folder
  - Encryption
  - IP-based cloaking
  - Proxies and anonymises
  - Steganography
- Data manipulation
  - Denial-of-Service
  - Infections (worm, Trojan or virus)
- Fundraising
  - Auctioneering
  - Casinos
  - Credit card theft
  - Donations
  - Drugs
  - Phishing
- Social networking
  - Applications

  - Blogs
  - Forums
  - Gaming
  - Music
  - Virtual personas
  - Websites
- Web defacement
  - Cross-side scripting
  - Standard Query Language (SQL) injection
- Web literature
  - Biographies
  - Encyclopaedias
  - Essays
  - Manuals
  - Periodicals
  - Poetry
  - Statements
  - Video

The list of practices is an indication of the range of practices that cyberterrorists typically utilise. Due to the growth of technology and digital capabilities, this list is not exhaustive and therefore can be extended as new practices are identified. Cyberterrorists usually have specific targets in mind when an attack is launched or in support of an attack. A discussion of the cyberterrorist targets follows.

9.4.6 Target

This class refers to the target of the cyber event or the type of system on which the event occurs. Gordon and Ford (2002) state that there are a large number of potential targets that involve, either directly or indirectly computers. In order to distinguish between a criminal activity, a small-scale incident, and a high-impact cyberterrorist event, the Target class is divided as follows (see Figure 47):

- Government or critical
- Individual
- Organisational

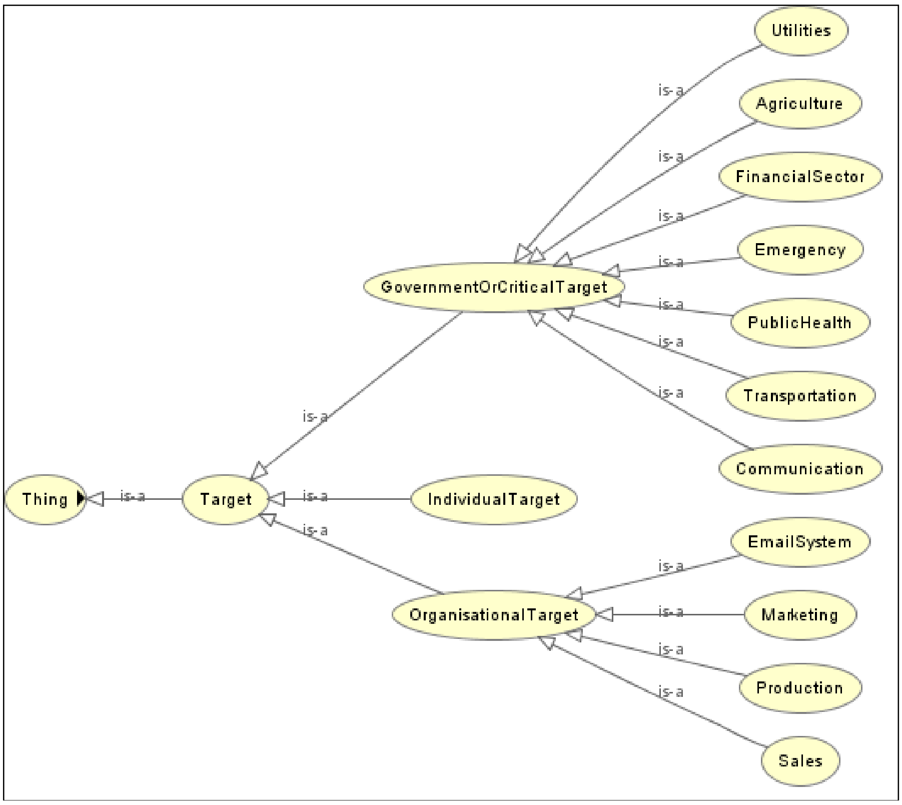


Figure 47: Target Class (Own Compilation)

For example, terrorists would target high-impact infrastructure, which would fall into governmental or organisational facilities. A virus affecting an unsuspecting single user's email address book would not be classified as cyberterrorism as cyberterrorists targets would seek to have a detrimental effect on a critical target. The various industries and services that fall within the government or critical sector are Agriculture, Communication, Emergency, Finance, Public Health, Transportation and Utilities (Veerasamy 2009a). Furthermore, critical systems in an organisation that would be a prime target for a cyberterrorist attack include email systems, marketing, production and sales.

The various classes in the ontology have been discussed. The discussion now moves on to an explanation of the main class CyberEvent that links the previously discussed classes.

9.4.7 CyberEvent

The CyberEvent class forms a critical aspect, as the aim of the overall ontology is to classify a cyber event as Cyberterror, a SupportTerror or as an unclassified OtherCyberEvent.

In Chapter 5, Framework for Cyberterrorism, it was shown that ICT infrastructure may not always be the target of an attack but can also serve a supporting role. Veerasamy (2009a) states that while many ICT based network devices and techniques may not always be used directly to carry out an attack; they can still provide support for communication, information gathering, planning and financial assistance. Thus, it is imperative to differentiate between a cyber event being an actual cyberterrorist attack, and a cyber event that provides technology support to terrorism in general.

In order to differentiate between a Cyberterror, SupportTerror and unclassified OtherCyberEvent, assertions were made in the ontology. The assertions relate to the motivation, objective, target, effect and practices.

With ontologies, the core assertions or defining attributes of classes need to be specified. The main class in the ontology is the CyberEvent class. Every CyberEvent could have more than one Actor, Objective, Practice and Target but only one Effect. The reasoning behind the assertion that a CyberEvent needs only one Effect, is that in order for a CyberEvent to be classified as Cyberterror it needs to have a major or catastrophic effect. For example, a cyberterrorist could be carrying out two activities simultaneously, fundraising and web defacement. The fundraising would be classified as a SupportTerror CyberEvent and the web defacement as Cyberterror CyberEvent. The fundraising may have a minor effect but overall the combined practices could have a major or catastrophic effect and the CyberEvent could be classified as Cyberterror CyberEvent.

Furthermore, in this ontology, the Cyberterror CyberEvent and SupportTerror CyberEvent attributes needed to be specified with detailed conditions in order for the cyber event to be correctly classified. To be classified as a CyberterrorEvent the following conditions were specified:

- The effect had to be major or catastrophic - terrorist attacks do not aim to have minor or null effect.
- The motivation had to be political religious or social - terrorists are primarily politically, religiously or socially motivated.
- The practice had to be data manipulation or web defacement - attacks usually constitute malicious behaviour like interfering with a web site of manipulating data using worms, Trojans or viruses.
- The target had to be an organisation, government or critical target as an attack on a minor individual computer or system would not cause terror.

To be classified as a SupportTerror CyberEvent, the event should have:

- A motivation that needed to be political religious or social - terrorists are primarily politically, religiously or socially motivated.
- A practice that had to be anti-forensics, fundraising or web literature - these are mainly practices that support terrorism support activities for recruitment, propaganda and planning.

Now that the various classes in the Cyberterror ontology have been introduced, this section is summarised briefly.

9.4.8 Overview of Ontology

The classes Actor Entity, CyberEvent, Objectives, Motivation, Practice, Effect and Target were identified to be the main classes in the Cyberterror ontology and form the basis for the development of the ontology. The discussion now moves on to the application of the ontology through the classification of individual cyber events.

9.5 Ontology Application: Classification of CyberEvent (Individuals)

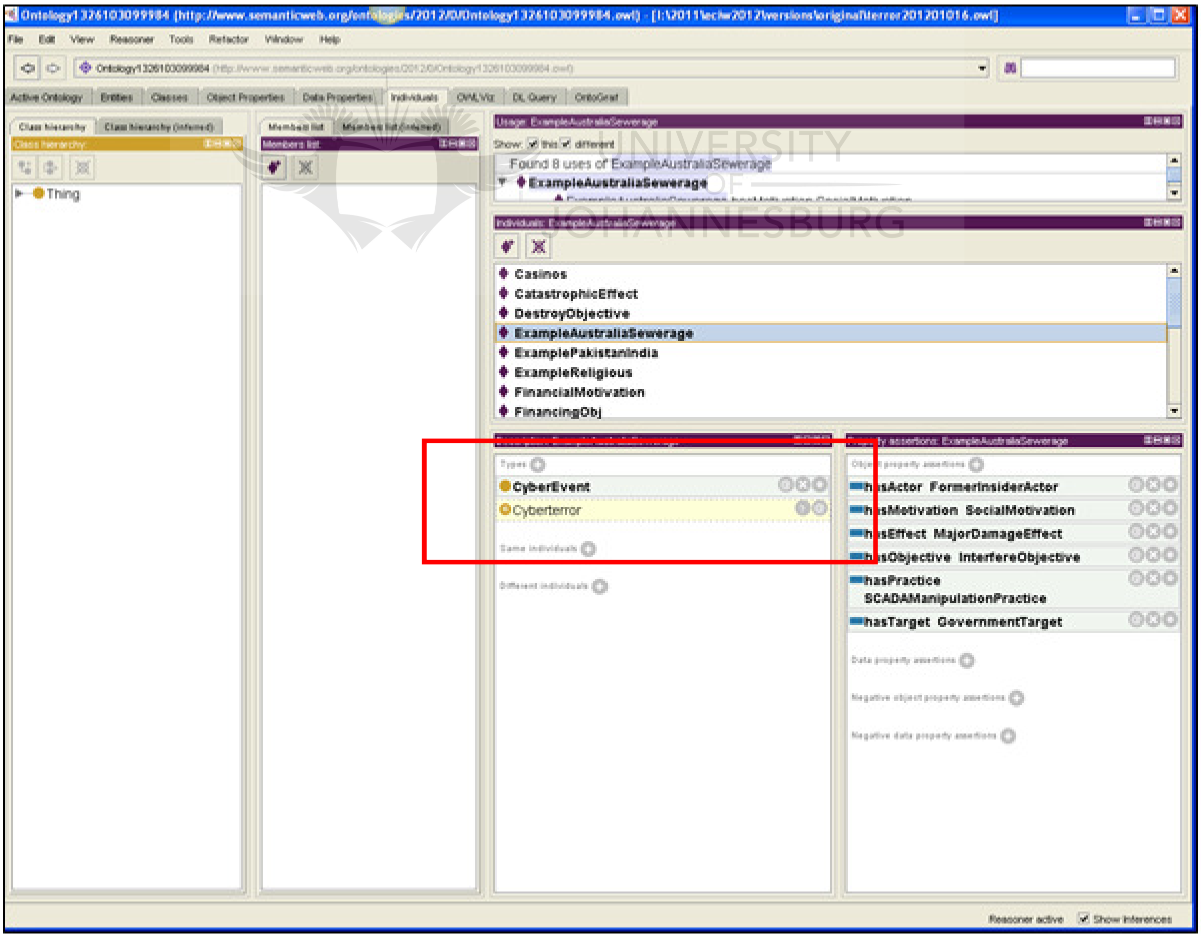
The description of the development of the ontology is given in the previous section. The main class is CyberEvent, which links all the other classes together. The CyberEvent class provides a means through which an event can be classified by the ontology as a Cyberterror, SupportTerror or OtherCyberEvent. Thereafter, individual examples can be instantiated with data and the reasoner tool in the ontology can be run in order to determine the cyber event's classification.

This section contains examples of individual-based incidents to show whether the reasoner can correctly classify the cyber event. Every cyber event has its own unique attribute specifications that would classify it as a Cyberterrorist CyberEvent, SupportTerror CyberEvent or an unknown OtherCyber Event. The attribute specifications of the individual cyber events are listed next.

9.5.1 Australian Sewerage Incident

Vitel Boden attacked the Australian Sewerage System in November 2001 (Lemos 2002). He was a former consultant on the project and after being refused a full-time position sought revenge. For this real-life example, the attribute specifications are as follows:

- Actor is a former insider.
- Motivation is social.
- Effect is major damage.
- Objective is a malicious objective of interfere.
- Practice is data manipulation (SCADA manipulation).
- Target is government or critical.


Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl) - [I:\2011\eciw2012\versions\original\terror201201016.owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl)
Active Ontology
Entities
Classes
Object Properties
Data Properties
Individuals
OWLViz
DL Query
OntoGraf
Class hierarchy
Class hierarchy (inferred)
Class hierarchy:
Thing
Members list
Members list (inferred)
Members list
Usage: ExampleAustraliaSewerage
Show: ☑ this ☑ different
Individuals: ExampleAustraliaSewerage
Property assertions: ExampleAustraliaSewerage
Types
Same individuals
Different individuals
Object property assertions
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner active
☑ Show Inferences

Found 8 uses of ExampleAustraliaSewerage

ExampleAustraliaSewerage

Casinos
CatastrophicEffect
DestroyObjective
ExampleAustraliaSewerage
ExamplePakistanIndia
ExampleReligious
FinancialMotivation
FinancingObj

CyberEvent
Cyberterror

hasActor FormerInsiderActor
hasMotivation SocialMotivation
hasEffect MajorDamageEffect
hasObjective InterfereObjective
hasPractice SCADAManipulationPractice
hasTarget GovernmentTarget

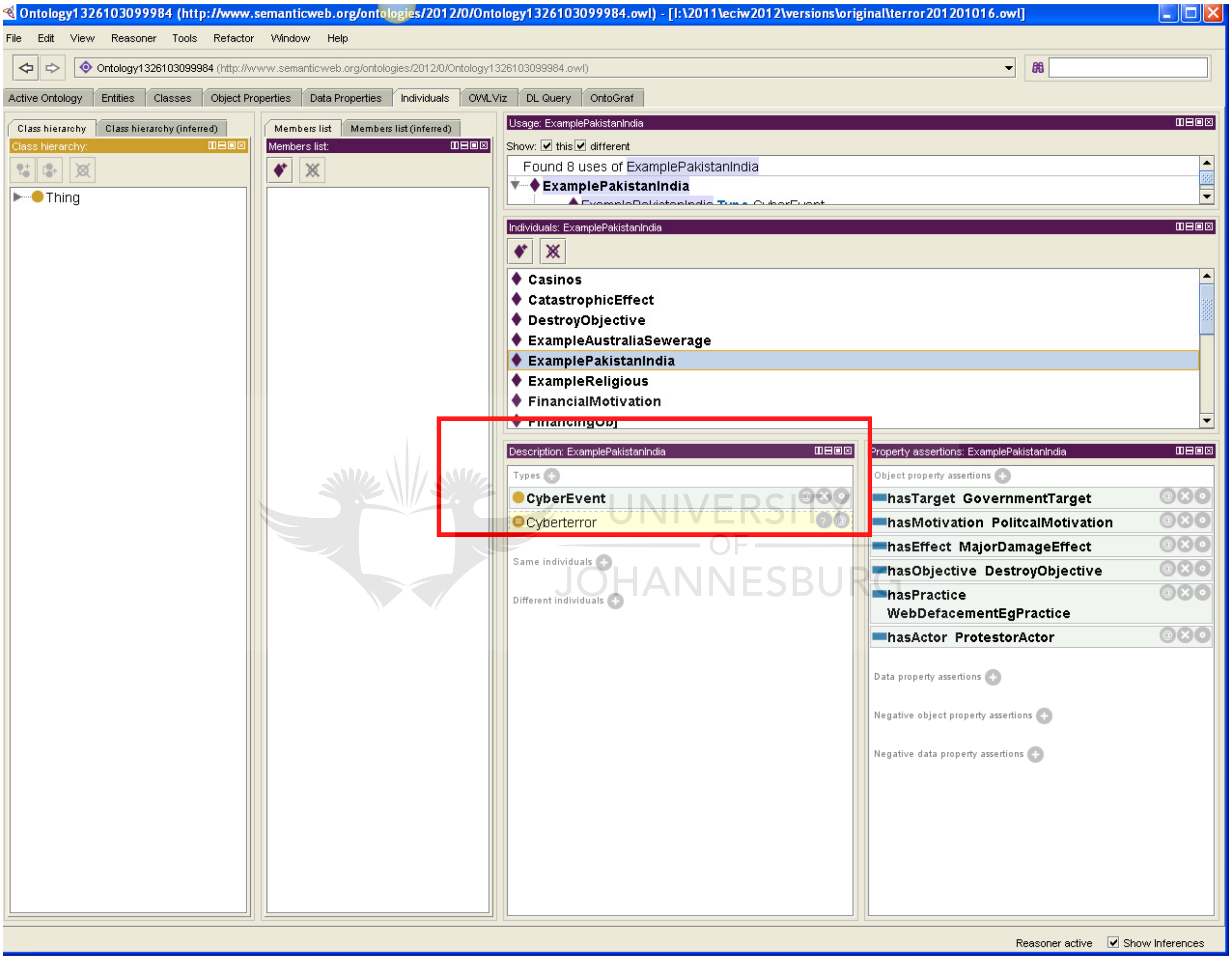
Figure 48: Classification of Australian Sewerage Incident (Own Compilation)

After the reasoner was run, it was inferred that the CyberEvent was of type Cyberterror (shown in Figure 48).

9.5.2 Pakistan India Example

The political conflict between Pakistan and India is represented in the ontology as follows:

- Actor is a protestor.
- Motivation is political.
- Effect is major damage.
- Objective is a malicious objective of destroy.
- Practice is web defacement.



Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl) - [I:\2011\eciw2012\versions\original\terror201201016.owl]
File Edit View Reasoner Tools Refactor Window Help
Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query OntoGraf
Class hierarchy Class hierarchy (inferred)
Class hierarchy:
Thing
Members list Members list (inferred)
Members list:
Usage: ExamplePakistanIndia
Show: ☑ this ☑ different
Individuals: ExamplePakistanIndia
Description: ExamplePakistanIndia
Types
Same individuals
Different individuals
Property assertions: ExamplePakistanIndia
Object property assertions
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner active ☑ Show Inferences

Found 8 uses of ExamplePakistanIndia

ExamplePakistanIndia

ExamplePakistanIndia Type CyberEvent

Casinos
CatastrophicEffect
DestroyObjective
ExampleAustraliaSewerage
ExamplePakistanIndia
ExampleReligious
FinancialMotivation
FinancingObj

CyberEvent
Cyberterror

hasTarget GovernmentTarget
hasMotivation PoliticalMotivation
hasEffect MajorDamageEffect
hasObjective DestroyObjective
hasPractice WebDefacementEgPractice
hasActor ProtestorActor

Figure 49: Classification of India/Pakistan Web Defacement (Own Compilation)

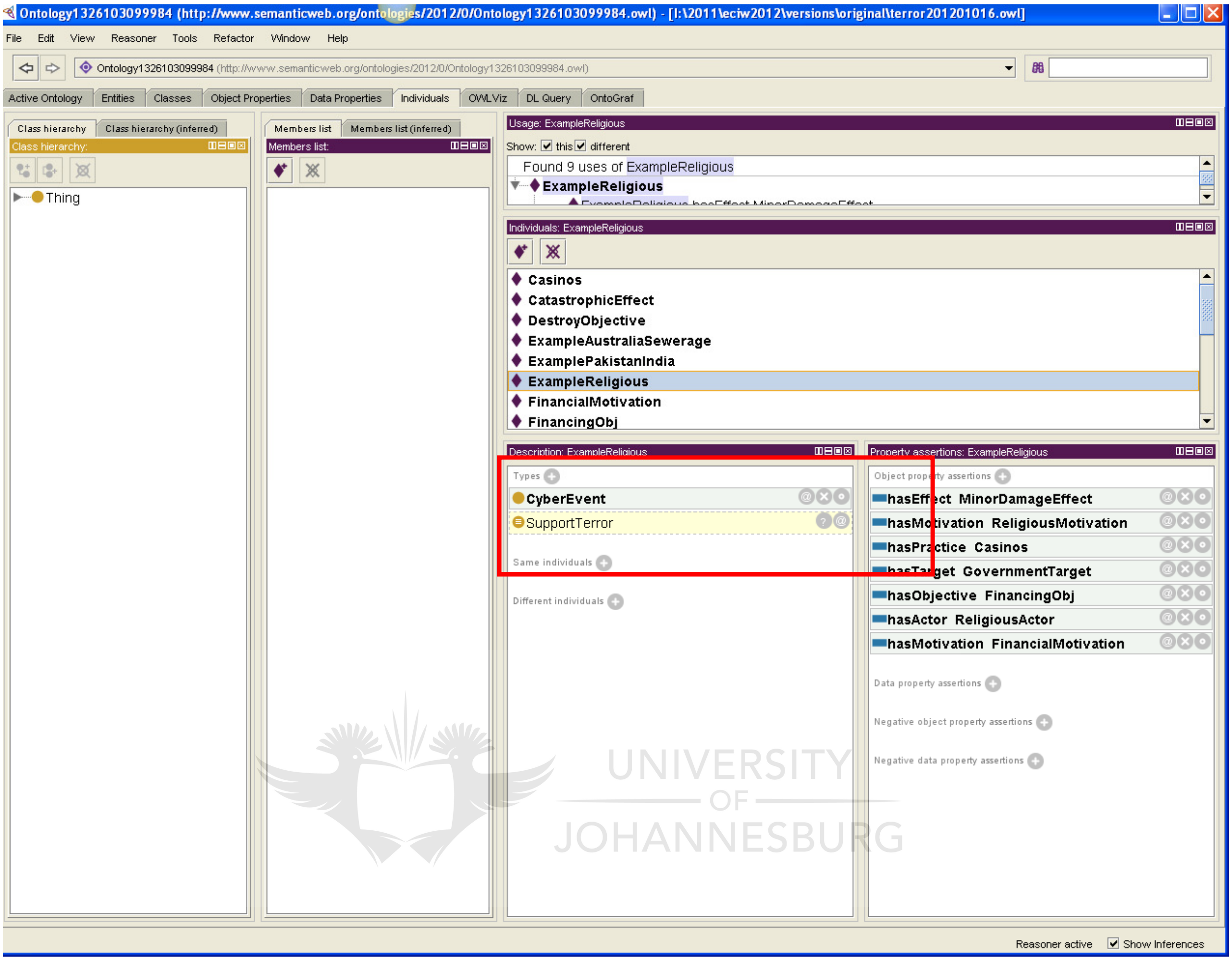
After running the reasoner, it was inferred that this example could be classified as a Cyberterror CyberEvent (shown in Figure 49).

9.5.3 Religious Example

Similarly, another example was set up to test for the deduction of Support CyberEvents as follows:

- Actor is a religious actor.
- Effect is minor damage.
- Objective is the support objective of finance.

- Motivations are financial and religious.
- Practice is casinos.



Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl) - [I:\2011\eciw2012\versions\original\terror201201016.owl]

Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl)

Usage: ExampleReligious

Show: ☑ this ☑ different

Found 9 uses of ExampleReligious

ExampleReligious

ExampleReligious hasEffect MinorDamageEffect

Individuals: ExampleReligious

- Casinos
- CatastrophicEffect
- DestroyObjective
- ExampleAustraliaSewerage
- ExamplePakistanIndia
- ExampleReligious
- FinancialMotivation
- FinancingObj

Description: ExampleReligious

Types

- CyberEvent
- SupportTerror

Same individuals

Different individuals

Property assertions: ExampleReligious

Object property assertions

- hasEffect MinorDamageEffect
- hasMotivation ReligiousMotivation
- hasPractice Casinos
- hasTarget GovernmentTarget
- hasObjective FinancingObj
- hasActor ReligiousActor
- hasMotivation FinancialMotivation

Data property assertions

Negative object property assertions

Negative data property assertions

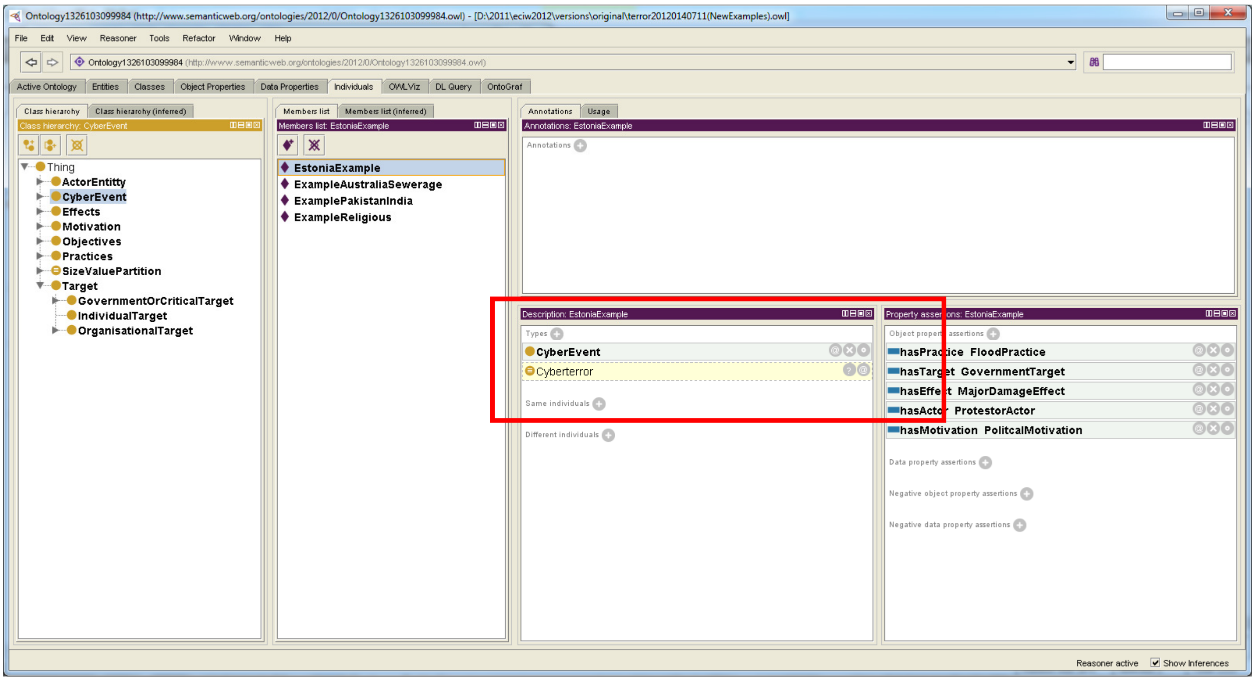
Reasoner active ☑ Show Inferences

Figure 50: Classification of Support Event (Own Compilation)

The inference engine in Protégé deduced that this example is a Support CyberEvent (shown in Figure 50).

9.5.4 Estonia Example

The flood of attacks on the Estonian governmental, news and broadcast web sites are encapsulated in the ontology as follows:


Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl) - [D:\2011\eciw2012\versions\original\terror20120140711(NewExamples).owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl)
Active Ontology
Entities
Classes
Object Properties
Data Properties
Individuals
OWLViz
DL Query
OntoGraf
Class hierarchy
Class hierarchy (inferred)
Members list
Members list (inferred)
Annotations
Usage
Annotations
Same individuals
Different individuals
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner active
☑ Show Inferences

Class hierarchy: CyberEvent

- Thing
  - ActorEntitty
  - CyberEvent
  - Effects
  - Motivation
  - Objectives
  - Practices
  - SizeValuePartition
  - Target
    - GovernmentOrCriticalTarget
    - IndividualTarget
    - OrganisationalTarget

Members list: EstoniaExample

- EstoniaExample
- ExampleAustraliaSewerage
- ExamplePakistanIndia
- ExampleReligious

Annotations: EstoniaExample

Description: EstoniaExample

Types

- CyberEvent
- Cyberterror

Property assertions: EstoniaExample

Object property assertions

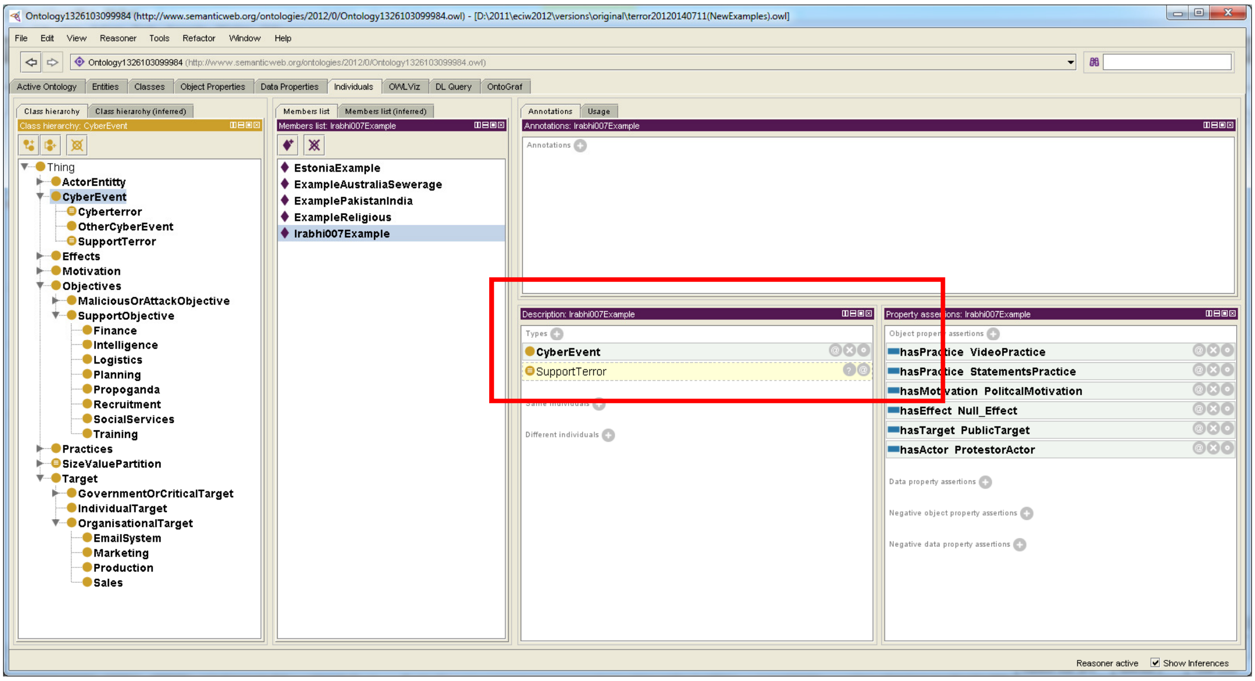
- hasPractice FloodPractice
- hasTarget GovernmentTarget
- hasEffect MajorDamageEffect
- hasActor ProtestorActor
- hasMotivation PolitcalMotivation

Figure 51: Classifcation of Estonian Attacks (Own Compilation)

- Actor is a protest actor
- Effects is major damage
- Motivation is political
- Objectives is disrupt
- Practice is flood (Denial-of-Service)
- Target is governmental

The results from the inference engine show that the incident is classified as Cyberterror.

9.5.5 Irabhi 007


Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl) - [D:\2011\eciw2012\versions\original\terror20120140711(NewExamples).owl]
File Edit View Reasoner Tools Refactor Window Help
Ontology1326103099984 (http://www.semanticweb.org/ontologies/2012/0/Ontology1326103099984.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query OntoGraf
Class hierarchy Class hierarchy (inferred)
Class hierarchy: CyberEvent
Thing
ActorEntitty
CyberEvent
Cyberterror
OtherCyberEvent
SupportTerror
Effects
Motivation
Objectives
MaliciousOrAttackObjective
SupportObjective
Finance
Intelligence
Logistics
Planning
Propoganda
Recruitment
SocialServices
Training
Practices
SizeValuePartition
Target
GovernmentOrCriticalTarget
IndividualTarget
OrganisationalTarget
EmailSystem
Marketing
Production
Sales
Members list Members list (inferred)
Members list: Irabhi007Example
EstoniaExample
ExampleAustraliaSewerage
ExamplePakistanIndia
ExampleReligious
Irabhi007Example
Annotations Usage
Annotations: Irabhi007Example
Annotations
Description: Irabhi007Example
Property assertions: Irabhi007Example
Same individuals
Different individuals
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner active
☑ Show Inferences

Types

CyberEvent

SupportTerror

Object property assertions

hasPractice VideoPractice

hasPractice StatementsPractice

hasMotivation PolitcalMotivation

hasEffect Null_Effect

hasTarget PublicTarget

hasActor ProtestorActor

Figure 52: Classification of Irabhi007 Web Publication (Own Compilation)

The publication of web literature by Irabhi 007 to influence the public is shown in the ontology as follows:

- Actor is a protestor
- Effect is null (no damage to systems)
- Motivation is political
- Objectives is web material (Propoganda)
- Practices is videos and statements
- Target is the public

This results in a classification of SupportTerror.

Note: This example does not refer to the terrorist practices later carried out by Irabhi007, but merely his inial activities to influence the public with web postings and video material.

9.5.6 Overview of Application

The ontology was set up to classify a cyber event as Cyberterror, SupportTerror or OtherCyberEvent depending on the details specified for its Actor, Motivation, Objective, Practice and Target attributes. Various examples can be instantiated in the ontology and therefore classified. The video on the accompanying CD shows the compilation of the various specified classes, the running of the reasoner and the classification of the examples in this text. The video captures the specification of the classes and their attributes, together with the instantiation of the first examples (known as Individuals in Protégé) together with the results from the reasoner.

9.6 Conclusion

This chapter proposed the use of ontologies to clarify the field of cyberterrorism. It is relevant as it aims to classify a cyber event as a being a cyberterror attack or a support practice. The other attributes in the ontology also show the dynamic use of ICT by terrorist groups in manipulating systems to their advantage.

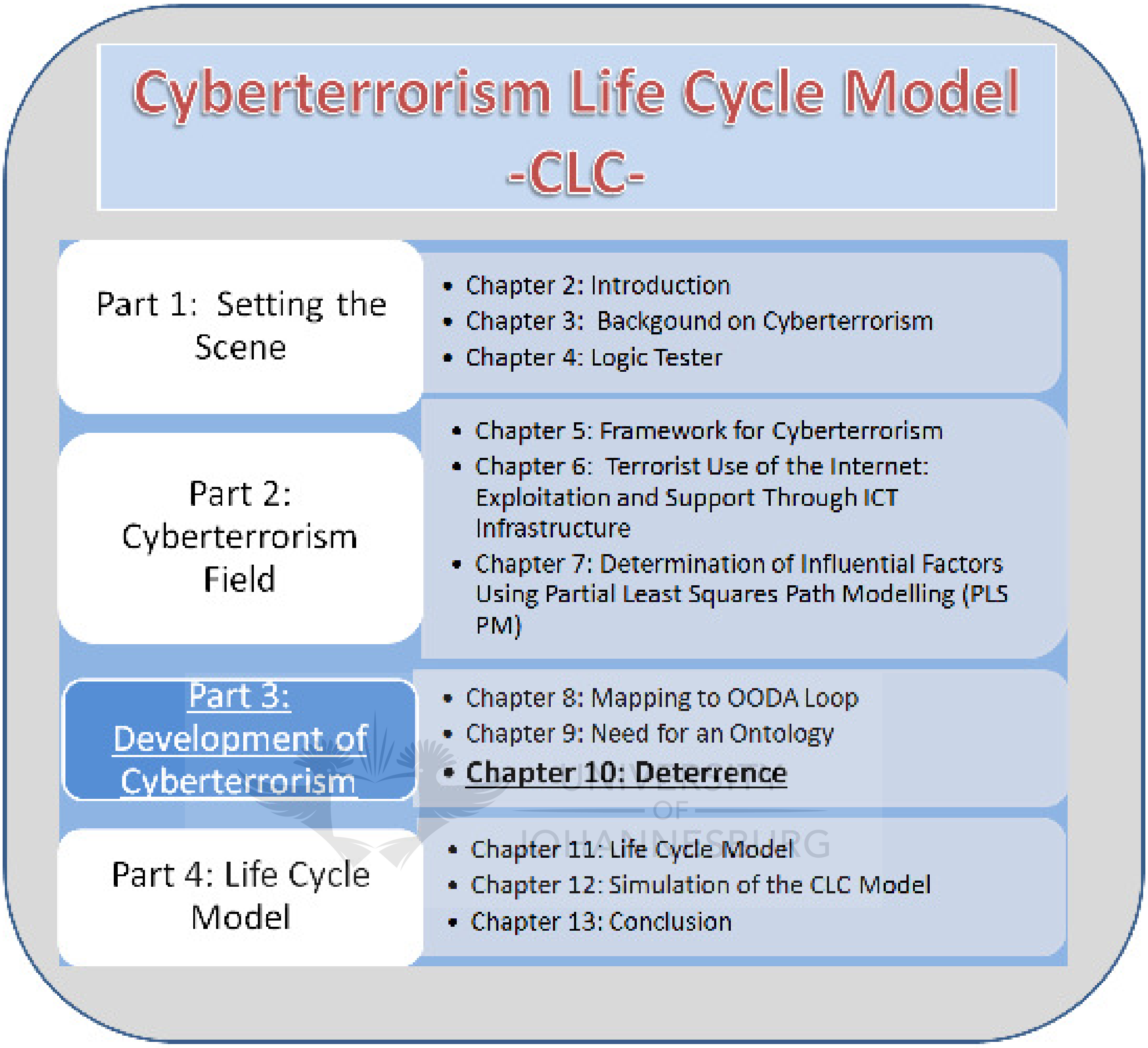
In summary, the compilation of an ontology was useful for classifying and structuring the field of cyberterrorism. The essential attributes that define and contribute to the field were captured, together with their core relationships. The following points were derived from the compilation of the ontology in this chapter that would contribute to the development of the CLC model:

- An actor is needed to initiate and execute an action. The following types of actors were identified: commercial competitor, hacker, insiders, criminal, and protestor. This classification is based on certain capabilities that the actor possesses. In order to capture this idea, the actor concept would be reflected in the capabilities element of the CLC model (Section 9.4.1.1).
- Cyberterrorism is often mistaken as any cybercrime event. However, in the ontology, the following concepts are introduced based on the motivation, objective, effect, target and practice: a cyber terror attack, support function and an unknown cyber event. The CLC model should cater for the different types of objectives and practices (Section 9.4).
- A cyber event can have different targeted effects, which are null, minor, major or catastrophic damage. The CLC model will show the effects that a cyberterrorist are trying to achieve depending on a malicious objective or support function (Section 9.4.2).
- In order to separate traditional cybercrimes from cyberterrorism, a key aspect is the motivation. The ontology shows motivations that correspond to cybercrime in general (criminal, ethical, financial, military and recreational) and those that relate to cyberterrorism (political, social and religious). The CLC model will specifically capture the motivations relating to cyberterrorism (Section 9.4.3).
- Cyberterrorism practices were previously broadly placed into groups to show the type of activities that are carried out. These include web literature, anti-forensics, fundraising, and social networking. Further practices that were identified and classified include web defacement and data manipulation. A broader range of cyberterrorism practices will be covered in the CLC model (Section 9.4.5).
- The types of cyberterrorist targets were classified in the ontology in order to distinguish between low-profile individual attacks and wider-spread government or organisation targets. The various targets identified in the framework in Chapter 5 were placed into the governmental and critical targets category. Examples in the organisational targets group are email, production sales and marketing systems. The range of targets would be specified in the CLC model (Section 9.4.6).
- In order for a cyber event to be classified as cyberterrorism the effect has to major or catastrophic, the motivation has to be political, religious or social, the practice has to data manipulation or web defacement and the target should be an organisation, government or critical target. The requirements for a cyberterror attack will be shown in the CLC model (Section 9.4.7)

- A support event needs a motivation of politics, religion or social issue and the practice can fall into the group of anti-forensics, fundraising, web literature and social networking (Section 9.4.7).

The attributes shown in the proposed ontology do not solely represent the only characteristics of a cyberterror attack but rather represent an abstraction of the most important considerations. By combining the ontology with other classification and development models, a better understanding of cyberterrorism can be gained. Later on, it is envisaged that the ontology proposed in this chapter will contribute to the development of the life cycle model. The chapter thus provides practical insight into the communication and intimidation methods used by terrorists over cyberspace.

In this chapter, further clarification was provided of the core attributes defining the field of cyberterrorism. Further analyses was carried out to classify and extend some of the attributes. Now that the field has been more formally structured, the discussion moves onto a presentation of countermeasures to curb the threat of cyberterrorism.



Cyberterrorism Life Cycle Model

-CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- **Chapter 10: Deterrence**

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

10 Deterrence of Cyberterrorism

> *"Our arsenal must also include tools that protect cyber and energy networks, halt the proliferation of weapons of mass destruction, counter threats of terrorism and destructive ideologies"*
>
> *- Hilary Clinton US Secretary of State*

Part 1 and 2 discussed various contributing drivers in the field of cyberterrorism and looked at structuring the field through various models. While cyberterrorism can be carried out through the execution of technical security exploits, it is essentially driven by differing social, ideological, political or religious views. Another objective of this study is to look at how cyberterrorism can be deterred through technical and strategic countermeasures. This chapter therefore, presents an overview baseline model to develop a countermeasure strategy. This chapter provides a high-level overview of the battle against terrorism and creates awareness of countermeasures that can be used to combat cyberterrorism. Figure 53 shows the current focus of this chapter.

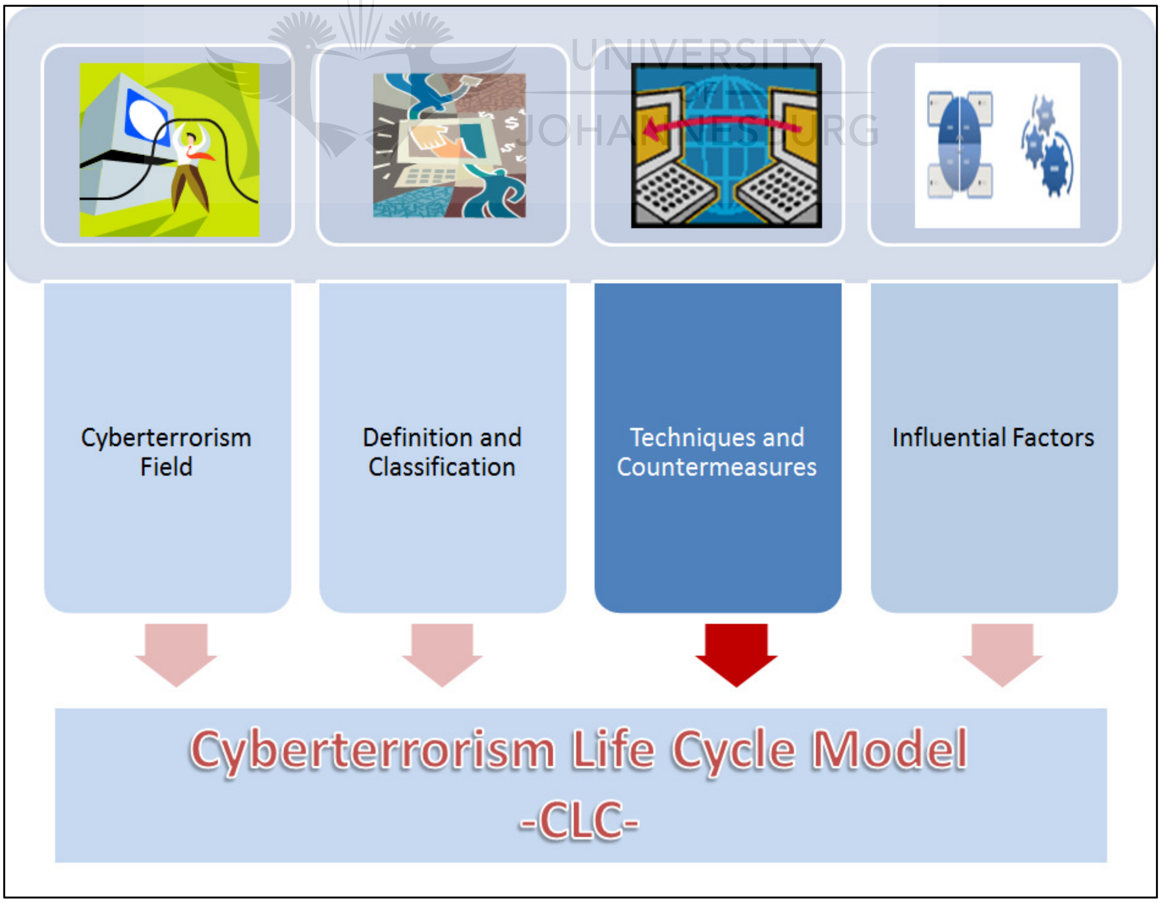

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 53: CLC Model Focus Chapter 10 - Cyberterrorism Consideration of Countermeasures (Own Compilation)

10.1 Background

Imperative to the deterrence of cyberterrorism is the understanding of what drives cyberterrorism, as well as the development of a strategy to change or influence the ideas and philosophy that are intrinsic to certain cultures and tribal groups. This is by no means a trivial task but requires extensive efforts to gain access to turbulent areas in the world. The significance of the social factors that influence the development of terrorism must be considered. Social factors relate to the surroundings and conditions that individuals are brought up in and include beliefs, culture, political views, as well as the personality traits that may lead to conformant or defiant behaviour.

Weimann (2004) explains that since society has become increasingly dependent on information technology, a new vulnerability has been created, with the potential risk of terrorists following the lead of hackers, resulting in a crippling effect on critical sectors like the military or financial services. The use of unconventional war techniques other than firepower has now evolved to include the domain of cyberspace. The threat, however still stems from social, political, economic, ideological and religious roots and therefore thought should not only be given to the technicality of the attack and defence methods but to influencing the behaviour and thinking patterns of insurgent groups.

Gangs, tribes, political parties, activist, religious and ethnic groups hold tremendous power in their communities of interest. Terrorism blurs the lines between civilians and the military. Therefore, the need arises to consider the high-level influence and shaping of opinions in order to deter the development of cyberterrorism.

Cyberterrorism stems from two areas: terrorism and technology. Accordingly, countermeasures need to address the issues from both perspectives. In some cases, issues cross over. For example, the establishment of cultural centres could affect both religious and social opinions. Another example is treaties and policies have both legal and political consequences.

Terrorism responses are for the most part reactive. When a bomb explodes in a market square, medical teams respond to the injured. Investigations are carried out after the event to determine the sequence of events that led to the explosion. However, proactive measures would offer better chances of combating cyberterrorism. Therefore, this chapter looks at a number of countermeasures from both a preventative and reactive point of view. The countermeasures are explained from the context of the law, religions, social conditions, economics, politics, and technical considerations. In the next sections a detailed discussion follows.

10.2 Cyberterrorism Countermeasures: Strategic Perspective

From the strategic perspective, cyberterrorism countermeasures can be considered in five broad categories: legal, political, economic, social and religious. Figure 54 shows a representation of these categories together with examples, which overlap categories in some cases. A discussion follows on the findings, which led to the compilation of Figure 54.

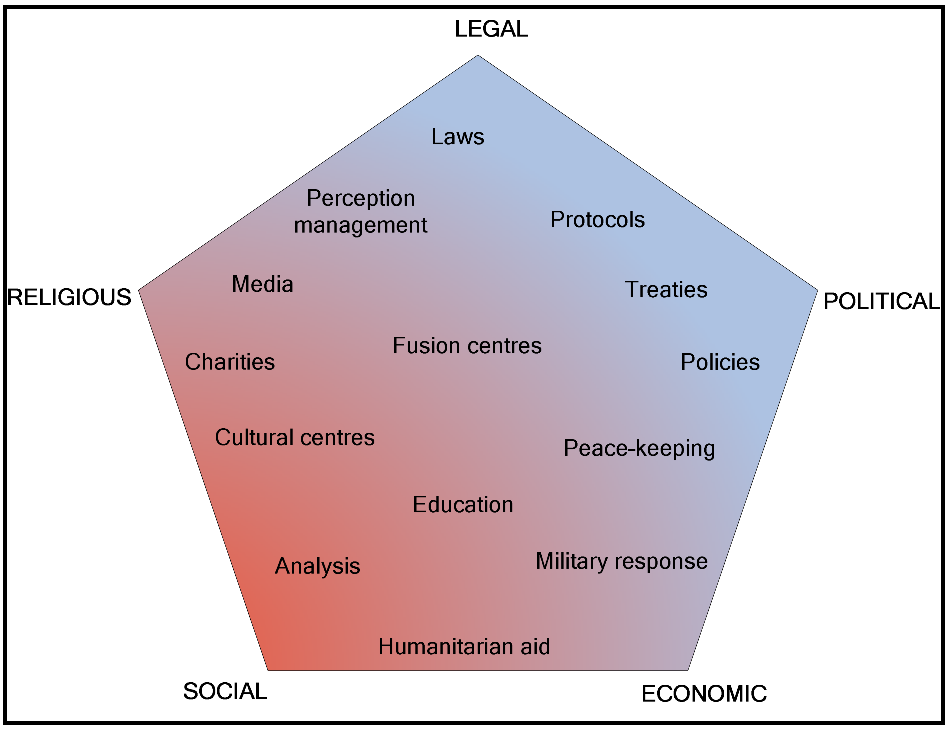


Figure 54: Counterterrorism Measures from a Strategic Perspective (Own Compilation)

10.2.1 Laws, Treaties, Protocols, Policies and Military Response

Firstly, Cronin (2002) explains that the major focus areas for terrorism response should be law enforcement and military responses. Furthermore, the South African Information Warfare Course promotes the establishment of treaties, protocols, regulations and acts of law to ensure the just and fair conduct of relations between nations (Williers et al. 2005/06). Laws can state that violence is an unacceptable form of protest demonstration and aim to deal with political and religious fanaticism more consistently. The government needs to maintain some type of public assurance that security will be enforced using policies and laws. These critical foundational blocks signal to the public that control and order will be upheld. An international presence from organisations like Interpol and the Council of European Convention on Cybercrime (who formed the first international treaty against cybercrime) can play a significant role in the combat against cyberterrorism (Elmusharaf 2004).

In extreme cases that an uprising or attack occurs, military force may be used to retaliate against attacks or enforce security. Groups could resort to hiding and carrying out operations from underground locations. Military force may be required to prevent plots against the government, which may entail attacks on critical infrastructure. The infiltration of a hierarchical group is no longer a viable option as members can operate remotely from anywhere and target the control systems of critical services like power or emergency services.

Cronin (2002) disputes that military force can only be effective if it forms part of a multi-faceted campaign that also includes social, economic, legal and political issues.

10.2.2 Fusion Centres, Charities and Humanitarian Aid

Wilson, Wilcox and Richards (2005) explains the concept of fusion centres consisting of intelligence, security personnel, political military specialists, cultural specialists, linguists, media relations engineers, psychological operations (PSYOPS), and economic advisors who can collect, process and analyse data for the definition of actions in specific regions. Furthermore, Wilson et al. (2005) also states that humanitarian aid and peacekeeping can assist with battle needs. Williers et al. (2005/06) concurs that providing assistance to people who suffer from famine, violence, political repression and natural disasters can significantly help with conflict resolution. Charity can create positive reactions through the provision of money, food, fuel, education, medication and job creation as this helps alleviate suffering in impoverished areas.

10.2.3 Cultural Centres, Perception Management, Media and Analysis

Cultural centres and perception management through the media try to discourage fanatical religious and political beliefs in affected areas. De Borchgrave, Sanderson and Harned (2007) claim that that extremists may be active in recruitment at charity and cultural centres but may also listen to the teachings from inspirational speakers. Therefore, using operatives at such centres can be helpful in identifying potential extremist recruiters.

Analysis at various levels is required to increase intelligence capabilities. Analysis capabilities includes studying forensic data, identification of patterns, links, analysing cultural, tribal, religious and communications-linguistics (Wilson, Wilcox & Richards 2004). Overall, intelligence efforts can be increased though fusion and cultural centres that look for emerging news and optimistically can provide insight into the sometimes-volatile behaviour of terrorist groups.

With regard to international collaboration, Jensen, Gordon and Spalding (in De Borchgrave, Sanderson & Harned 2007) make the following comments in a report by the Centre for Strategic and International Studies in order to aid analysis efforts:

- There needs to be greater co-operation between agencies and the highly specialised intelligence agents placed in the field.
- When information is lacking, the public may speculate. This can be quite dangerous if information is not relayed to the public. To prevent this, the media and the public have a vested interest in informed sharing of analysed data. There is a strong need for greater international collaboration, specifically via the European Union.
- Similar to the USA, the community and academia need to interact regularly to ensure information sharing and exchange.
- The location of the terrorist act should be noted. Thus, support can be raised for an environment experiencing political or extremist instability.
- Reading the mail of convicted terrorists can help identify potential crimes. For example, the three criminals who were involved in the 1993 World Trade bombing, whilst imprisonment at the federals highest security prison exchanged around 900 letters with extremists between 2002 and 2005 including terrorists in Spain.

Overall, the war on terror strongly entails influencing people’s ideas, viewpoints and beliefs. However, for cyberterrorism this issue also requires the deployment of protection, detection, and reactions mechanisms at a technical level. The next section addresses the combat of cyberterrorism from a technical perspective.

10.3 Cyberterrorism Countermeasures: Technical Perspective

Carr (2007) has stated that the use of the Internet and web-based software applications has become a growing phenomenon among extremist groups. According to the article “Cyberterrorism on the rise” at Mybroadband.co.za (2010), terrorists are showing a clear interest in hacking skills and using real attacks together with cyber attacks. In order to fight against sophisticated cyberterrorists electronically entering computer systems, which control life critical systems like dams or air traffic, it is essential to make use of technical countermeasures. Wreaking havoc with critical infrastructure affects national security and therefore technical countermeasures are essential to combatting these types of attacks. Weimann (2005a) has stated that “the more technologically developed a country is, the more vulnerable it is to cyber attacks aimed at targeting its infrastructure".

Technical cyberterrorism countermeasures can be categorised into six groups: Computer Security Incident Response Team (CSIRTs), intrusion prevention, network monitoring, interception and blockage, disaster recovery and forensics. Figure 55 shows a summary of these countermeasures. A discussion follows on the findings, which led to the compilation of Figure 55

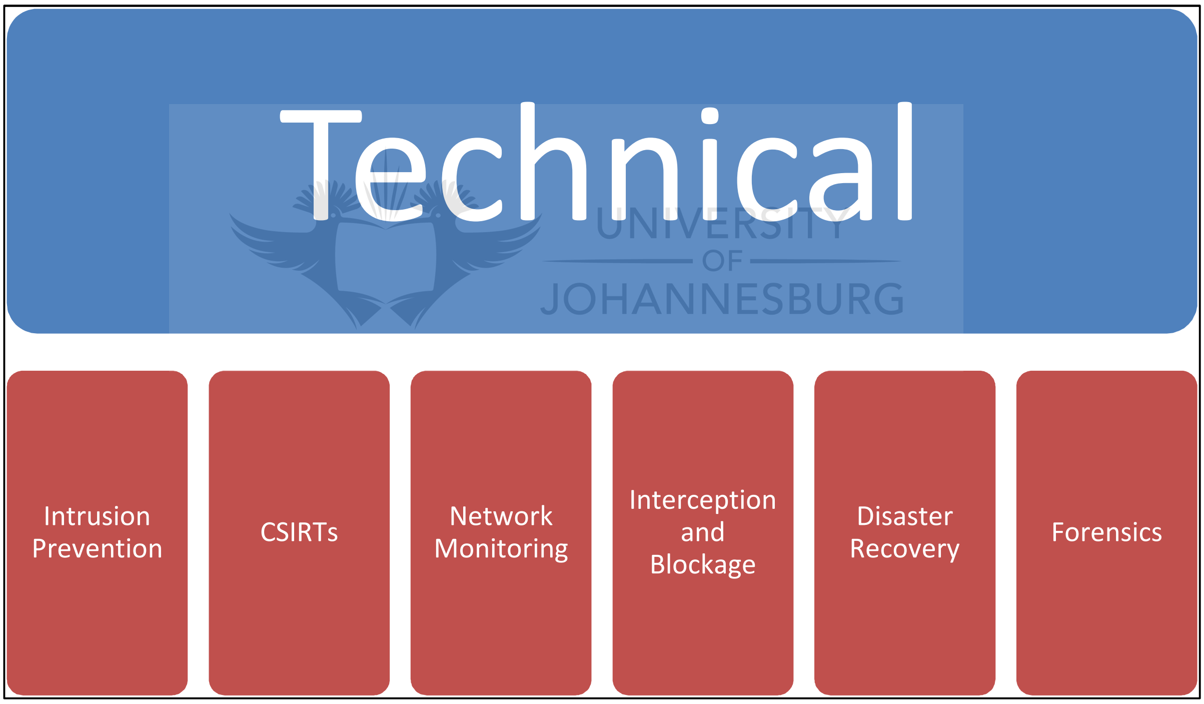


Figure 55: Technical Counterterrorism Measures (Own Compilation)

10.3.1 Intrusion Prevention

Due to unique conditions of a cyberterrorism attack, countermeasures can be developed at proactive, detective and reactive level. To elaborate, cyber attackers usually follow a similar strategy to that of traditional warfare. Initially, the target is spied on to identify any vulnerabilities. Thereafter, the vulnerable points are probed to gauge whether access can be granted. The identification of vulnerabilities and probing for access is based on various elements of the technology, implemented policies, procedures and behaviour of the system users. The actual attack is aimed at the intrusion and destruction of the infrastructure and systems (Ho 2008). Proactive countermeasures entail the implementation of specific measures to prevent a cyberterrorism attack. Detective countermeasures entail the implementation of specific measures to detect a cyber attack or a potential cyber attack. Reactive countermeasures will entail the implementation of specific measures to deal with a cyberterrorism attack while it is occurring to prevent further damage or post the attack to get the victim system operational again.

Intrusion prevention relates to the provision of proactive technical countermeasure to deter cyberterrorism. An intrusion refers to *"any intentional event whereby an intruder gains access in order to compromise the confidentiality, integrity, or availability of computers, networks, or resident data "* (Hansen et al. 2007). Intrusion prevention aims for proactive protection of equipment like computers from attacks to its programs, applications and data, which essentially threaten the operation of the critical systems it runs. The main differences between intrusion detection and intrusion prevention are the security mechanisms that are implemented to prevent any intrusions before the system is violated, and without influencing the system's functionality (Rrushi 2006). It also prevents a computer from being infiltrated by automated malware or intrusion scripts by a terrorist group. A machine once infected can also become a pawn in carrying out other attacks. Bots or zombies can launch attacks on other machines and are often involved in Denial-of-Service attacks that cause systems to crash and lose availability. Intrusion prevention mechanisms are thus aimed at the prevention of terrorist spying and uncovering of system vulnerabilities. Since standard security control techniques are known to be fallible, both intrusion prevention and intrusion detection are indispensable (Hansen et al. 2007).

10.3.2 CSIRTs

Another form of countermeasures is Computer Security Incident Response Teams (CSIRTs). CSIRTs are equipped to provide proactive and reactive security services that can be used against cyber attacks like cyberterrorism. Proactive services provided by CSIRTs include information and assistance to prepare, protect and secure systems in expectation of possible attacks or future problems. By performing proactive services, the number of incidents in the future can potentially be reduced. Other services offered by CSIRTs include security announcements (intrusion alerts when locally detected or from partnered international alliances, vulnerability notices and security advisories), technology watch (publication of emerging technical developments and trends) security audit reports, security tool releases and the dissemination of other security-related information. Reactive services may include alerts and warnings, the handling of incidents vulnerabilities and artefacts (CERT 2002). Each CSIRT provides for a range of services that are dependent on the funding and constituency capabilities of the hosting organisation and sponsors.

10.3.3 Network Monitoring

An example of a detective countermeasure is network monitoring. A series of network attacks at the State, Commerce, Defence and Homeland Security departments led to US president Bush signing a directive in January 2008 that expanded the role of the intelligence community in monitoring Internet traffic (Nakashima 2008). Federal agencies computer systems were authorised to be monitored by the National Security Agency. This was aimed at curtailing the onslaught of attacks on federal agencies computers.

10.3.4 Interception and Blockage

Both network monitoring and interception can be beneficial, in that it can track the number of times a specific entity is mentioned or referred to in electronic communications. When suspicious behaviour is detected through either network monitoring or interception, that specific website, IP address or port can be blocked as an effective countermeasure. A network may experience undesired data traffic (virus, rogue code or attack) and accordingly there exists the need for systems to filter and/or prevent undesired data communication (Jackson 2003).

10.3.5 Disaster Recovery

The risk of cyber attacks and potentially cyberterrorism should definitely be covered in a country/organisation's disaster recovery/business continuity plan. As a minimum requirement, contact information for technology service providers should be listed to assist a country/organisation in recovering from a cyber disaster (Mortman 2009). Furthermore, procedures should also be put in place to restore backups or return systems to a level of basic operation.

10.3.6 Forensics

After a cyber attack has occurred, forensic investigations will try to piece together the sequence of events and identify evidence of the perpetrator. Initial forensic investigations entail cyber first responder (CFR) procedures. CFRs are trained to effectively and efficiently respond to any type of cyber-based terror attack carried out across the Internet, communications and network-based infrastructure (Cyberterrorism Defense Initiative 2010). Actions by CFRs are reactive in nature and will entail the collection of evidence for further investigation of the actual cyberterrorism attack. Matusitz (2013) explains that computer forensics is a way of improving investigation into crimes that use computers, computer-aided terrorism, cyberterrorism and espionage.

10.4 Conclusion

This chapter addresses a number of useful countermeasures that can aid the fight against cyberterrorism. This chapter summarised various political, religious, legal, economic, social and technical issues that can help establish a solid foundation of security control and implementation. Various countermeasures were proposed and included laws, policies, fusions centres, treaties, education, the use of the media and perception management. At technical level, countermeasures can include activities like CSIRTs, network monitoring, interception and blockage. The effectiveness of strategic countermeasures is difficult to evaluate as it requires political, cultural, economic and religious collaboration. However, strategic countermeasures strive to deter interest in terrorism and therefore its value, while hard to quantify is still a valuable contribution. Technical countermeasures have metrics like violations count, number of forensic investigations, number of interceptions and system downtime before recovery.

In summary, various countermeasures can be used in the combat of cyberterrorism. The following drivers made in this chapter contribute to the CLC Model and include:

- Countermeasures need be devised from a strategic and technical point of view. The CLC model will reflect this requirement (Section 10.1).

- Strategic countermeasures can be grouped as legal, political, economic, social and religious categories. This will be shown in the CLC model (Section 10.2).
- Examples of countermeasures cannot be strictly be classified to belong to a single category. For example, the establishment of cultural centres, which promotes the understanding of religion and culture while exposing visitors to outside opinions, can be considered as both a social and religious countermeasure. The CLC model will show the overlapping classification of countermeasures (Section 10.2).
- Other examples of strategic countermeasures include: media, charities, cultural centres, analysis, education, humanitarian aid, military response, peacekeeping, policies, treaties, protocols, laws, perception management and fusion centres. The range of countermeasures will be captured in the CLC model (Section 10.2).
- Technical countermeasures include: CSIRTs, intrusion prevention, network monitoring, interception and blockage, disaster recovery and forensics. These technical countermeasures will form part of the CLC model (Section 10.3).

Cyberspace has emerged as a new target through which terrorists can cause disorder and thus influence the psyche of communities. Cyberterrorism stems from its political, social or religious reasoning that tries to justify violent and extremist behaviour. To execute cyberterrorism various information security exploits can be carried out. Therefore, in order to curb counterterrorism various measures from both a strategic and technical point of view need to be devised and implemented. This chapter highlighted some of the critical countermeasures that can be introduced to combat the threat of counterterrorism. Previous chapters discussed the various contributing factors and phases in the development of a cyberterrorist. The next chapter will now address the design of the CLC model by combining the significant points made in earlier chapters.

Part 4 Life Cycle Model

This study, CLC- Cyberterrorism Life Cycle Model, is divides into four parts (originally shown as Figure 1). Figure 56 shows the status of the CLC model development study.

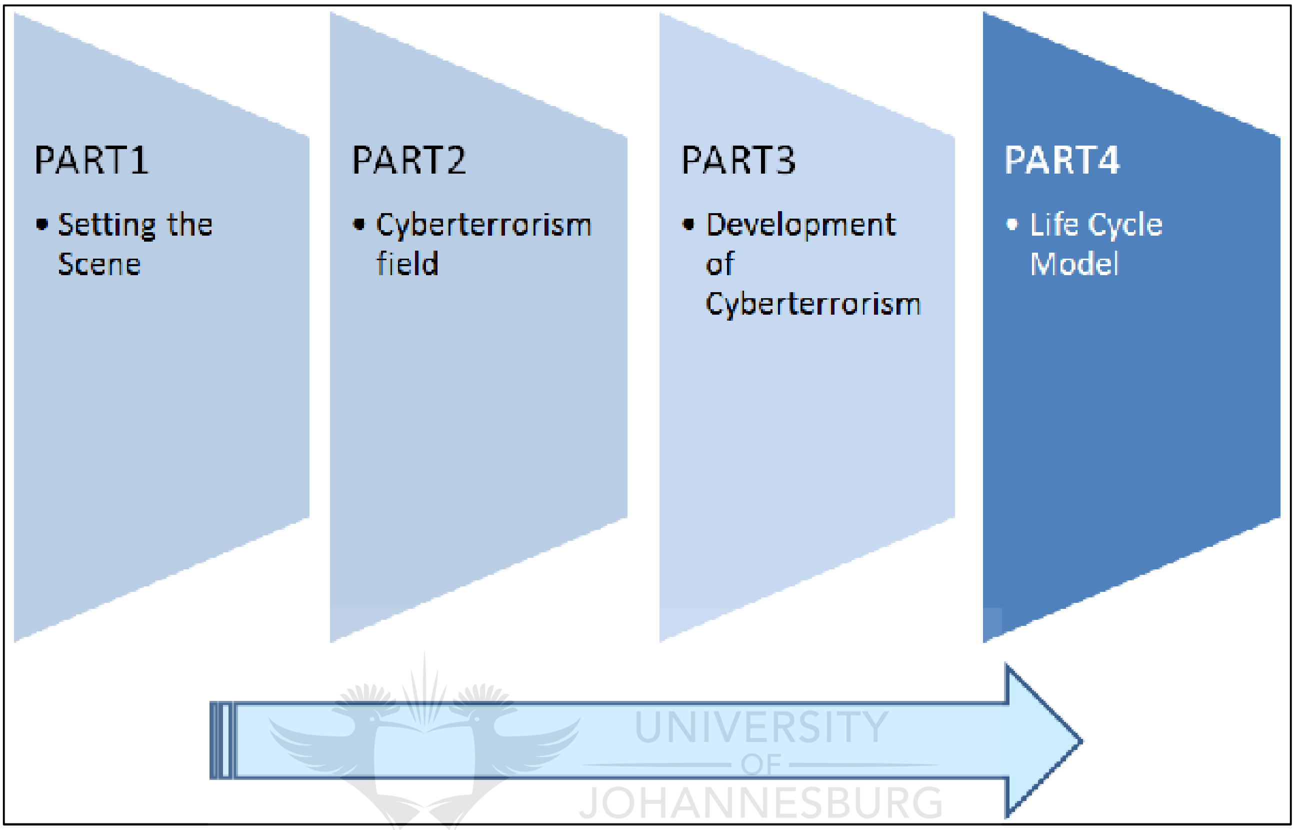


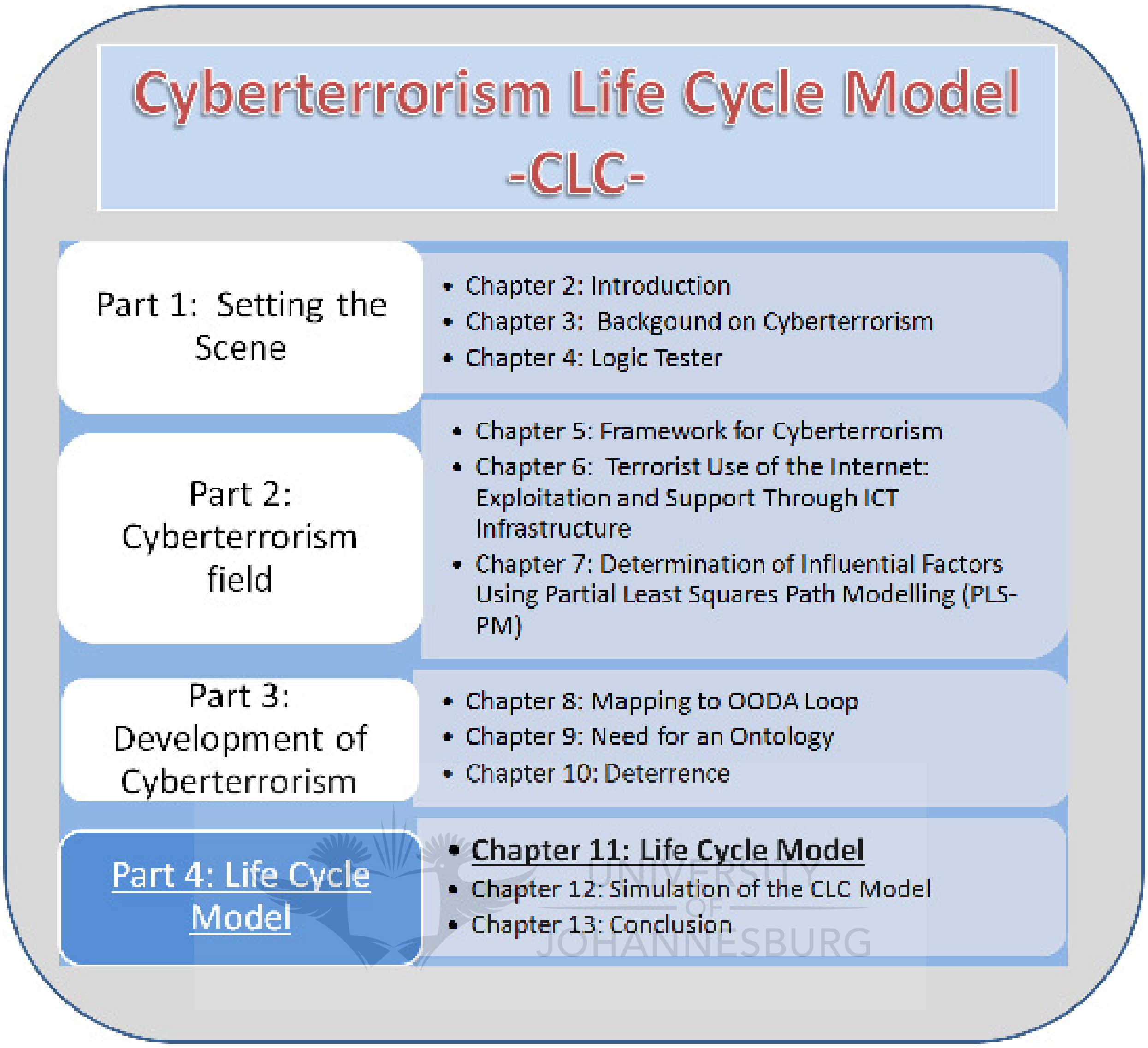
Figure 56: Part 4 of the CLC Model Development Study (Own Compilation)

Part 1, 2 and 3 have already been completed. Part 4 the life cycle model presents the visual representation..

Chapter 11, Cyberterrorism Life Cycle (CLC) Model forms the main crux of this research study. It brings together the critical aspects discussed previously and so shows the development of a cyberterrorist. This chapter will show the importance of modelling, as well as the various operating forces that are critical to cyberterrorism and thus contribute to the CLC model. The opening chapter states that the aim of this thesis is to develop a model that describes the development of a cyberterrorist to gain insight into their motivation and modes of operation. Chapter 3 - 10 have provided the background to the discipline of cyberterrorist and thus the foundation for compiling the model framework. Chapter 11 will now incorporate the important aspects previously discussed to compile the basic model describing the development of a cyberterrorist.

Chapter 12, Simulation of CLC Model will present a simulation of the CLC model. The aim of the simulation is to show a dynamic representation of the influential factors affecting cyberterrorism. The vividness of a simulation will convey to the reader the interaction and effect of these influential factors.

Chapter 13, the Conclusion provides the concluding remarks to this research. It presents a justification of the CLC model in that it aims to provide a structured representation showing the dynamic interaction of influential and technical aspects in the field. It also describes the limitations of this study and future work that can arise from this study.



Cyberterrorism Life Cycle Model
-CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS-PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- **Chapter 11: Life Cycle Model**
- Chapter 12: Simulation of the CLC Model
- Chapter 13: Conclusion

11 Cyberterrorism Life Cycle (CLC) Model

"Why assassinate a politician or indiscriminately kill people when an attack on electronic switching will produce far more dramatic and long-lasting results."

- William Laquer Historian and Terrorism Expert

Section 2.2 states that the aim of this thesis is to provide insight into the dynamic interaction of the various influential and emerging factors in the field of cyberterrorism. Chapters 2 - 10 have been providing the various building blocks to construct the model. The previous chapters have provided the framework for the model and Chapter 11 will now incorporate the various aspects previously discussed to build a life cycle model that demonstrates the development of a cyberterrorist.

Part 4, The Cyberterrorism Life Cycle Model, forms the main crux of this research study. Chapter 11 brings together the important aspects of the proposed CLC Model. This chapter will demonstrate the importance of using modelling and combines all the drivers identified in previous chapters to present the reader with a merged view of the most important concepts in the field of cyberterrorism. The research carried out in previous chapters, forms the building blocks of the CLC model in Chapter 11.

Figure 57 shows how the various building blocks contribute to the CLC model. All the objectives have been addressed in the preceding chapters, with Chapter 11 now purposely addressing the conglomeration of the various drivers to establish the CLC model.

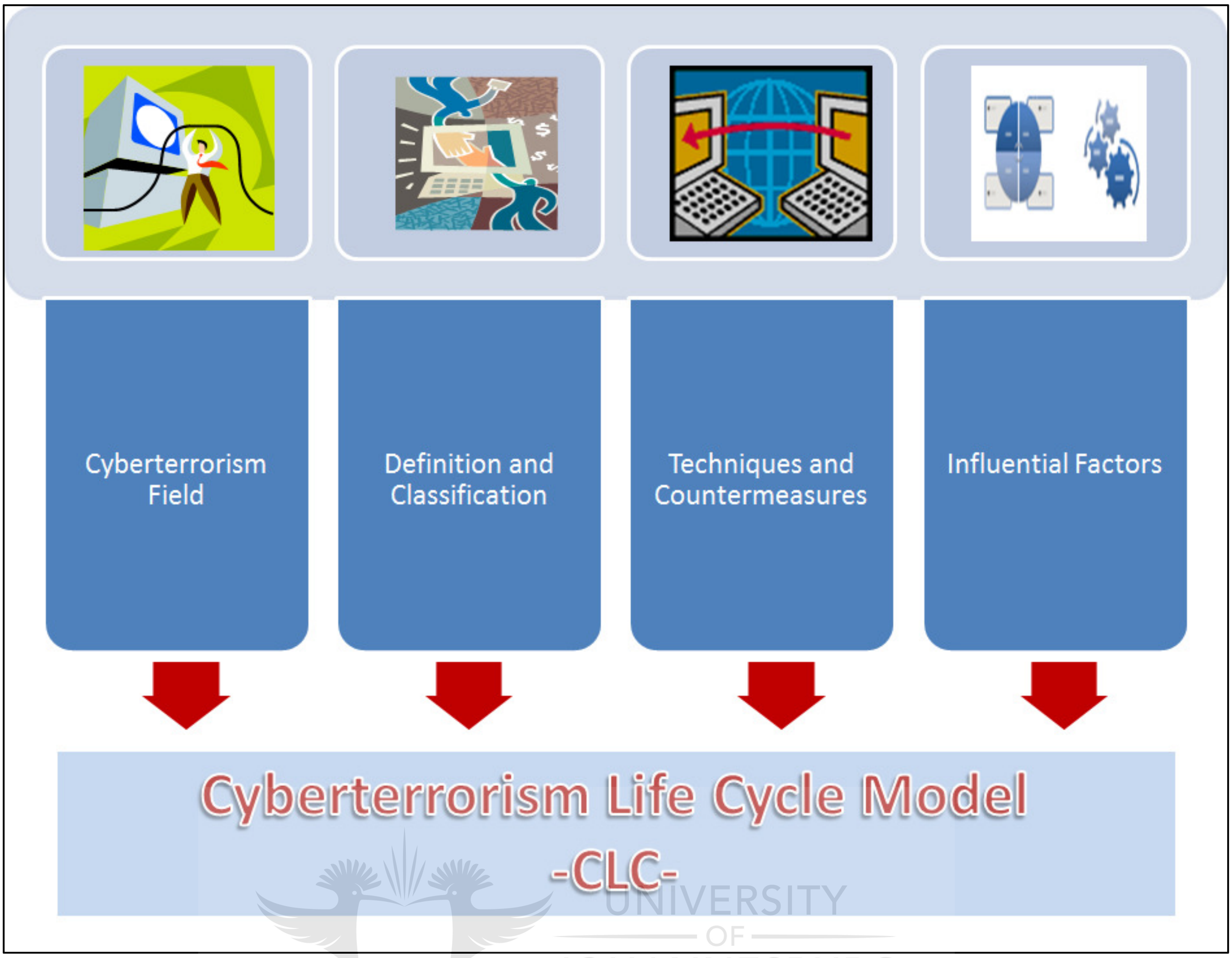

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 57: CLC Model Focus Chapter 11 (Own Compilation)

The aim of this thesis is to develop a model that describes the development of a cyberterrorist. The previous chapters have been building the readers' knowledge base to establish the foundation principles that will form the root of the model. This chapter will now incorporate important aspects discussed in previous chapters and so present the Cyberterrorism Life Cycle (CLC) model.

11.1 Introduction

In order to ensure that cyberterrorism can be opposed, it is important to understand the various forces that operate in the field. These range from motivational factors to technical methods of carrying out attacks. In order to ensure that countermeasures can be effective, it is important to identify these drivers, as well as establish links between these drivers. This chapter unites all the drivers identified in the previous chapters to establish a solid foundation for the CLC model.

Firstly, a motivation is given on the benefits of modelling. Thereafter, the CLC model is introduced. In addition, an explanation of the various dimensions and factors in the CLC model is given.

Why model?

Models can be used to explain complex fields as models can abstract, simplify or condense many concepts into a visual representation that can be easier to understand. Therefore, this chapter focuses on building a model that encompasses the various concepts related to cyberterrorism.

Epstein (2008) describes various reasons for modelling. Some of these reasons include (Epstein 2008):

- Explain (by giving more details and helps elaborate)
- Illuminate core dynamics
- Suggest dynamical analogies
- Discover new questions
- Bound outcomes to plausible ranges
- Illuminate core uncertainties
- Demonstrate trade-offs/suggest efficiencies
- Educate the general public
- Reveal the apparently simple to be complex

Thus, models provide a useful manner of explaining, exploring, analysing, discovering, illuminating, identifying, educating and revealing critical aspects of a subject matter.

Models provide the ability to explore a research field, by showing relationships and interactions between concepts. Modelling thus helps in portraying a concise representation of a field that may have various complex components. Eriksson and Penker (2000) explain that a model represents a simplified view of a complex reality and thus provides a way of abstraction so as to eliminate irrelevant details and allow the focus to fall on one or more important aspects at a time. In this way, models help provide understanding of a field by abstracting to a necessary level and showing the most important aspects. It is thus important to focus on the fundamental abstractions in order to convey the most critical aspects. Therefore, by using models, the most important elements of a field can be portrayed.

Throughout chapters 3 - 10, important aspects relevant to the field of cyberterrorism have been discussed and the various drivers have been identified. The drivers span various aspects like effects and techniques, which cover motivation and means. Overall, there is large number of critical aspects relevant to the field of cyberterrorism. For this reason, as a means of portraying some of the most critical aspects of cyberterrorism, this chapter proposes the CLC model.

The main goals of the CLC model are:

- Integrate all the salient factors
- Display these factors in parallel
- Provide a tangible model to work with
- Visualise the conceptual knowledge

- Frame the factors against the context of their dynamic operation

The next section presents the generic CLC model, based on the findings presented in earlier chapters. The CLC model allows for adaptation, while still providing clarification of the groundwork definitions, concepts and ideas relating to the field of cyberterrorism. The model also allows for the identification of future areas of research and development by looking at emerging methods of attack and deterrence. In addition, the model can be useful for introducing and explaining the field to an audience who have no prior background or knowledge. This is especially important in reducing the confusion about cyber attacks being perceived as cyberterrorism instead of cybercrime.

11.2 Generic Cyberterrorism Life Cycle Model Framework

In order to develop a helpful model, it is important to include a number of far-ranging drivers that span the field of cyberterrorism. The aim of the model is not to present a set of rigid steps of execution and deterrence, but rather to represent the dynamic nature of the field and demonstrate how the various drivers are related in order to identify the best approaches of combating attacks.

This chapter largely borrows from Chapter 8 in which the mapping to the OODA loop was initially explained. Thereafter, the concepts were further refined and tested in the ontology in Chapter 9. Furthermore, countermeasures were identified in Chapter 10. All these findings contribute to the development of the CLC model.

Similar to the Sociocultural Behaviour Capability Areas Framework in Figure 35, the CLC model has been adapted from the OODA loop. The Sociocultural Behaviour Capability Areas Framework consists of the capabilities of Understand, Detect, Mitigate and Forecast. Figure 58 shows the proposed generic CLC model. It is composed of four dimensions of: Prepare, Acquaint, Choose, Execute which are largely based on steps in the OODA loop (in Chapter 8), as well as the dimension of Deterrence. This helps to depict a simple representation of cyberterrorism. The model is thereafter elaborated to show the incorporation of the other critical drivers identified in this study and listed at the end of Chapters 3 to 10.

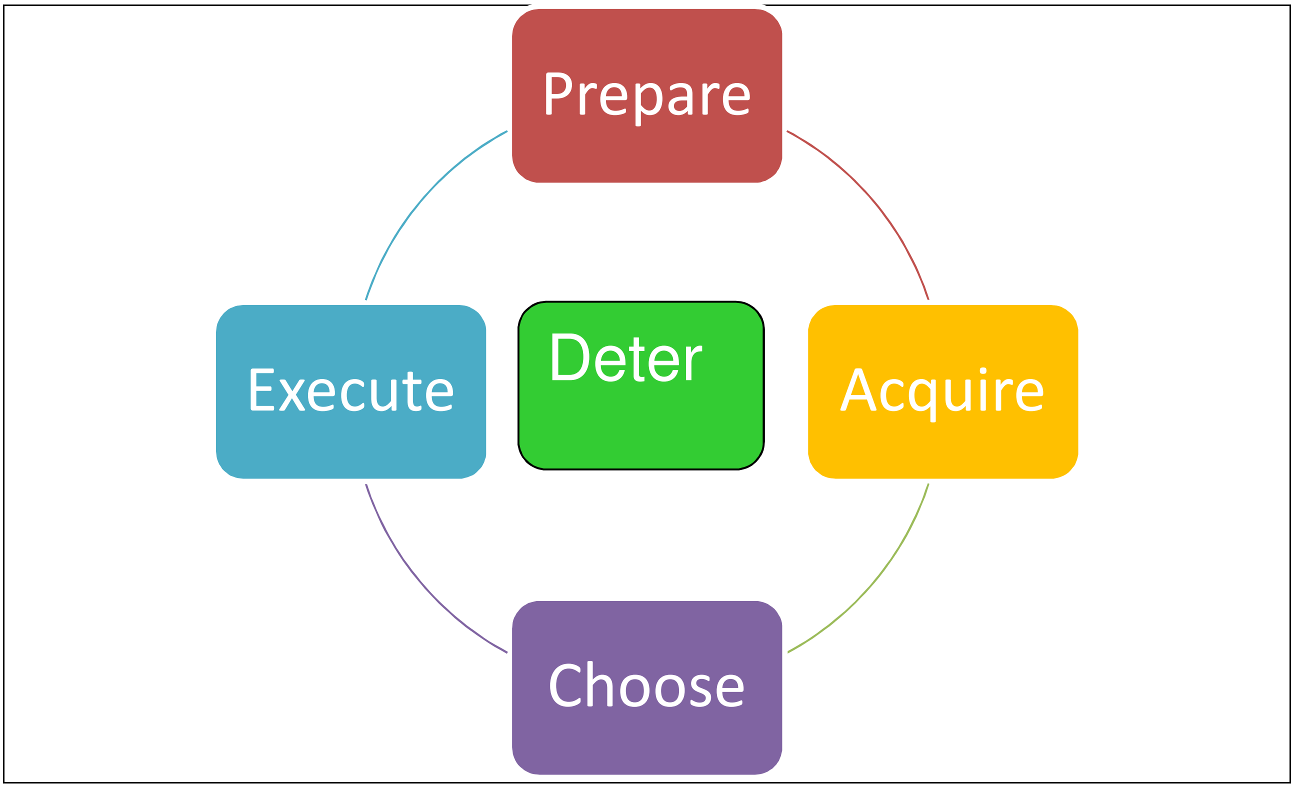


Figure 58: High-level CLC Model (Own Compilation)

In this chapter, specific terms are used to describe aspects of the proposed CLC model. The terms are explained below.

- **Dimension.** □

  An aspect or feature of a situation (Oxford Dictionary 2013). It can refer to the scope and show importance. Dimension also indicates features, attributes, and aspects of objects or subjects. In this context, it refers to the high-level main concepts relevant to the CLC model.

- **Factors.** ⬭

  Something that actively contributes to the accomplishment, result or process (The Free Dictionary 2013). Overall, a factor indicates something that affects a result or outcome. In the CLC model, factors refers to the essential components that influence the development of a cyberterrorist. Factors may take into consideration various drivers.

- **Drivers.** Something or someone that provides impulse or motivation (Merriam-Webster 2013). Driver can refer to the driving force behind an activity. In this perspective, at the end of Chapters 3 to 10, a list of drivers for each chapter was compiled and its inclusion in the CLC model explained. These drivers form the baseline of the various concepts encapsulated in the CLC model.

Figure 59 shows the relationship between the CLC model terminologies to explain their use in the CLC model.

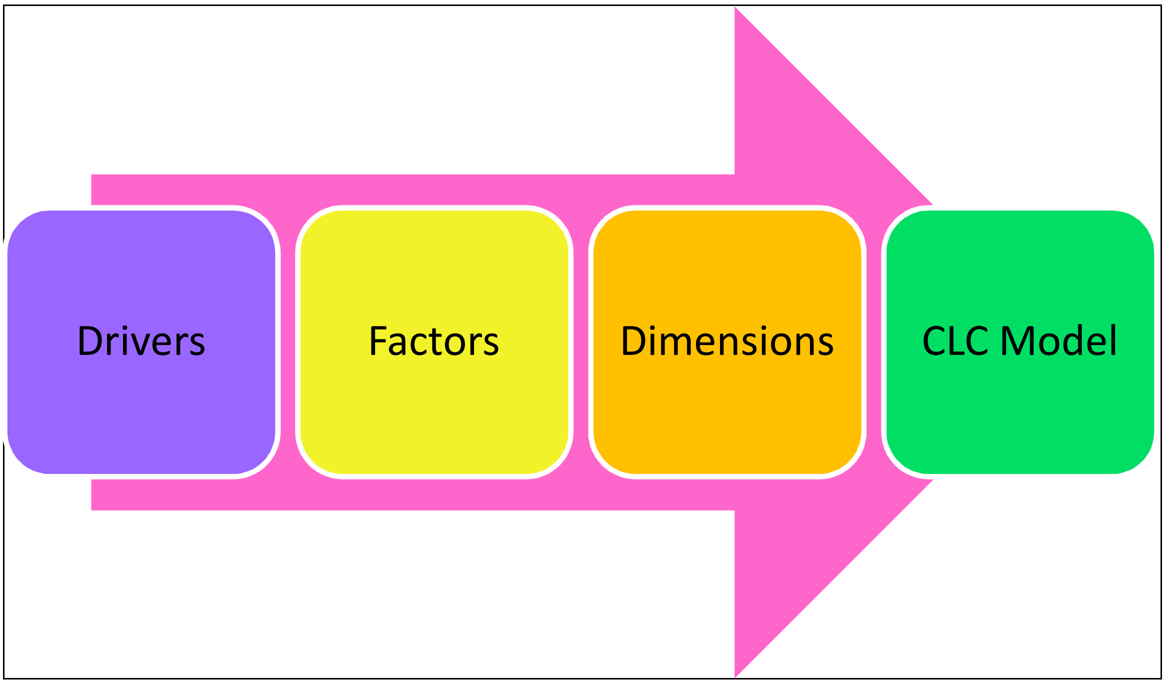


Figure 59: Relationship Between CLC Model Terminology (Own Compilation)

The various summaries provided in Chapters 3 to 10 not only highlighted significant contributing drivers but also helped formulate the dimensions. The various discussions around the contributing drivers, the exploration of the OODA loop, and the compilation of the ontology all assisted in the identification of the four dimensions, as well as a grouping of the contributing factors into a dimension. The contributing drivers identified at the end of each of the previous chapters were thus the key forces that influenced the formulation of the four dimensions, together with the countermeasures dimension.

The study now focuses on showing how the various drivers identified at the end of previous chapters fit into the CLC model in order to show their contribution and representation. Each of the dimensions also consists of a number of contributing factors that influence and guide each dimension. Therefore, this chapter presents all these factors in an abridged format.

This model largely borrows from the OODA loop, but also adds the dimension of countermeasures. In addition, the CLC model shows how the various contributing factors are not strictly bound to one dimension due to the dynamic nature of cyberterrorism. However, by representing the dimensions in a model, insight can be gained into how a cyberterrorist develops and where best to implement countermeasures.

11.3 Presenting the Drivers

Chapters 3 to 10 all concluded with a summary of the critical drivers of that chapter. These summaries also highlighted the key ideas that should be captured in the model. Table 9 combines all these critical drivers. It also shows how each critical driver is related to an applicable aspect of the CLC model. In essence, the critical drivers listed are a duplicate of the summaries given at the end of Chapters 3 to 10 but are now presented as one single list.

Table 9 can be seen as a grouping and drawing attention to the most critical drivers that influence the development of a cyberterrorist. During each dimension of the CLC model, other contributing drivers play an influential role. Therefore, in Table 9 the critical drivers are classified into a contributing factor column and a dimension column. In addition, in some cases, the contributing factor spans dimensions and therefore more than one dimension is indicated.

Table 9: Summary of Critical Drivers in Field of Cyberterrorism (Own Compilation)

Driver	Original Section	CLC model contributing factor	CLC Dimension
ICT as a target or weapon	3.10	Objectives	Choose Execute
Support functions include training, recruitment, networking and funding.	3.10	Objectives	Acquaint Choose
Cyberterrorism definition	3.10	All	All
Cyberterrorism is motivated by political, social or religious reasons	3.10	Motivation	Prepare Acquaint
Cyberterrorism has governmental or critical targets	3.10	Targets	Choose
Cyberterrorism practices include crashing critical systems	3.10	Practices	Execute
Preparation, means and target can be a combination of digital and physical aspects	3.10	All	Prepare Acquaint Choose Execute
Cyberterrorism aims to cause interference with electronic systems	4.7	Objectives, Practices	Choose Execute
Differentiation between cybercrime and cyberterrorism-cyberterrorism is threat, disturbance or infliction of violence	4.7	Motivation Practices Objectives	Prepare Acquaint Execute Acquaint Choose
Cyberterror objectives are related to causing fear	4.7	Objectives	Acquaint Choose
Various characteristics of ICT make it a viable target or weapon of attack	5.7	Characteristics	Prepare
Social factors affect the development of a cyberterrorist	5.7	Social factors	Prepare Acquaint Choose Execute
Cyberterrorism stems from a high-level motivation	5.7	Motivation	Prepare Acquaint
Capabilities will determine the scope of attack	5.7	Capabilities	Acquire
Malicious goals differentiates cyberterrorism from cybercrime	5.7	Objectives	Acquaint Choose
ICT can be used to support a terrorist group	5.7	Objectives	Acquaint Choose
High-profile targets will have maximum damage and coverage of the attack	5.7	Target	Choose

Driver	Original Section	CLC model contributing factor	CLC Dimension
Practices will incorporate hacking and other technical methods	5.7	Practices	Execute
ICT can be used traditionally for malicious objectives and innovatively as support functions for cyberterrorism	6.6	Objectives	Acquaint Choose
Additional support functions include distributing propaganda and psychological warfare	6.6	Objectives	Acquaint Choose
Support practices can be classified as web literature, social-networking tools, anti-forensics and fundraising	6.6	Practices	Execute
Examples of web literature include periodicals, essays, manuals, encyclopaedias, poetry, videos, statements and biographies.	6.6	Practices	Execute
Social-networking tools include forums, blogs, websites, gaming, virtual personas, music and applications.	6.6	Practices	Execute
Identified anti-forensics methods that are being used include: steganography, draft message folders, encryption, IP-based cloaking, proxies and anonymisers.	6.6	Practices	Execute
Fund-raising is carried out using various scams including auctioneering, casinos, fake drugs, donations, credit card theft and phishing	6.6	Practices	Execute
Technical skills and the willingness to commit piracy strongly influence people's willingness to engage in cyber deviance	7.5	Capabilities	Prepare Acquaint Choose Execute
People who more likely to commit cyberterrorism can sway to a certain gender, age group and marital status.	7.5	Social factors	Prepare Acquaint Choose Execute
Social factors are an influential factor throughout the life cycle of a cyberterrorism	8.4	Social factors	Prepare Acquaint Choose Execute
Initially, the important influential factors are the characteristics of ICT that make it a viable target or weapon, together with initial motivating forces that stems from the classification of terrorism types.	8.4	Characteristics Motivation	Prepare
Critical to the familiarisation of a potential cyberterrorist is the capabilities that they possess, as well as the motivation forces that stem from terrorism types, together with the formulation of initial malicious goals.	8.4	Capabilities Motivation Objectives	Acquaint
The Choose Dimension features the objectives of malicious goals or support functions, as well as the target.	8.4	Objectives Target	Choose

Driver	Original Section	CLC model contributing factor	CLC Dimension
The Execute Dimension will reflect the various practices that can be carried out	8.4	Practices	Execute
Actors can be classified as commercial competitor, hacker, insider, criminal or protestor and thus possess these capabilities.	9.6	Capabilities	Prepare Acquaint
Cyberterrorism has a motivation, objective, effect, target and practice that differentiates it from a cyber event and a support function	9.6	Motivation Objective Target Effect Practice	Prepare Acquaint Choose Choose Choose Execute Execute
Cyber event has different effects null, minor, major or catastrophic damage	9.6	Effect	Choose Execute
Cybercrime motivation is criminal, ethical financial, military and recreational whereas cyberterrorism is political, social and religious	9.6	Motivation	Prepare Execute
Further identified practices include web defacement and data manipulation.	9.6	Practices	Execute
Targets can be classified as individual, organisational, governmental and critical systems	9.6	Targets	Choose
To be cyberterrorism, a cyber event has: • Major or catastrophic effects • Political, religious or social motivation • Practice is data manipulation or web defacement • Target is organisation, government or critical system	9.6	Effect Motivation Practice Target	Choose Execute Prepare Execute Execute Choose
To a support function a cyber event can have : • Political, religious or social motivation • Practice of anti-forensics, fundraising, web literature and social networking	9.6	Motivation Practice	Prepare Execute Execute
Countermeasures need be devised from a strategic and technical point of view	10.4	Countermeasures	Prepare Acquaint Choose Execute
Strategic countermeasures can be grouped as legal, political, economic, social and religious categories	10.4	Countermeasures	Prepare Acquaint Choose Execute

Driver	Original Section	CLC model contributing factor	CLC Dimension
Examples of countermeasures cannotstrictly be classified to belong to a single category	10.4	Countermeasures	Prepare Acquaint Choose Execute
Other examples of strategic countermeasures include: media, charities, cultural centres, analysis, education, humanitarian aid, military response, peace-keeping, policies, treaties, protocols, laws, perception management and fusion centres	10.4	Countermeasures	Prepare Acquaint Choose Execute
Technical countermeasures include CSIRT's, intrusion prevention, network monitoring, interception and blockage, disaster recovery and forensics	10.4	Countermeasures	Prepare Acquaint Choose Execute

Figure 60 shows an expansion of the CLC model, with the four main dimensions shown in the innermost circle. The Deter dimension appears on an outer edge, as the encompassing countermeasures are applicable across all four main dimensions.

The CLC model is reconciliation, integration, and organisation of all the concepts explored in the previous chapters. The encapsulation in a conceptual model displays all the ideas in parallel and thus captures the diverse concepts and knowledge.

The original OODA loop phases (see Figure 38) are adapted to the PACED dimensions: *Prepare, Acquaint, Choose, Execute and Deter* (see Figure 60). The Deter phase consists of countermeasures specific to cyberterrorism. Within each of the four main dimensions, factors are displayed that applies to those specific dimensions. These factors are labelled A-H in Figure 60, and include *Social Factors (A), Characteristics (B), Motivation (C), Capabilities (D), Objectives (E), Targets/Focus (F), Effects (G) and Practices (H)*. Some factors do not map strictly to one phase only. For example, *Social Factors* like culture, beliefs, political views, and personality traits will affect all the dimensions (indicated by the overarching outer circle of Figure 60).

A social factor like *Upbringing* is influential in the initial dimensions of *Prepare* and *Acquaint* (indicated by the A in the innermost circle). However, other social factors like beliefs or political views can change over a time span. Thus, *Social Factors* are represented as a ring covering all dimensions, as well as a specific factor overlapping during the *Prepare* and *Acquaint* dimensions (in Figure 60).

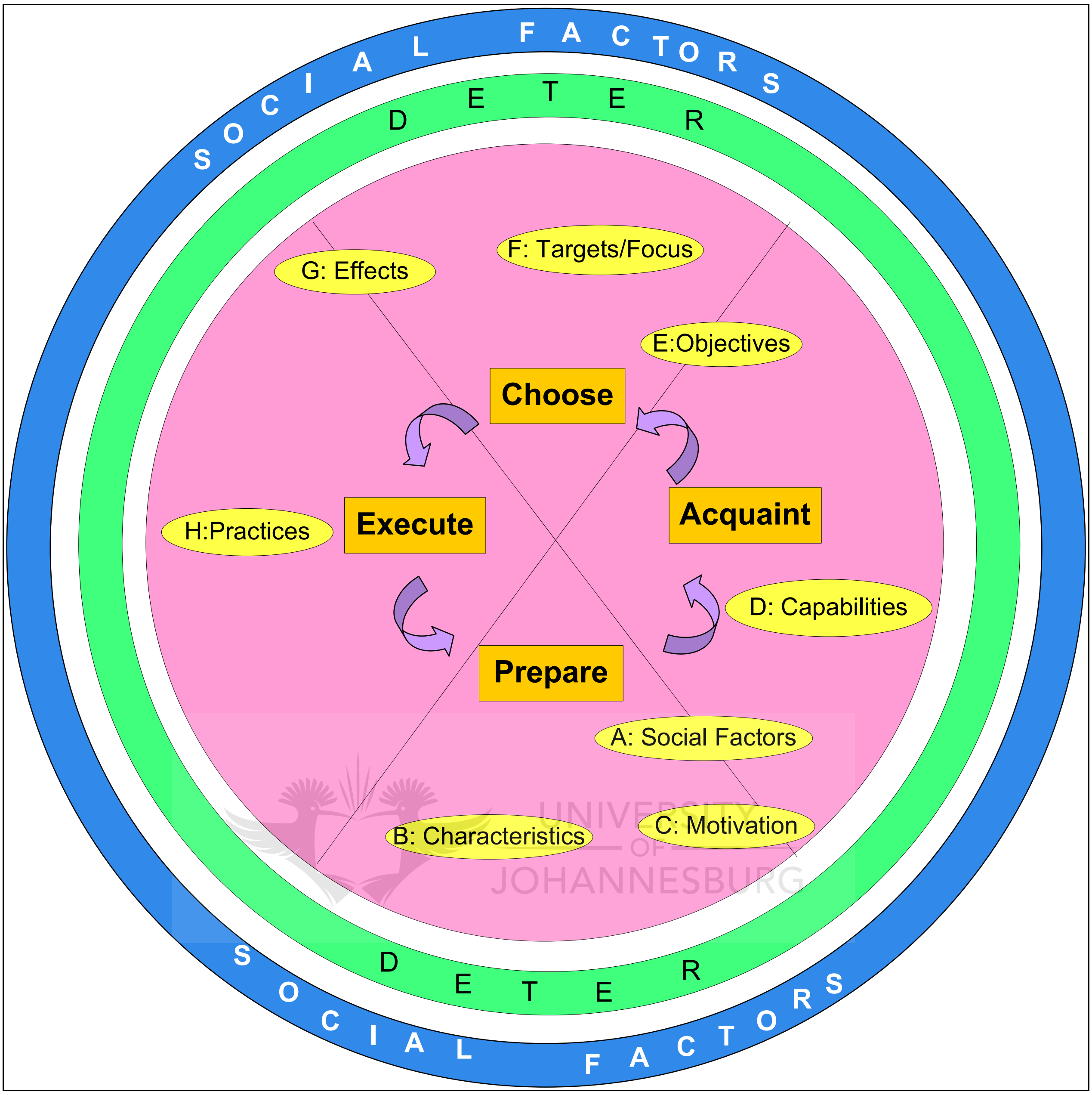
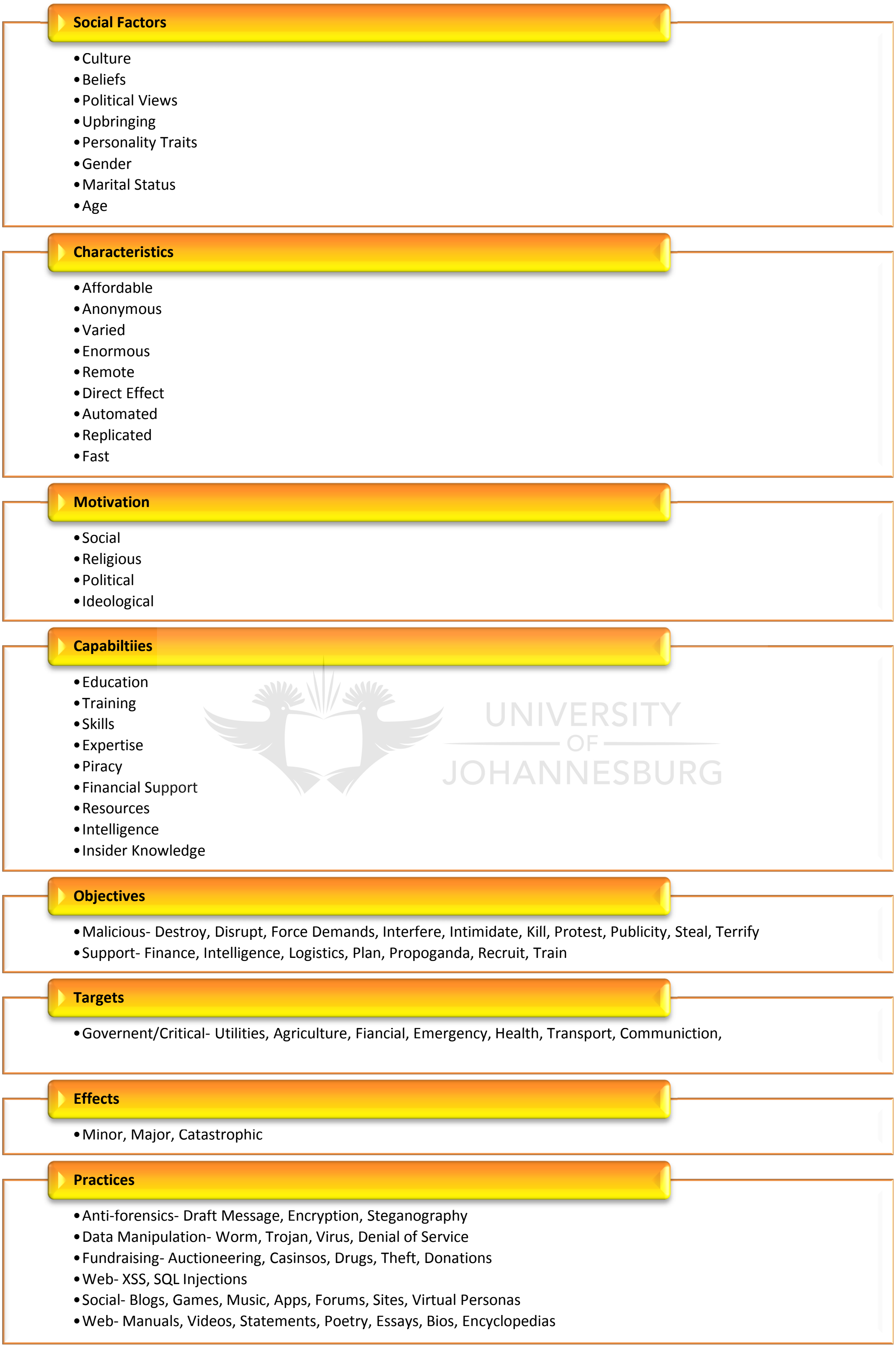


Figure 60: Expansion of CLC Model (Own Compilation)

Some of the factors captured in the model were slightly adapted from the original OODA loop mapping. For example, *Malicious Goals and Support Functions* (first introduced in Figure 16 and discussed in Chapter 5) have been encapsulated into a single factor entitled *Objectives (E)* in the CLC model (in Figure 60). Similarly, *Attack Levels and Modes of Operation* (first introduced in Figure 16 and discussed in Chapter 5) have been removed and *Effects (G)* has been added (in Figure 60). These changes are based on the analysis carried out during the compilation of the ontology in Chapter 9, which closely examined the core concepts related to the field of cyberterrorism. The cyberterrorist effects were identified to be a core factor in the life cycle development during an ontological study of the field Section 9 and were thus included in the CLC model.

Overall, an expanded list of the factors in the CLC model is shown in Figure 61.



Social Factors

- Culture
- Beliefs
- Political Views
- Upbringing
- Personality Traits
- Gender
- Marital Status
- Age

Characteristics

- Affordable
- Anonymous
- Varied
- Enormous
- Remote
- Direct Effect
- Automated
- Replicated
- Fast

Motivation

- Social
- Religious
- Political
- Ideological

Capabiltiies

- Education
- Training
- Skills
- Expertise
- Piracy
- Financial Support
- Resources
- Intelligence
- Insider Knowledge

Objectives

- Malicious- Destroy, Disrupt, Force Demands, Interfere, Intimidate, Kill, Protest, Publicity, Steal, Terrify
- Support- Finance, Intelligence, Logistics, Plan, Propoganda, Recruit, Train

Targets

- Governent/Critical- Utilities, Agriculture, Fiancial, Emergency, Health, Transport, Communiction,

Effects

- Minor, Major, Catastrophic

Practices

- Anti-forensics- Draft Message, Encryption, Steganography
- Data Manipulation- Worm, Trojan, Virus, Denial of Service
- Fundraising- Auctioneering, Casinsos, Drugs, Theft, Donations
- Web- XSS, SQL Injections
- Social- Blogs, Games, Music, Apps, Forums, Sites, Virtual Personas
- Web- Manuals, Videos, Statements, Poetry, Essays, Bios, Encyclopedias

Figure 61: Summary of Factors in CLC Model (Own Compilation)

The Deter Dimension consists of various countermeasures as discussed in Chapter 10. Both strategic and technical countermeasures can help reduce the devastating growth of cyberterrorism. Figure 62 shows a summary of the Deter Dimension. These countermeasures need to work in harmony with each other in order to deter the original conditions, which foster negative political, social, religious or ideological views. Technical regulations also need to operate in a synchronised manner in order to prevent, detect and react to cyberterrorism acts.

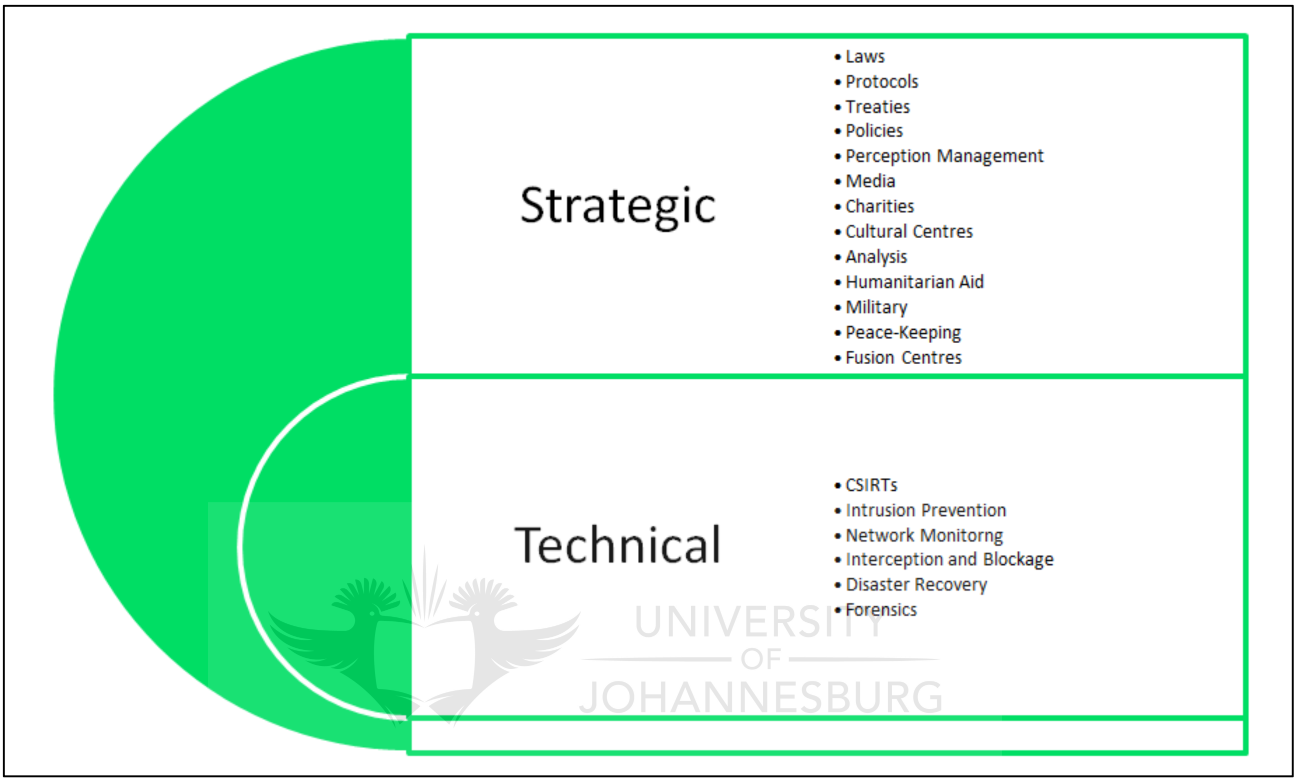


Figure 62: Summary of Deter Dimension of CLC Model (Own Compilation)

Overall, the model is broken down into different layers in order to show more levels of detail. Thus, the model begins with a high-level representation in Figure 58. Figure 60 shows the different dimensions and factors. The factors are shown in detail in Figure 61 with the Deter Dimension summarised in Figure 62.

The next section looks at comparing CLC to other models so as to show the benefits of the CLC model.

11.4 Comparison to Other Models

In this chapter, the main goals are to propose a more holistic model representing cyberterrorism so as to explain and analyse the field better. The initial conceptual framework of cyberterrorism is presented in Chapter 5. This empirical framework is critiqued by Ahmad and Yunos (2012). The main criticisms are that the framework is not interactive and quite complex and that cyberterrorism should be considered from a holistic perspective. Therefore, this chapter strives to use the conceptual framework together with the various other drivers identified in previous chapters to show a more dynamic representation of cyberterrorism.

Another model relating to depicting the actor-target effect chain of cyberterrorism stems from Heickero (shown in Figure 63).

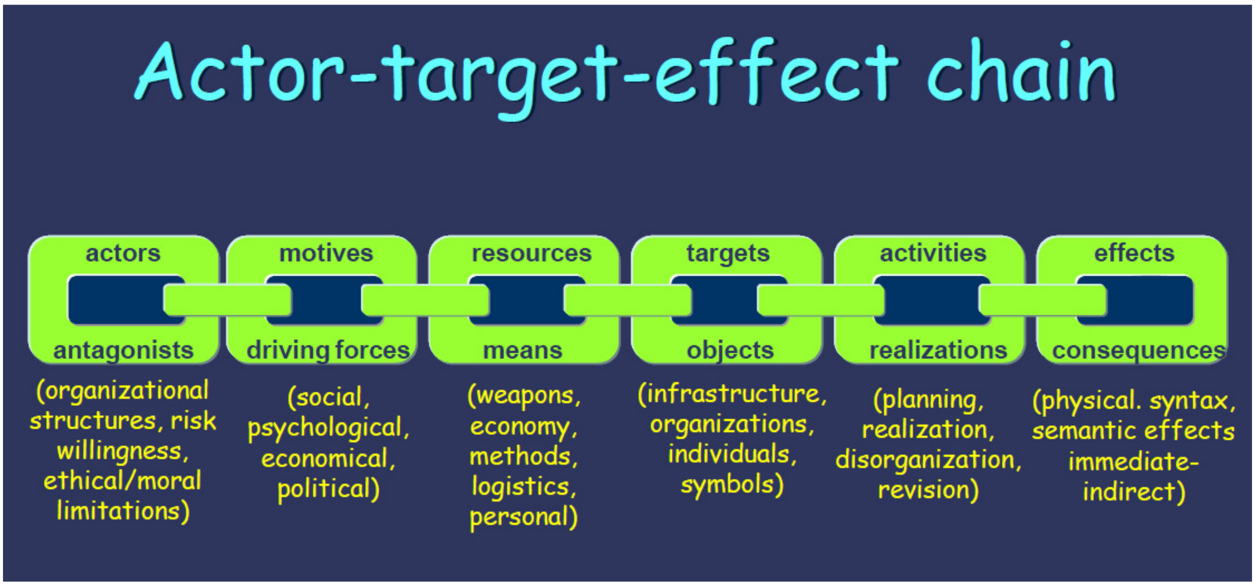

Actor-target-effect chain
actors
antagonists
(organizational structures, risk willingness, ethical/moral limitations)
motives
driving forces
(social, psychological, economical, political)
resources
means
(weapons, economy, methods, logistics, personal)
targets
objects
(infrastructure, organizations, individuals, symbols)
activities
realizations
(planning, realization, disorganization, revision)
effects
consequences
(physical. syntax, semantic effects immediate-indirect)

Figure 63: Actor- Target Effect Chain (Heickero 2007)

This framework depicts the modus operandi of cyber terrorists by encapsulating the attributes in a chain. The framework comprises: actors which are antagonists; the driving forces directing the motives like social, psychological or political; the types of means and resources like weapons, economy and methods; objects like infrastructure and organisations that become the targets; realisation of activities like planning and the consequences like physical, semantic, immediate or indirect. However, this framework requires more research into the types of activities, as well differentiation of terrorism support activities and cyberterrorism. The Actor-target effect chain also does not describe countermeasures or the social factors that drive people to cyberterrorism.

Figure 64 shows the “Dynamic Cyberterrorism Framework” from Ahmad and Yunos (2012). This framework aims to be dynamic since Ahmad and Yunos propose that all the attributes (components) contribute to the decision-making as to whether a person will carry out cyberterrorism or not. This means that each of the components is necessary to constitute cyberterrorism. Upon closer inspection the attributes proposed by Ahmad and Yunos resemble some of the classes developed in the ontological model in Chapter 9, as well as some of the categories in the conceptual framework in Chapter 5. However, there are some distinct differences. These differences are tabulated in Table 10.

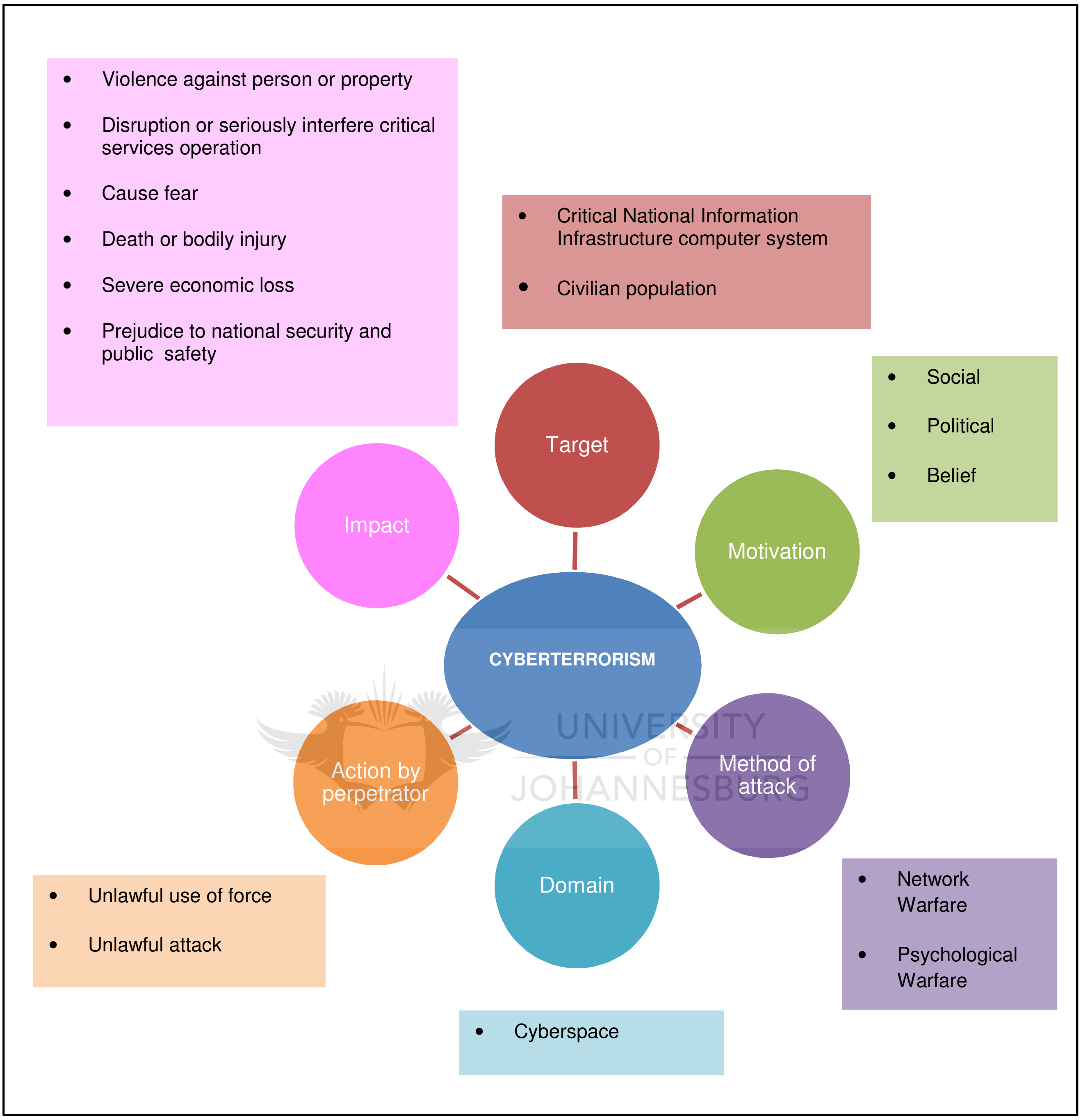


Figure 64: Dynamic Cyberterrorism Framework (Ahmad, Yunos 2012)

Table 10: Comparison of Dynamic Cyberterrorism Framework to CLC Model (Own Compilation)

Dynamic Cyberterrorism Framework	CLC Model
Target	Encompasses classifications and more detailed examples of targets
Motivation	Addresses Motivation in model (and also lower level objectives)
Method of attack	Does not focus on classifications of Network Warfare and Psychological Warfare but rather practices that can be countered
Domain	Dynamic Terrorism Framework model refers to domain of cyberspace Wide domain of electronic systems and ICT infrastructure is used. This model encompasses cyberspace as well
Action by perpetrator	Dynamic Terrorism Framework lists unlawful forces or attacks. CLC model incorporates emergent practices that can be carried out
Impact	Impact is shown as effects
Incorporation of all concepts into one dimension	Model that is broken down into layers to show dynamism and different aspects relevant to cyberterrorism

Overall, the CLC model is much more in-depth in that it incorporates other vital factors like the reasons that make cyberterrorism so appealing and the social factors that drive people to cyberterrorism. Other topics covered in the CLC model that are not covered in the Dynamic Cyberterrorism Framework include the characteristics of ICT infrastructure, the capabilities that are used to carry out cyberterrorism and the immediate objectives that are trying to be achieved. Furthermore, the CLC model is multi-layered with each layer providing more insight into the dynamics of cyberterrorism. The model can be viewed from a high-level with the main dimensions and thereafter decomposed into its various factors.

11.5 Benefits of CLC Model

The CLC has the following benefits:

- Shows various factors that are influential to cyberterrorism
- Indicates that the motivation, target, effect and objectives are critical to cyberterrorism
- Shows the importance of considering the field from both a strategic and technical point of view
  - Strategic motivations, technical implementation and both strategic and technical countermeasures
- Encapsulates the various drivers in a structured conceptual manner so as to provide insight into a field often perceived as all of cybercrime (which can later be represented in a more dynamic method)

The CLC model allows for adaptation, while still providing clarification of the groundwork definitions, concepts and ideas relating to the field of cyberterrorism. The model also allows for the identification of future areas of research and development by looking at emerging methods of attack and deterrence. In addition, the model can be useful for introducing and explaining the field to an audience who have no prior background or knowledge. This is especially important in reducing the confusion about cyber attacks being perceived as cyberterrorism instead of regular cybercrime.

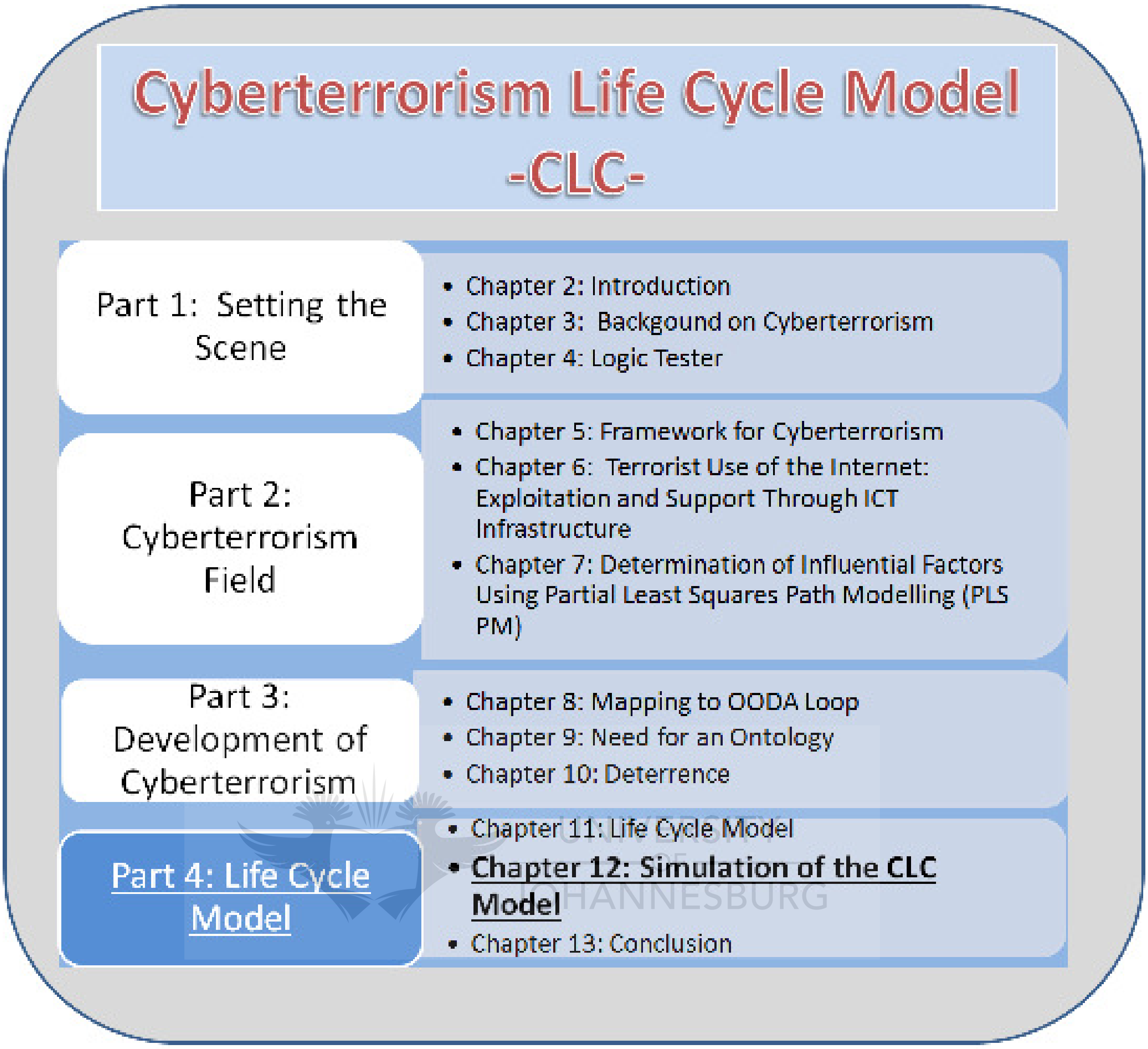
11.6 Conclusion

Chapter 11 initiated Part 4 as a bridge between the literature rich chapters in Part 1-3 and the construction of the CLC model (Part 4). This chapter addressed the benefits of modelling against the context of the field of cyberterrorism. This chapter also presented a visual model showing the lifecycle development of cyberterrorism.

Table 9 unifies all the previously identified drivers that contribute to the development of the model. This table is a detailed lists of the most vital aspects discovered in the research field so far. The CLC model synthesises all the information gained in the preceding chapters.

Chapter 11 plays an important role in summarising the study thus far. Chapter 12 will now discuss a dynamic representation of the CLC model using simulation techniques

.



Cyberterrorism Life Cycle Model

-CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- **Chapter 12: Simulation of the CLC Model**
- Chapter 13: Conclusion

12 Simulation of CLC Model

> *"This is what terrorism is occupied with as well: making real, palpable violence surface in opposition to the invisible violence of security."*
>
> *- Jean Baudrillard, Simulacra and Simulation*

Figure 65 shows the various objectives for compiling the CLC model. These objectives have been addressed in the preceding chapters, with Chapter 11 specifically addressing the union of the various drivers proposed over this research project and so put forward the CLC model.

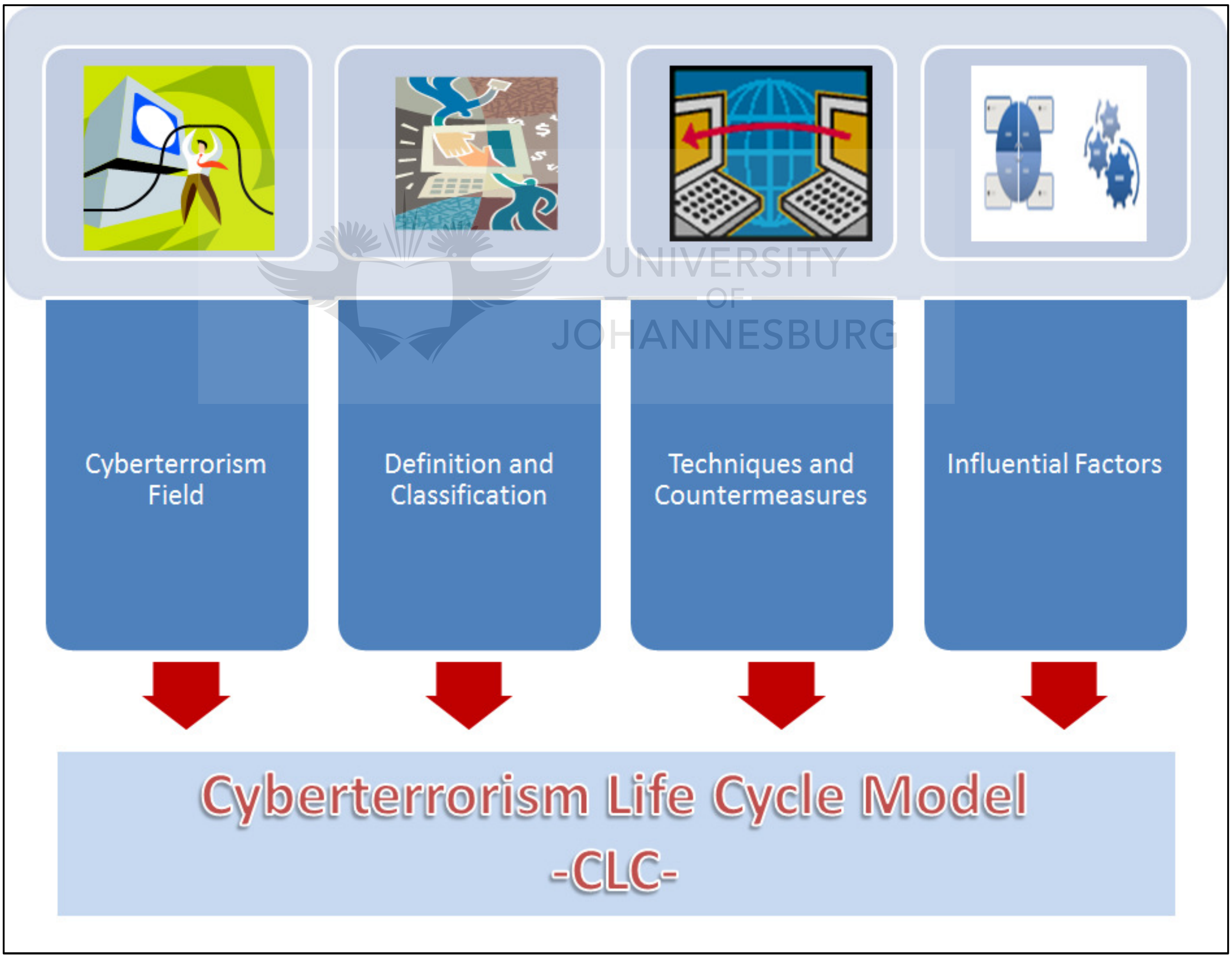

Cyberterrorism Field
Definition and Classification
Techniques and Countermeasures
Influential Factors
Cyberterrorism Life Cycle Model
-CLC-

Figure 65: CLC Model Focus Chapter 12 (Own Compilation)

The overall goal of this thesis is to compile a model that depicts how a cyberterrorist may develop. In the initial sections, background knowledge was provided. This established a firm foundation from which the CLC model could be developed. Furthermore, the previous chapters proposed a number of drivers that affect the cyberterrorism field. These drivers were then placed into essential factors influential to the field of cyberterrorism. The identification of the factors was used in the development of the CLC model, presented in the previous chapter.

Since these various factors either can directly or indirectly influence the development of a cyberterrorist, there is a lot of uncertainty in terms of how these factors play a role. This chapter therefore introduces a more dynamic representation of the CLC model with the use of simulation to show the interaction between factors.

12.1 Need for Simulation

Simulation is a form of modelling which aims to represent key characteristics, behaviour of functions of a selected physical system or abstract process. The Merriam Webster dictionary (2013) defines simulation as something that is intended to look, feel or act like something else, especially so that it can to studied. Computer simulation can be used to carry out this imitative representation to examine a problem often not subject to direct experimentation. Winsberg (1999) states that simulation may entail a complex chain of inferences that can transform theoretical structures into specific concrete knowledge. Thus, simulation can help to study real or hypothetical events in order to gain more insight into the system or process. The benefits of simulation include:

- **Practicality**: Costs or fragility of the conditions may not allow for the creation of a prototype or test. In such cases, the creation of a simulation is an ideal solution.
- **Time-saving**: A simulation can help identify important design requirements, flaws or potential issues. Developing a complete system and identifying critical issues or requirements at a later stage can be time and effort consuming.
- **Replication**: With simulations, tests can be run over again to adapt new analysis data or tests. The critical results can be captured and changes introduced without long delays.
- **Understanding**: Simulations can create a high impact through visual and computational effects. Animations and graphical representation can help capture behaviour and results, which can all influence decision-making.
- **Adaptable**: Simulations provide for flexibility that may not be feasible on actual systems. By providing for the ability to adapt to new data, analysis and decision-making can be enhanced.

Through virtual investigations, different experiments can be run which can even provide predictive results. Simulations can also facilitate analytic solutions to complex problems. Furthermore, simulations can utilise different scenario data and then determine emergent outcomes. Such an example is disaster relief preparedness, whereby simulations of emergency scenarios can teach participants better response actions. Moreover, one of the most common uses of simulations is the aviation industry. Flight simulation programs are used to train pilots without endangering equipment or lives. Another area in which simulations are commonly utilised is the manufacturing industry. Simulations can help introduce improvements in terms of the production process, assembly, and packaging. Overall simulations are useful in studying flow, movement, interactions, behaviour and various types of functionality. Cyberterrorism is a complex field that is influenced by many factors. Thus, a simulation of the CLC model is introduced in this chapter to depict the intricate interactions between the various factors.

12.2 Abstraction

Winsberg (2003) has explained that the use of computationally intensive methods can help learn about the behaviour of systems. In order, to build simulations some form of mathematical modelling is required in order to represent the components of the system. Furthermore, Winsberg has termed simulations numerical experiments that evoke the metaphor of the experiment in a powerful way. Thus, for the CLC simulation the factors needed to be translated into a mathematical format. This transformation of data will produce results based on the interaction of the various factors.

However, it is also necessary to consider fundamental abstractions in order to simplify a complex field and not lose focus. Eriksson and Penker (2000) have explained that a model is a simplified view of a complex reality and with the use of abstraction; one can eliminate irrelevant details and thus focus on the significant aspects. Therefore, the CLC model will make use of abstraction together with mathematical transformations in order to depict a representation of the cyberterrorism field.

In order to build a dynamic model, Winsberg (1999) states that a simulationist should specify a class of parameters, boundary values and initial conditions. Therefore, in setting up a simulation it is important to establish the initial data. However, this process is far from trivial. Smarr already in 1985 has stated that the specification of values is rarely straightforward but rather a delicate balancing act between accuracy and tractability (Smarr 1985). Empirical data on cyberterrorists is very scarce. Furthermore, data on behavioural influences, frequency, effect or even costs about cyber attacks are also limited. Companies are hesitant to disclose details about cyber attacks in fear of the consequences. Behavioural profiling covers various issues that may influence the development of cyber dissident behaviour. Shaw (2006) conducted research on profiling malicious cyber users as not much data had been gathered on the subject. Shaw's results coincide with many findings of the CLC model and are shown in Table 11.

Table 11: Comparison of Behavioural Research on Malicious Cyber Users to CLC Model (Own Compilation)

Behaviour Research of Malicious Cyber Users	CLC Model Similarity
Demographics	Social Factors
Personal Characteristics	Social Factors: Personal Traits
Risk Averse (work with known allies)	Support Function: Planning, Logistics,
Planned versus impulsive attacks	Support Function: Planning, Logistics
Personal history and traits	Social Factors: Upbringing , Personal Traits

However, this study was based on ten subjects and while the findings are useful, they do not provide substantial empirical data. In addition, The Economic Impact of Cyber Attacks report from Cashell, Jackson, Jickling and Webel (2004) shows the lack of statistical data about cyber attacks as companies have various incentives not to release this information or there is great uncertainty about its exact details. Furthermore, Clauset and Gleditsch (2012) state that very little research has been carried out on modelling terrorist event frequency and severity. The CLC simulation tries to address these issues by specifying input data and inferring the cyberterrorist behaviour based on the knowledge captured in the CLC model presented in the previous chapter. Thus, the CLC model aims to provide a dynamic representation and abstraction of the model presented in the previous chapter based on inferences. Therefore, in order to simulate the CLC model the initial step entailed specifying the initial conditions, parameters and boundaries. This was carried out on a selection of suitable values that would demonstrate the theoretical concepts captured in the CLC model in a dynamic manner. Since empirical data on terrorist behaviour is scarce, the author selected suitable values for the initial conditions that would capture the essence of the CLC model. The overall goal of the CLC model is show the interaction of the factors at an appropriate level of abstraction. Therefore, the main design of the simulation was to base it on the main factors identified in Chapter 11.

- The simulation would show the transition of the ordinary population to supporters of terrorism and eventually the transformation into terrorists. The ordinary population is referred to as *PotentialTerrorists* as they have the potential to become a supporter and then a terrorist.
- Initially the model starts out with a population of 1000 people. (This value was selected by the author as it is a small enough group of people to perform the transformations). The plotting of the population, supporters and terrorists growths suits an initial size of 1000. If a larger population size is used, significant details on the graph plot will not be seen).
- The number of births per 1000 people was set to 19.4 (World Population Prospects 2008a) and deaths 8.3 (World Population Prospects 2008b).

12.3 Simulation Overview

Figure 66 shows a high-level view of the simulation developed in AnyLogic. AnyLogic is a multi-method simulation tool that supports various simulation methodologies like Agent-Based or Discrete-Event modelling. In this simulation, the System Dynamic methodology was used which helped to capture this social and technical field heterogeneously. The benefits of AnyLogic are that it helps speed up the development process with a number of object libraries with pre-built simulation elements (Anylogic.com 2013). In addition, it supports custom Java code, which aids with the simulation development. Furthermore, due to the sophisticated animation functions, the visual impact of the model is powerful. This is particularly helpful in conveying the CLC model and explaining the field of cyberterrorism. Moreover, AnyLogic has an excellent statistical distribution function set that aptly covers inherent uncertainly present in all systems. An explanation of the CLC simulation follows in the next few sections. The accompanying video shows the live simulation running.

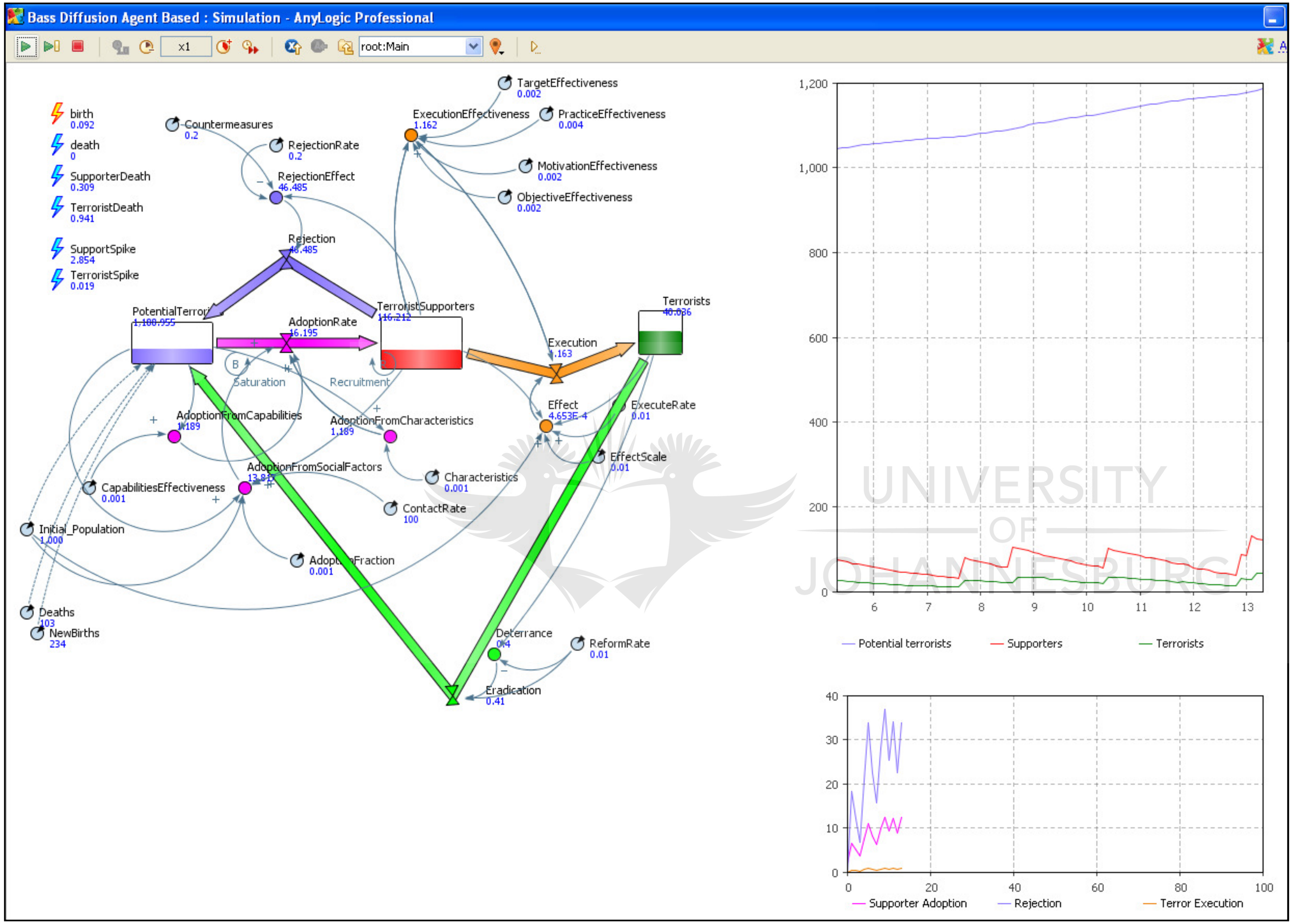


Figure 66: Simulation of Cyberterrorism (Screenshot 1) (Own Compilation)

(Please note that the simulation is randomised each time it runs and therefore will not correlate exactly to Figure 66. However, the premise remains the same). Figure 66 and the video are explained as follows: People are born (*InitialPopulation +births*) (shown as an orange event flash in Figure 66).

- People die (*InitialPopulation-deaths*)
- *TerroristSupporters= InitialPopulation+births-deaths*
- A random event could spike the number of *TerroristSupporters* or *Terrorists* (The occurrence of a terrorist event is highly unpredictable and therefore the model simulates random spikes in a following based on an event or uprising)
- *TerroristSupporters* or *Terrorists* die

The simulation is based on the concept of flow similar to those used in a production plant. The simulation uses this flow approach to show the transformation of people into supporters or terrorists. The following flows occur in the simulation:

- *PotentialTerrorists* can adapt into being *TerroristSupporters*
- *TerroristSupporters* can reject being a supporter and become a *PotentialTerrorist* once again
- *TerroristSupporters* can become a *Terrorist* after execution of a terrorist activity
- A *Terrorist* could become reformed and go back to being *PotentialTerrorist*

The simulation makes use of theorised mathematical values in order to communicate the interactions and show the dynamic representation of the CLC model. The CLC model is a new proposal that covers influential factors in order to explain a complex field. The simulation is used to show the development of cyberterrorist behaviour based on the CLC model and thus to show the multi-faceted field, the values had to be balanced in order to depict all the intricacies. The following conditions and parameters were among those specified in the simulation:

- The *AdoptionRate* into a *TerroristSupporter* is based on the overall effect of *AdoptionFromCharacteristics, AdoptionFromSocialFactors, AdoptionFromCapabilities, AdoptionFraction and ContactRate*. *AdoptionFromCharacteristics, AdoptionFromSocialFactors and AdoptionFromCapabilities* maps to three of the factors found in the Prepare and Acquaint Dimension of the CLC model. *AdoptionFraction* and *ContactRate* are two variables that are used in the simulation to calculate the rate of adoption based on the frequency of contact and propensity for adoption.
- These parameters are numerically specified as very low fractions.
- The Deter dimension of the CLC model is encapsulated in the Countermeasures and Deterrence parameters, which results in a decline of support or continued execution.
- Countermeasures may result in *TerroristSupporters* rejection of terrorist or over time interest may wane and therefore an ordinary *RejectionRate* parameter has been specified.

-

- With Deterrence efforts, the *ReformRate* of terrorists can increase and an eradication of terrorists can occur.
- Execution and transformation into a terrorist are influenced by the *Effect* and *ExecutionEffectiveness* conditions (based on the parameters *EffectScale, EffectRate, TargetEffectiveness, ObjectiveEffectiveness, MotivationEffectiveness and PracticeEffectiveness*).
- These parameters are numerically specified as extremely low fractions to show the conversion of *TerroristSupporters* into actual cyber terrorists.

12.3.1 Graph Overview

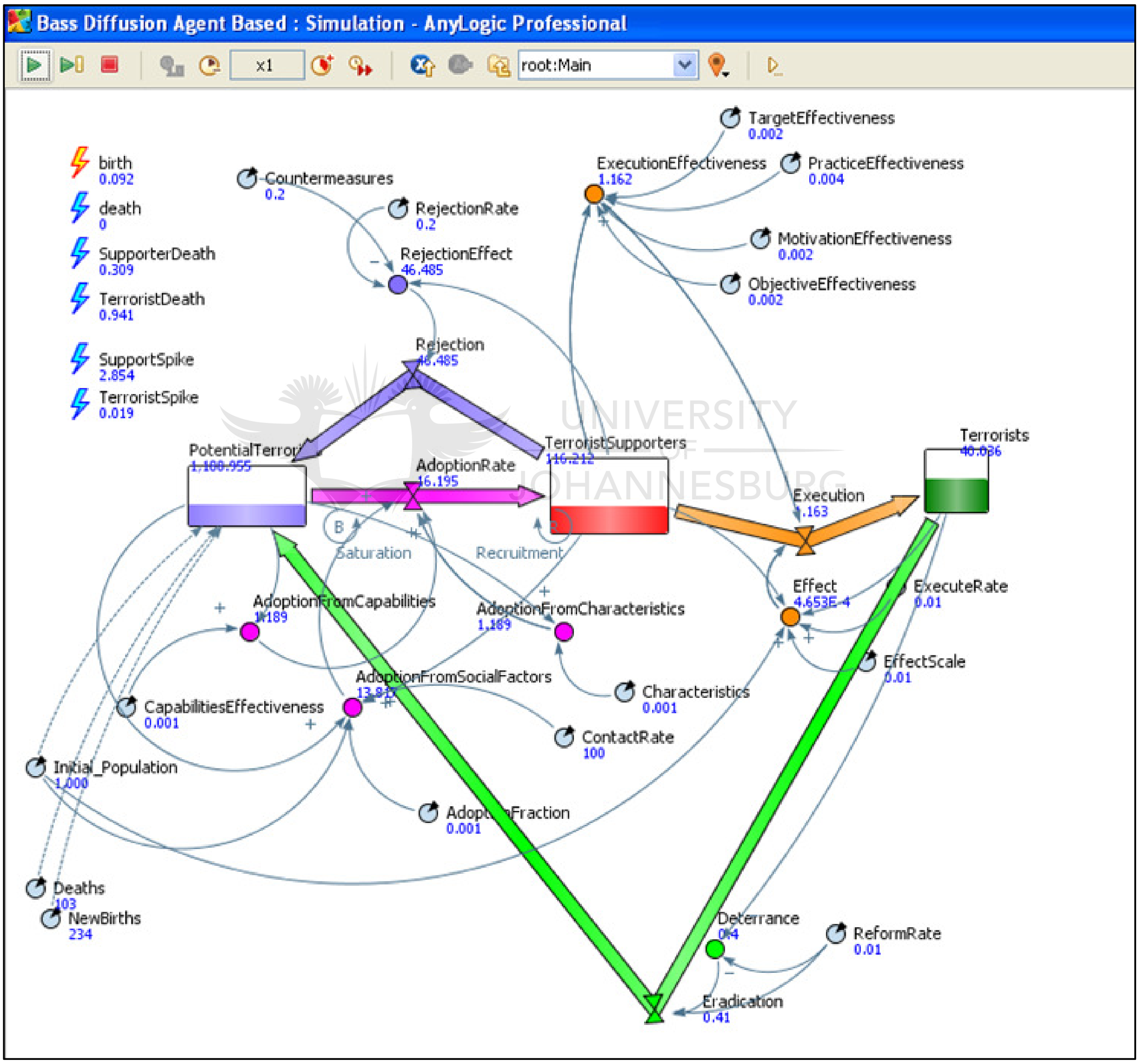


Figure 67: Cyberterrorism Simulation Flow View (Own Compilation)

The CLC Simulation Flow View (Figure 67 and video), shows the movement of *PotentialTerrorists* to *TerroristSupporters* and eventually *Terrorists* based on the influence of the Adoption and Execution rates.

-

The events of *Birth, Death, SupporterDeath, TerroristDeath, SupportSpike* and *TerroristSpike* are shown in the left corner. The *PotentialTerrorists* initially begins with 1000 people and then grows over time (based on births, deaths and movement of people into becoming supporters/ terrorists, reforming/rejecting the following and then returning to become a *PotentialTerrorist* or *TerroristSupporter*). The flow view depicts the effects of the different variables which affect the rates of adoption and rejection.

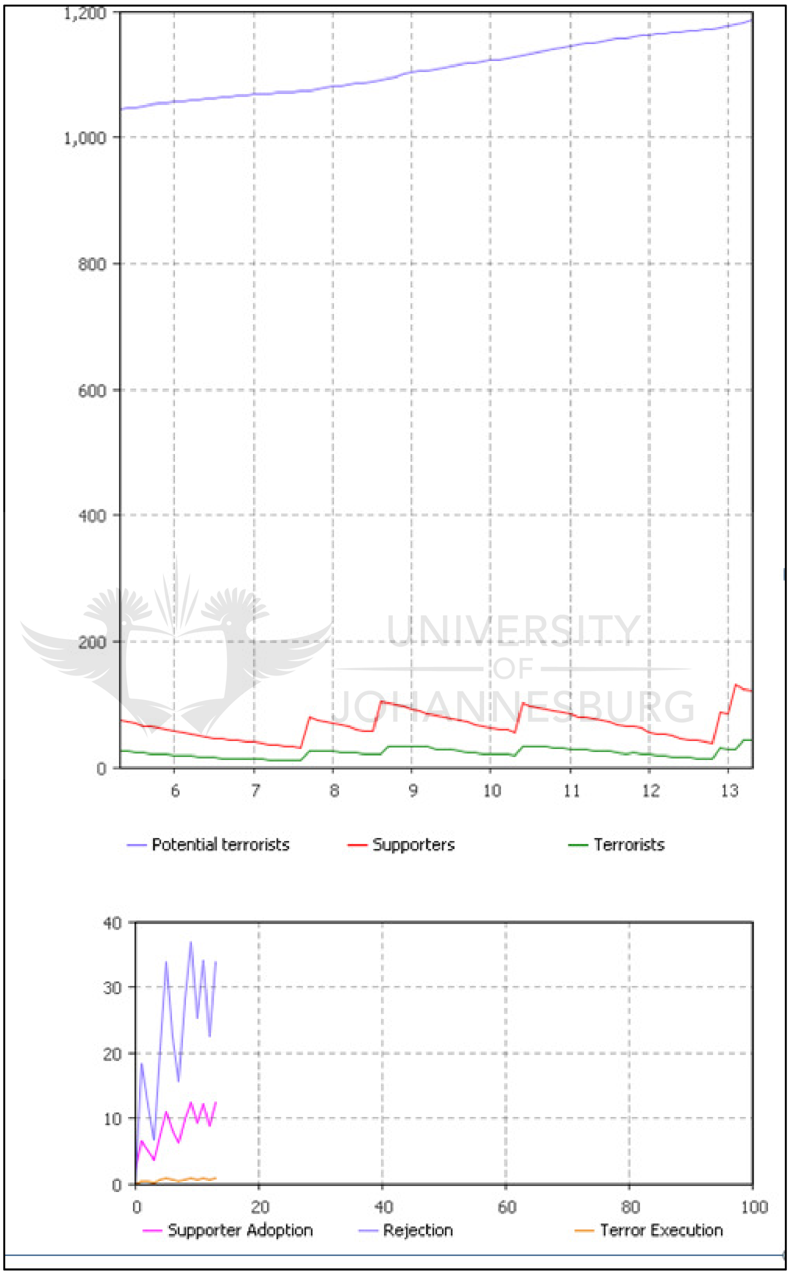


Figure 68: CLC Simulation Graphical View (Own Compilation)

Figure 68 shows the graphical view of the CLC Simulation (Please note that the graphs are produced by the software without any labels. The author was not able to insert labels due to the software restrictions). These graphs capture the growth over time in:

-

1. PotentialTerrorists (Population), Terrorist Supporters and Terrorists
    a) X-axis shows Time
    b) Y-Axis shows number of people
2. Adoption Rate, Rejection Rate and Execution Rate
    a) X-Axis shows Time
    b) Y-Axis shows Rate

The graphs are automatically configured using the pre-defined time plot element in AnyLogic. The two timings of the graphs cannot be configured to map each other since they represent different aspects of the cyberterrorism field.

This population growth is indicated by the purple line that steadily moves upward (typical population growth behaviour). The CLC Simulation commences with 1000 people who become PotentialTerrorists. As the simulation proceeds, people may be born, die, change into supporters/terrorists and even reform. This movement is captured graphically in Figure 68 and the video.

The *TerroristSupporters* numbers are shown in red. This line has frequent fluctuations- showing the constant growth and decrease in support. In addition, the line spikes periodically. This correlates to random events that may cause an uproar or uprising in terrorists groups and thus lead to an influx of support.

The growth in terrorists is shown on the green line. This demographic group is by far smaller. It also has periodic jumps to show unpredictable terrorist practices.

On the second graph, the *Rejection* rate is indicated in purple. It is by far much higher that the Adaptation (into *TerroristSupporters*). It oscillates quite frequently to show the fluctuation in rejection and adoption but rejection will always be considerably higher than adoption and execution. Execution is a slight oscillating wave shown in orange at the bottom of the graph to depict the slight adaptation of supporters into terrorists.

Figure 69 shows another screenshot from the simulation after some time has elapsed. The population has now grown to just over 1400. The *TerroristSupporters* and *Terrorists* graphs continue to oscillate with frequent spikes correlating to an event increasing interest in a terrorism cause. Similarly, the *Adoption* and *Rejection* graphs fluctuate slightly with *Rejection* also slowly alternating to some extent.

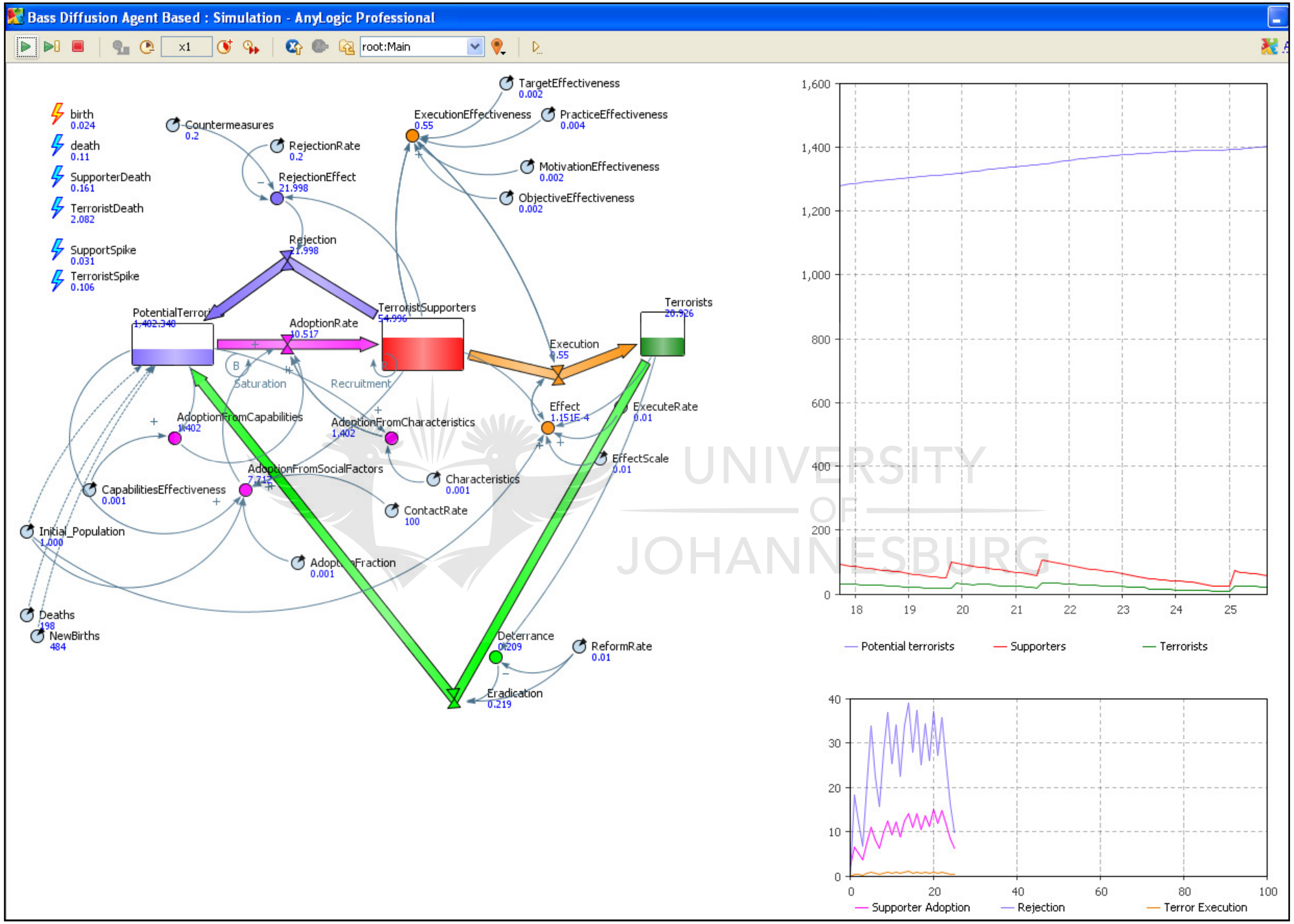


Figure 69: Simulation of Cyberterrorism (Screenshot 2) (Own Compilation)

12.4 Reduction in Countermeasures

One of the uses of simulations is to run different experiments and test different theories. In this model, one such hypothesis is to determine the effect of lowering countermeasure efforts. It is predicted that the number of *TerroristSupporter* and *Terrorists* will increase much more rapidly. A comparison of the scale of *TerroristSupporters* and *Terrorists* with lowered countermeasures is carried out in this section. Figure 70 and the video on the accompanying CD show the output of the simulation when the countermeasures are at a high level.

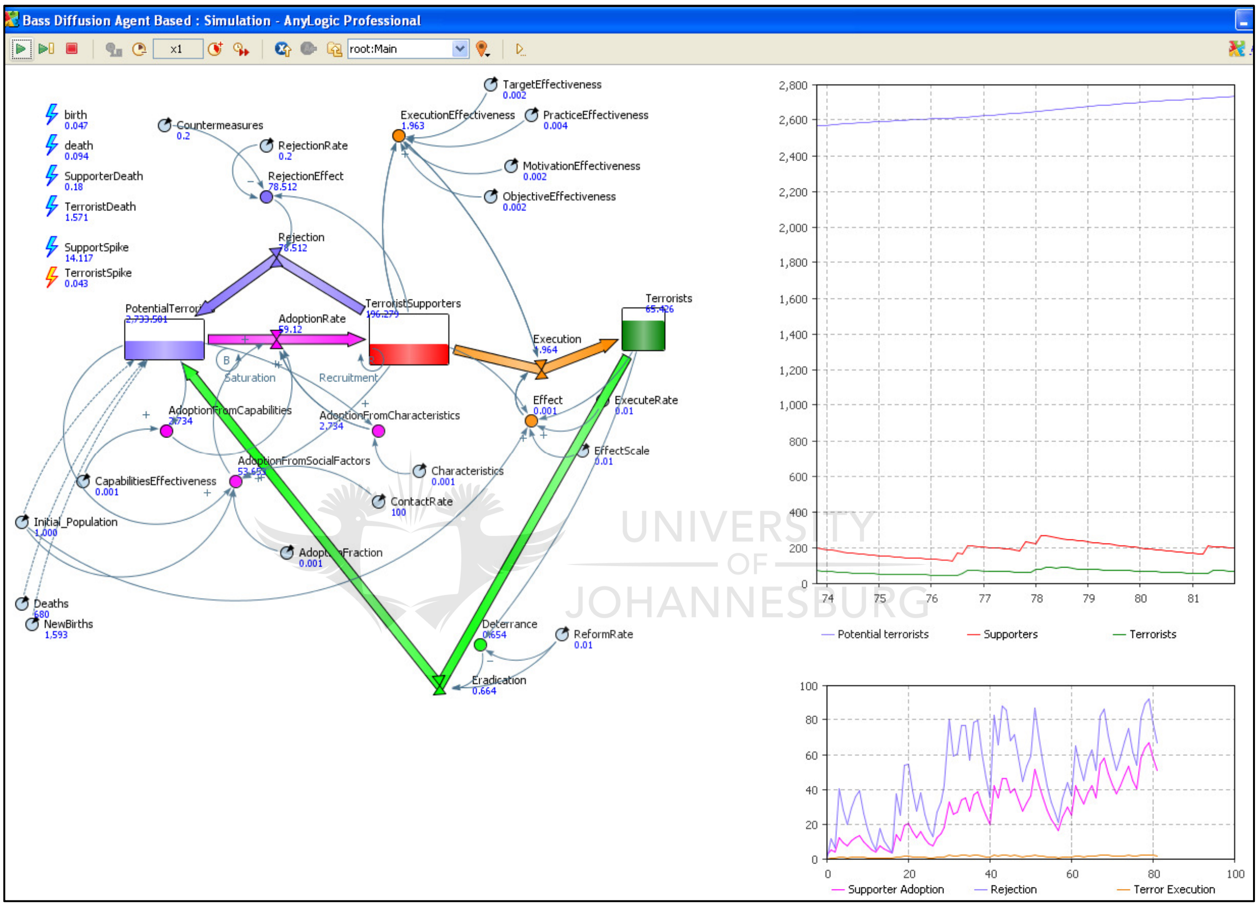


Figure 70: Simulation of Cyberterrorism – High Countermeasures (Screenshot 3) (Own Compilation)

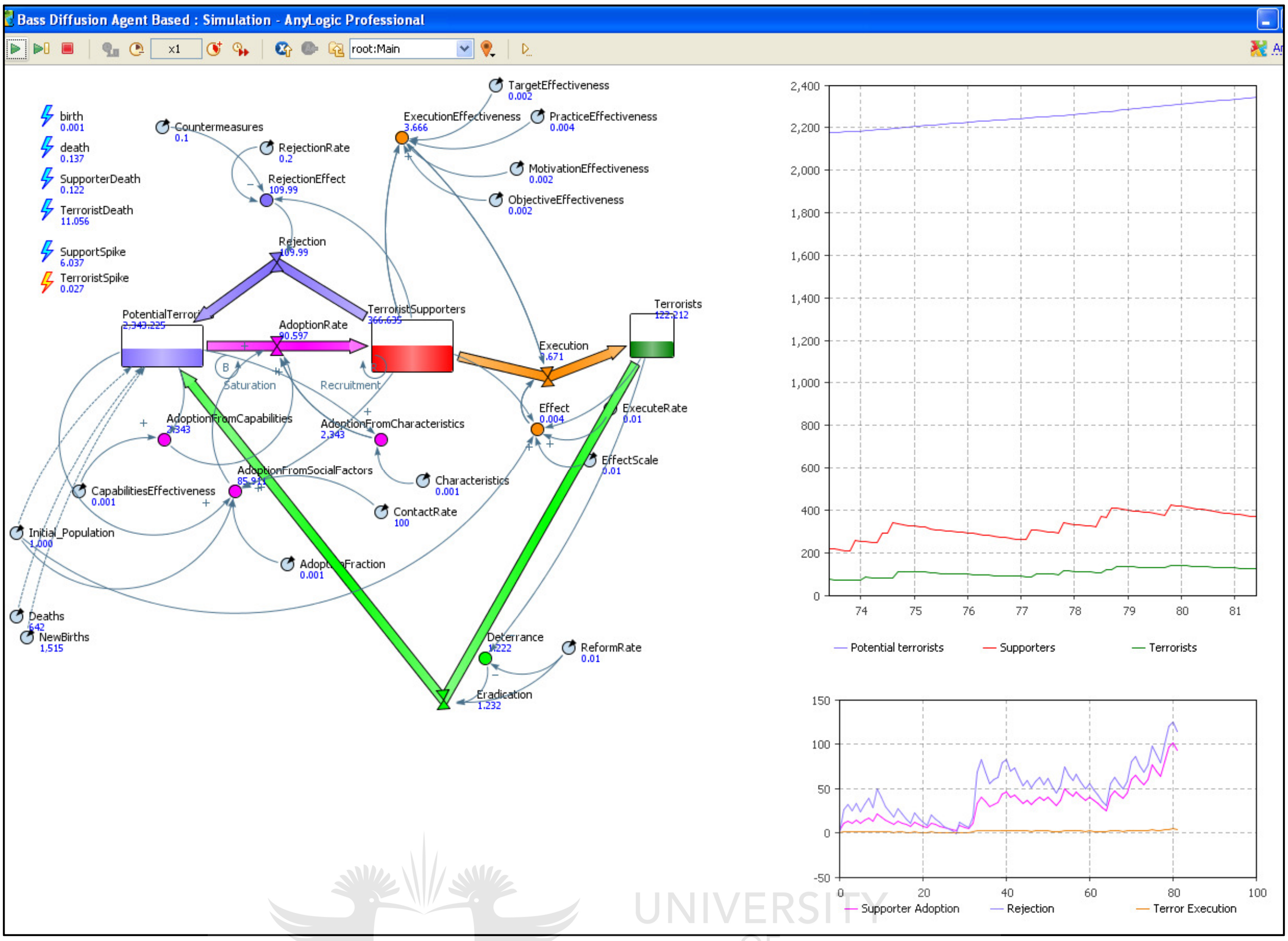


Figure 71: Simulation of Cyberterrorism – Lowered Countermeasures (Screenshot 4) (Own Compilation)

The results in the graph in Figure 71 and the video show substantial jumps in the number of *TerroristSupporters* and *Terrorists*, which supports the original hypothesis. A comparison demonstrates that the *TerroristSupporter*s numbers reach above 200 and even approaches 400 in Figure 71. This is far more significant than Figure 70 since there are stronger countermeasures in place (TerroristSupporter numbers only reach 200). The *TerroristSupporter Spike Event* is shown as a lightning flash in both Figure 70 and Figure 71.

Over time, the *TerroristSupporters* and *Terrorists* will continuously increase at a sharp rate. Figure 72 (and the video) shows the number of supporters reach 600. This shows that if countermeasures are not strongly carried out, this will result in a sharp increase in the support and execution of terrorism.

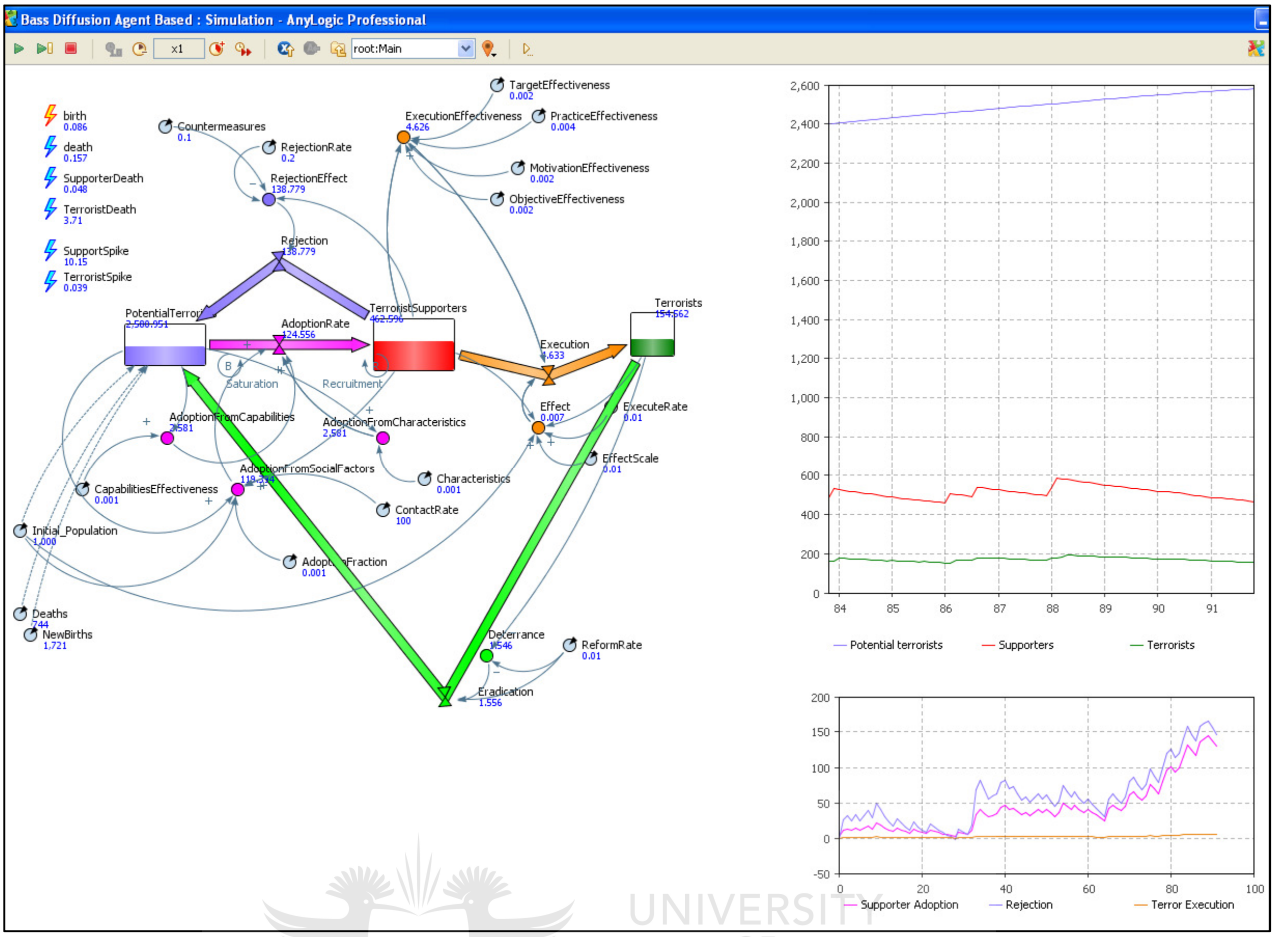
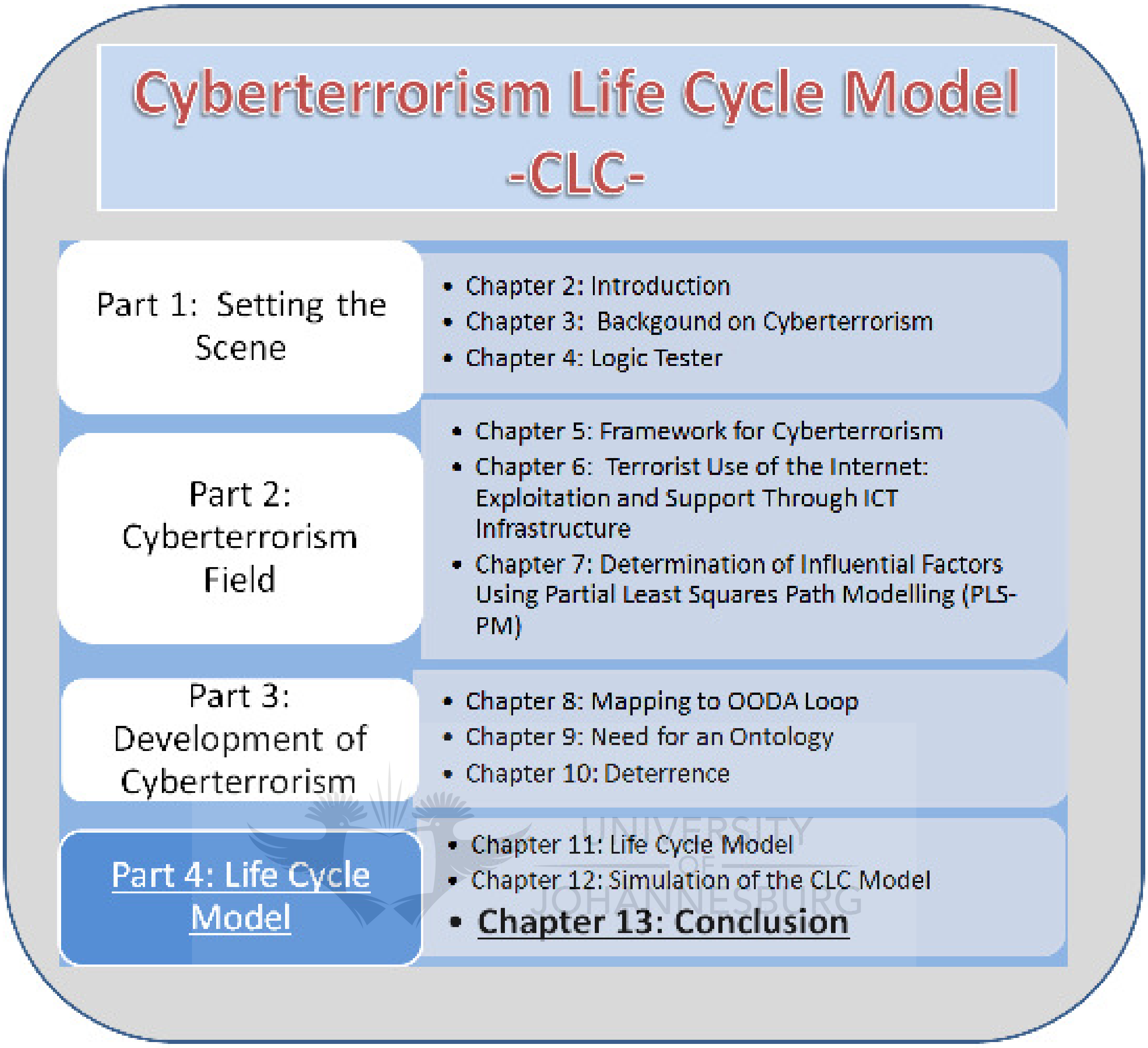


Figure 72: Simulation of Cyberterrorism – Lowered Countermeasures (Screenshot 5) (Own Compilation)

12.5 Summary

Part 4 forms the crux of this research and shows how all the different aspects of the study fit together. Part 4 links all the research findings together by presenting the CLC model, as well as dynamic representation of the CLC model using simulation techniques. The simulation presented encapsulates the theoretical concepts of the CLC model in a practical manner to indicate how a population may adopt and reform from terrorist behaviour.

Chapter 13 is the final chapter of this thesis and provides a conclusion to the research, as well as the benefits of the CLC model and future work. Chapter 13 will also evaluate the research carried and demonstrate how the objectives were addressed throughout this investigative study.



Cyberterrorism Life Cycle Model -CLC-

Part 1: Setting the Scene

- Chapter 2: Introduction
- Chapter 3: Backgound on Cyberterrorism
- Chapter 4: Logic Tester

Part 2: Cyberterrorism Field

- Chapter 5: Framework for Cyberterrorism
- Chapter 6: Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure
- Chapter 7: Determination of Influential Factors Using Partial Least Squares Path Modelling (PLS-PM)

Part 3: Development of Cyberterrorism

- Chapter 8: Mapping to OODA Loop
- Chapter 9: Need for an Ontology
- Chapter 10: Deterrence

Part 4: Life Cycle Model

- Chapter 11: Life Cycle Model
- Chapter 12: Simulation of the CLC Model
- **Chapter 13: Conclusion**

13 Conclusion

> *““Science, my lad, is made up of mistakes, but they are mistakes which it is useful to make, because they lead little by little to the truth.”*
>
> *— Jules Verne, A Journey to the Center of the Earth”*

This study, CLC Cyberterrorism Life Cycle Model, focussed on the development of a cyberterrorist. The motivation of this study is based on providing insight into how a cyberterrorist grows and progresses. This study showed that ICT could serve as powerful tool to support terrorism and also be a critical target.

Chapter 2 argued that terrorists are now embracing the realm of ICT and cyberspace in order to voice their politically, religiously or ideologically motivated viewpoints. Terrorists now recognise the importance of critical information infrastructure (CII) and realised that an attack of critical information services or infrastructure is an apt method of reaching high-profile targets and generating interest in their movement. This has led to a strong need to understanding how cyberterrorism develops and how it can be deterred.

13.1 Introduction

Figure 73 shows that the approach used in the CLC research was to establish the theory, find data and then build models in order to explain, clarify and describe the field of cyberterrorism.

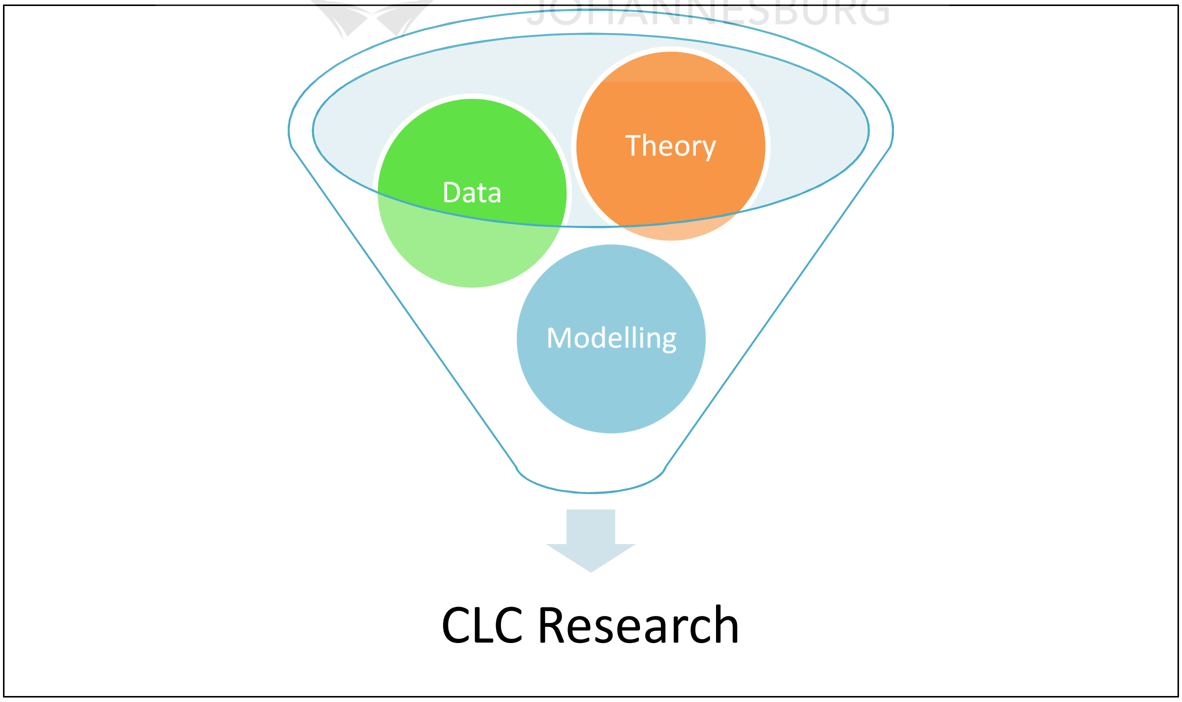


Figure 73: CLC Research Approach (Own Compilation)

The research problem, introduced in Section 2.1, states that in the past, terrorism mainly operated in the realm of bombings, gas attacks and kidnappings but it has now entered the domain of cyberspace. Cyberterrorism is strongly influenced by behavioural forces that motivate attacks and technical aspects, which affect how attacks are executed. Furthermore, ICT can be both a weapon and the target of attacks. However, there is no structured representation showing the dynamic interaction of these influential and technical aspects.

This research study discussed the development of the Cyberterrorism Life Cycle Model - CLC. The CLC model is a wide-ranging model that encapsulates the various aspects associated with cyberterrorism, reflecting social factors, characteristics, motivation, capabilities, objectives, targets, effects and practices of cyberterrorism. The study is divided into four related parts, with each part directly contributing to the development of the CLC model. The four parts of this research, (originally shown in Figure 1) are:

- Part 1: Setting the Scene
- Part 2: Cyberterrorism Field
- Part 3: Development of Cyberterrorism
- Part 4: Life Cycle Model

These four parts were designed to help develop a comprehensive model depicting the cyberterrorism life cycle in Chapter 11. The research in the first three parts helped formulate drivers, which served as input to the CLC model, whilst the last part addressed the development and implementation of the CLC model. The next section discusses each of the twelve chapters to establish whether the research study has met its goals and objectives.

13.2 Discussion of the Research Study

Currently, cyberterrorism is a well-coined expression globally. However, it is important to differentiate between a cybercrime attack and a cyberterrorist attack. Furthermore, ICT can be used to support terrorism in general and can also be the target of attack. It is therefore vital to show practices, targets, effects and objectives that a cyberterrorist is trying to achieve. Overall, cyberterrorism is driven by behavioural components and technical aspects.

In view of these dispositions, this thesis developed a model that captures the interaction of these influential factors in the field of cyberterrorism. Table 12 shows the four parts and thirteen chapters of the study, together with its crucial evaluation.

.

Table 12: Critical Evaluation of CLC Model Development (Own Compilation)

Part/Chapter	Contents	Evaluation
Chapter 1 **CLC- Cyberterrorism Life Cycle Model**	- Introduces the study	Context of research provides strong motivation
Part 1 **Setting the Scene**	- Suitable introduction to field of cyberterrorism - Establishment and basic testing of definition - Introduction of examples and groups to show real-life cyberterrorism situations	
Chapter 2 Introduction	- Introduces reader to the field - Establishes objectives - Describes research methodology - Explains limitations	**Deliverable** - Lists sub-objectives - Lists research problem
Chapter 3 Background on Cyberterrorism	- Defines terrorism and cyberterrorism - Differentiation with cybercrime - Scenarios, incidents, driving forces, terrorist groups - Effects	**Deliverable** - Definitions - Links to sub-objective 3 - Addresses research problem
Chapter 4 **Logic Tester**	- Logic Tester Implementation - Examples using Logic Tester	**Deliverable** - Logic Tester Worksheet - Links to Sub-objective 3
Part 2 **Cyberterrorism Field**	- Focuses on the main influential factors in cyberterrorism - Investigates traditional uses of ICT for cyberterrorism and also more innovative functions - Explores the use of Partial Least Squares Path Modelling to identify social factors	

Part/Chapter	Contents	Evaluation
Chapter 5 Framework for Cyberterrorism	Framework containing: - Operating Forces (Characteristics, Target, Types, Social Factors, Capabilities) - Techniques (Practices, Attack Levels, Modes of Operation) - Objectives (Malicious Goals, Support Functions)	**Deliverable** - Framework for cyberterrorism - Links to sub-objective 4
Chapter 6 Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure	- Literature study of some of the most common cyberterrorism practices - Identification of innovative uses of the Internet - Explains to reader traditional cyberterrorism practices and novel uses of ICT	**Deliverable** - Current cyberterrorism practices - Current terrorist support functionality - Links to sub-objective 2
Chapter 7 **Determination of Influential Factors using Partial Least Squares Path Modelling (PLS PM)**	- Context of PLS Path Modelling - Survey data - Implementation and explanation of PLS Path Model to identify social factors	**Deliverable** - PLS Path Model - Links to sub-objective 4
Part 3 **Development of Cyberterrorism**	- Deeper analysis of cyberterrorism	
Chapter 8 **High-level Mapping of Cyberterrorism to the Observe-Orient-Decide-Act (OODA) Loop**	- Motivation for mapping to OODA loop - Representation of cyberterrorism influential factors using OODA loop reasoning - Establishes foundation of CLC model	**Deliverable** - Mapping to OODA loop - Links to sub-objective 4

Part/Chapter	Contents	Evaluation
Chapter 9 **Need for an Ontology**	- Introduction of uses of ontologies - Refinement of influential factors - Classification of cyber events as cyberterrorism using ontologies - Classification examples using implemented ontology	- **Deliverable** - Ontology for cyberterrorism - Links to sub-objective 3
Chapter 10 **Deterrence of Cyberterrorism**	- Investigation of strategic countermeasures - Exploration of technical countermeasures	**Deliverable** - Strategic and Technical Countermeasures to help combat cyberterrorism - Links to sub-objective 2
Part 4 **Life Cycle Model**	- Proposes CLC model - Presents CLC model simulation - Concludes research	
Chapter 11 **Cyberterrorism Life Cycle (CLC) Model**	- Presents the drivers that influences planned CLC Model - Visual representation and explanation of CLC Model	**Deliverable** - Model drivers - CLC Model - Addresses research problem
Chapter 12 Simulation of CLC Model	- Need for abstraction and simulation context - Dynamic representation of CLC Model	**Deliverable** - CLC Model Simulation - Addresses research problem
Chapter 13 **Conclusion**	- Concludes the study - Justifies development of CLC Model	**Deliverable** - CLC Model evaluation - structured representation showing

Part/Chapter	Contents	Evaluation
		the interaction of influential and technical aspects

The original research objective (in Section 2.2) is to compile a model that traces the development of a cyberterrorist by demonstrating how the ICT can be used in both the pursuit and support of terrorism. The CLC model is developed in such a way to differentiate between cyberterrorism practices and support functionality. The model explains the terrorists may use ICT to attract members into their organisation and thereafter carry out communication, fund-raising and various other supportive functions using ICT. In this way, ICT can provide an integral command and control functionality to terrorists. In addition, the life cycle model shows typical practices that are used to commit acts of cyberterrorism.

Overall, the CLC model provides a visual representation of the interaction of the various factors that influence the field. From the evaluation shown in Table 12, the conclusion is this study completed the tasks set out in Chapter 2. In addition, Table 12, also clearly indicates which chapters addressed the sub-objectives (originally depicted in Figure 3).

13.3 Problems Encountered

Although the CLC model addressed various issues relevant to the field of cyberterrorism, a number of problems were encountered during the study. Some of these issues were anticipated at the beginning of the study, but some of them only manifested during the research and development phases.

Due to the nature of the field of cyberterrorism, many of the references are Internet-based. Cyberterrorism is not yet an established field in the domain of information security due to the influence of behavioural and technical issues. The concept is often debated and thus literature pertaining to the topic often contains argumentative content. Resources are often limited to cyber experts, newspaper articles and blogs. Newspaper articles and cyber experts sometimes dispute the threat of cyberterrorism and in other cases offer a wealth of information relating to the influential factors. Blogs are not scientific in nature but do contain relevant information.

Terrorism is driven by various behavioural and psychological reasons, which fall outside of the scope of this study. During this research, high-level motivations and social factors were discussed. However, the extent of these factors was covered at a very basic level. The psychology of terrorism covers a wide domain of reasons, factors, and issues, which are not covered in this research. This area of research is complex and specialised and far beyond the bounds of this study which aimed to show a structured representation of the interaction of behavioural and technical factors.

Terrorism is a sensitive field in that it encompasses the threat or execution of violence. Death, injury and destruction of resources are all results of terrorist behaviour. Due to the delicate nature of cyberterrorism, studying actual cyberterrorism examples in detail is impractical. During the original planning of this study, I intended to complete a chapter focussed on a case study. The plan involved following a cyberterrorism attack throughout its life cycle. However, exact details of a terrorist attack are unfeasible since most cyber experts argue over the definition of cyberterrorism.

Furthermore, data related to cyberterrorism is very limited. Studies on terrorists are scarce or do not address the influential factors revealed in this study. For this reason, a survey was carried out to determine the effect of social factors. However, the study itself was limited to a few social factors. Furthermore, the statistical analysis of the data using PLS PM was challenging. My lack of statistical knowledge required that I first familiarise myself with basic principles and functioning of the R software. To carry out the PLS Path Modelling, the data had to be formatted in order to process the data. The formatting and processing of the results was rather intricate and required many improvements in order to satisfy the processing and interpretation requirements.

AnyLogic is a simulation package that provides for multi-methods like Agent-Based or Discrete-Event modelling. Since this was my first encounter with simulation software, I needed to first experiment and grasp the main principles of the tool. Thereafter, building the simulation also entailed various experiments in order to balance the data in order to capture a realistic representation of cyberterrorism. The Any Logic software thus provided its own set of challenges and tests in the process of developing the CLC model simulation.

Furthermore, another software package that was used in this research was Protégé. I first completed software training in order to learn the basics of ontology development. The implementation of the ontology in Protégé also provided a few challenges but this was tackled with an enthusiastic and persevering attitude.

The listed problems and limitations made for a very thought-provoking and challenging study. Despite these issues, the study provided an interesting and stimulating topic to research. The developed model provides a simplified yet practical and structured representation of a fairly complex field. The next section discusses the way forward with regards to cyberterrorism and the CLC model.

13.4 The Way Forward

Technology is continually evolving at a rapid pace. However, as new capabilities, tools and systems are introduced, no sooner is there a new vulnerability that can be exploited. ICT affects human life in a myriad of ways and as the dependencies on technologies grow so will the ability to interfere with critical services and systems. Attackers' strategies, techniques and practices will also evolve as new functionality and capabilities advance. As new practices are revealed, the CLC model can be updated.

The concept of cyberterrorism is highly debatable as many cyber experts claim that it is not a threat. Thus, as new arguments and theories in the field emerge, the definition can be more firmly established and clarity in the field gained. Since cyberterrorism is a highly debatable topic, as the definition is agreed upon, incidents can be classified and treated as acts of terror.

Since the field is relatively new, many of the factors covered in this study can be further investigated. This study can serve as an ideal starting point for familiarisation with the field of cyberterrorism. Compared to current literature, this study comprises of various issues that are relevant to cyberterrorism instead of just presenting one short argument usually found in news articles, reports and blogs. The study can thus provide the background knowledge, context and practical representation to familiarise a novice on the topic.

Due to the debate that rages on about cyberterrorism, it is difficult to classify an incident and address the issues as such. Cyberterrorism statistics are rare, if not non-existent. As the field evolves and is more firmly established, cyberterrorism attacks can be classified as such. The proposed ontology will serve as an ideal tool for this task. The ontology can be further expanded as new definitive concepts are established.

The CLC model discusses the influential factors that cover the principles and concepts relevant to this field. Cyberterrorism is strongly dependant on the use of ICT, which in itself is subject to continuous improvements, changes and advancement. As these new ICT developments occur, so too can the various practices, objectives, targets, effects, characteristics and capabilities. New additions to the CLC model can also be updated to the simulation.

More research can be carried out to gather statistics on cyberterrorism. This could be used to perform more statistical analysis like regression or PLS PM. These techniques can help explain, describe and explore the social factors and motivations that drive cyberterrorism.

The simulation of cyberterrorism could also be implemented in a number of ways. Actual cyberterrorist incidents could be simulated showing the effect, practice, target, capabilities and objectives. There is a host of opportunities within the area of simulation.

Even though the study encountered a few limitations and issues, it still provided a valuable opportunity to research a topical and thought-provoking field. Various spin-off research ideas stemmed from the study and can be further investigated.

13.5 Summary

The political and ideological drive for terrorism together with the emergence of technological capabilities has created a new realm for terrorist activity. However, ICT can also support terrorism in general. Nor should it be confused with traditional cybercriminal activities. Cyberterrorism is influenced by various factors like motivation, characteristics, social factors, effects, target, capabilities and practices. This study showed the interaction of these various factors in a structured representation.

Considering the study as a whole, it successfully completed all the objectives set out to establish a structured representation of the cyberterrorism field. As this new risk threatens civilians and the government through the technological landscape, it is imperative that knowledge is created on its influential factors to develop ways of deterrence. This study shows the interaction of these various factors, as well as strategic and technical methods of deterrence. This research thus provides an apt representation to clarify a frequently mis-conceived field and provide greater insight into the operating forces, techniques and objectives driving cyberterrorism.

14 Publications and Presentations

> *"Cyberterrorism is, to be sure, an attractive option for modern terrorism who value its anonymity, its potential to inflict massive damage, its psychological impact and its media appeal"*
>
> *- US Institute of Peace*

1. **Towards a Conceptual Framework for Cyberterrorism**	
Author:	N Veerasamy
Date	26 March 2009
Type	Conference 4th International Conference on Information Warfare and Security (reviewed and published)
ISBN	978-1-906638-28-3
Abstract	Terrorism has entered a new wave in that the latest battleground to emerge is cyberspace. Cyberterrorism reflects a current concern in the way terrorists will seek to strike the innocent and wreak havoc. Since explosives are no longer the only means to bring a system down, many are uneasy about random cyber attacks that could leave us with difficult conditions due to the disruption of critical services. Because of our increased dependency on networked communications, the outcomes of such interruptions could be quite disastrous. Cyberterrorism is an aspect of cybercrime that has thus become a growing interest in this the Digital Age. Various hacking and computer intrusion scenarios could possibly play a critical role in cyberterrorism. In the global battle of information and network warfare, cyberterrorism has become a more dominant force. However, much misconception exists over what exactly cyberterrorism entails. Media has sensationalised the possibility of cyberterrorism attacks causing great havoc. Images of eccentric activists taking down critical infrastructures like power stations or railway lines bombard us. Many live in fear of the possibility of vital resources being taken down. The role of security violations and hacking techniques also need to be better investigated to better understand the reality of such threats. Various theories surround cyberterrorism. However, there is a need for a more structured approach to understanding the various components of cyberterrorism. A conceptual framework outlining the core aspects of cyberterrorism is therefore proposed.

1. **Towards a Conceptual Framework for Cyberterrorism**	
	This paper focuses on clarifying the field of cyberterrorism through a conceptual framework that addresses the techniques, objectives, target, types, effects, characteristics and capabilities required. The framework strives to provide a more descriptive synopsis of the field of cyberterrorism. It therefore aims to form a good baseline to place the area of cyberterrorism in context against the backdrop of other computer and network related crime.

2. **A Conceptual High-level Framework of Cyberterrorism**	
Author:	N Veerasamy
Date	April 2009
Type	International Journal of IW, Vol 8, Issue 1 (reviewed and published)
ISSN	1445-3312 (Printed) 1445-3347 (Online)
Abstract	Uneasiness arises from the possibility of random cyber attacks. In the global information and network warfare battle, cyberterrorism has become a critical concern in that terrorists may seek to strike the innocent and wreak havoc due to dependency on networked communications. However, much misconception exists over what exactly cyberterrorism entails and the role of cybercrime and hacking. A conceptual framework is therefore proposed and focuses on clarifying the field by summarising techniques, objectives, targets and capabilities. The framework strives to provide a more descriptive synopsis of cyberterrorism and form a good baseline to place the area of cyberterrorism in context against the backdrop of other computer and network crime.

3. **An Introduction to Emerging Threats and Vulnerabilities**	
Author:	N Veerasamy and B Taute
Date	6-8 July 2009
Type	Conference Information Security South Africa (ISSA) (reviewed and published)
ISBN	978-1-86854-740-1
Abstract	With technological change and advancement, attackers are increasingly becoming more sophisticated in their attack strategies and techniques. Other global factors and developments also impact the line of attack. This paper provides an introduction to the most current, pertinent attack strategies and trends. It aims to create an awareness of emerging areas that should be better studied and understood. The paper addresses the blurring lines of cybercrime, information warfare and cyber terror to indicate the key concerns at a national, commercial, governmental and individual level. Thus, the paper proposes and discusses topical security threats to elucidate their methodology and gauge their impact such that further strategic, operational and technical measures can be taken

4. **The Different Faces of Cyberterrrorism**	
Author:	N Veerasamy
Date	20-23 July 2009
Type	Symposium Military Information and Communications Symposium of South Africa (MICSSA)

4. The Different Faces of Cyberterrrorism	
Abstract	The Different Faces of Cyberterrrorism, Network centric operations and warfare provides for tremendous interoperability in terms of the synchronisation and integration provided by computer networks and communication systems. Network centric operations encapsulate various activities relating to the sharing, accessibility and protection information and thus promote creativity and innovation. The battle space and field of operations now extends to the virtual world of networks and cyberspace, and even though enhanced functionality is provided by the various technologies, the potential threats and risks should not be overlooked. Cyberterrorism reflects an emerging wave of Information warfare in that cyberspace is now being used as the battleground to promote political/social activism. However, cyberterrorism encompasses both social aspects as well as the technical means through which exploitation is carried out. Thus, it is imperative to consider both the practical implications as well as the psychological factors to ensure that increased interoperability does not cause a disproportionate risk to be introduced. This paper outlines the various factors contributing to the field of cyberterrorism. The paper focuses on showing the key considerations that arise from this form of cyberwarfare and the possible implications, for example financial, psychological, operational, etc. The aim of this paper is to create awareness of the development, execution and impact of cyber terrorist activities.

5. A High-level mapping of Cyberterrorism to the OODA loop	
Author:	N Veerasamy and M Grobler
Date	9 April 2010
Type	Conference International Conference on Information Warfare and Security (reviewed and published)
ISBN	97-1-906638-60-3
Abstract	Cyberterrorism relates to the convergence of the two worlds of terrorism and cyberspace. Technically cyberterrorism can be carried out through various information security exploits like targeting Supervisory Control and Data Acquisition (SCADA) systems or Denial-of - Services attacks on critical governmental web sites. Various factors have an influence on cyberterrorism and include the social factors, capabilities, goals, modes of operation and practices. In order to analyse how these various factors influence the development of a

5. A High-level mapping of Cyberterrorism to the OODA loop	
	cyberterrorist, a mapping to the Observe- Orient, Decide, Act (OODA) loop is proposed. The OODA loop, previously proposed by Col. John Boyd, provides an apt framework to structure and describe issues that contribute to the development and operation of a cyberterrorist. The aim of this paper is to describe how various observations made by sections of the world population direct people into making decisions and committing acts of cyberterror. The paper will thus look at issues like the environmental factors, social standing, culture, religion, tribal relations, loyalties, and the drive for power and self-fulfilment. In addition, the mapping will also consider how information is received, transformed and utilised by cyberterrorists, by considering the evolution of information in the Information Hierarchy. The proposed model will thus map various aspects pertinent to the field of cyberterrorism to capture a more dynamic representation of the interacting forces. The mapping will try to show the main relationships between the OODA loop, Information Hierarchy and various factors like characteristics, social factors, terrorist types, capabilities, goals, targets, attack levels, support functions, practices and modes of operation. Overall, the goal of this paper is to succinctly represent some of the psychological and technical issues relating to cyberterrorism. The OODA loop will be utilised to convey these ideas as well mapping to other relevant fields like the Information Hierarchy. Overall, various components that impact the field of cyberterrorism will be integrated to show a more holistic representation of various operating forces.

6. Motivation for Cyberterror	
Author:	N Veerasamy
Date	2 August 2010
Type	Conference Information Security South Africa (ISSA)
Abstract	Cyberterrorism represents the convergence of the virtual world of cyberspace and the intimidation techniques of terrorism. To better understand why cyber terrorist acts are committed, this paper investigates the motivation behind terrorism by looking at traditional terrorist groups and how their objectives can be met by Information and Communication Technology (ICT). This paper addresses the reasoning behind cyberterror by discussing a few incidents and elaborating on known terrorist groups before providing a classification of

6. **Motivation for Cyberterror**	
	terrorist types and an explanation of some support terrorist functions with regard to ICT infrastructure. In this way, insight can be gained into the objectives that are trying to be achieved by terrorist organizations, as well as shedding light into real-life groups and their operations.

7. **Determining vulnerabilities: The understanding of attacks and security breaches i.e. Cyberterrorism, Hacking, Cybercrime and Denial of Service Attacks**	
Author:	N Veerasamy
Date	October 2010
Type	Seminar Ekwinox Information Warfare and Cyberterrorism Seminars
Abstract	Lecture on the following topics: An introduction to emerging threats and vulnerabilities to create awareness Cyberterrorism an cybercrime Threats (hacking and security exploits) High-level methodology for carrying out attacks Botnets and Denial-of-Service capabilities

8. **Countermeasures to Consider in the Combat against Cyberterrorism**	
Author:	N Veerasamy
Date	11 October 2010
Type	Workshop Workshop on ICT Uses in Warfare and the Safeguarding of Peace (reviewed and published)
ISBN	978-0-620-47586-0

8. Countermeasures to Consider in the Combat against Cyberterrorism	
Abstract	Cyberterrorism addresses the convergence of the fear-causing world of terrorism with the abstract realm of cyberspace, computers and networks. While cyberterrorism can be executed using various technical security exploits, it inherently stems from various social, political or religious views. This paper presents an overview of the motivating forces behind cyberterrorism which can provide the baseline to develop a countermeasure strategy. In this paper, countermeasures that can be used to deter cyberterrorism from both these psychological and technical perspectives are covered. It provides a high-level overview of the fight against terrorism and discusses countermeasures that can be used to combat cyberterrorism to create awareness.

9. Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure	
Author:	N Veerasamy and M Grobler
Date	17 March 2011
Type	Conference International Conference on Information Warfare and Security (ICIW) (reviewed and published)
ISBN	97-1-906638-92-4
Abstract	The growth of technology has provided a wealth of functionality. One area in which Information Communication Technology (ICT), especially the Internet, has grown to play a supporting role is terrorism. The Internet provides an enormous amount of information, and enables relatively cheap and instant communication across the globe. As a result, the conventional view of many traditional terrorist groups shifted to embrace the use of technology within their functions. The goal of this paper is to represent the functions and methods that terrorists have come to rely on through the ICT infrastructure. The discussion sheds light on the technical and practical role that ICT infrastructure plays in the assistance of terrorism. The use of the Internet by terrorist groups has expanded from traditional Internet usage to more innovative usage of both traditional and new Internet functions. Global terrorist groups can now electronically target an enormous amount of potential recipients, recruitees and enemies. The aim of the paper is to show how the Internet can be used to enable terrorism, as well as provide technical examples of the support functionality and

9. **Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure**	
	exploitation. This paper summarises the high-level functions, methods and examples for which terrorists utilise the Internet. This paper looks at the use of the Internet as both a uni-directional and bi-directional tool to support functionality like recruitment, propaganda, training, funding and operations. It also discusses specific methods like the dissemination of web literature, social-networking tools, anti-forensics and fund-raising schemes. Additional examples, such as cloaking and coding techniques, are also provided. In order to analyse how ICT infrastructure can be used in the support of terrorism, a mapping is given of communication direction to the traditional Internet use functions and methods, as well as to innovative Internet functions and methods.

10. **Terrorist Use of the Internet: Exploitation and Support Through ICT Infrastructure**	
Author:	N Veerasamy and M Grobler
Date	October 2011
Type	Book chapter Leading Issues in Information Warfare & Security Research
ISBN	978-1-908272-08-9
Editorial Commentary	The concept of cyberterrorism is one, which is hyped by politicians and scorned by many technologists. In this paper, Veerasamy and Grobler point out the real use that terrorists have for the Internet and other communications infrastructure: that of recruiting, that of fund-raising, and that of communicating between themselves. Numerous examples of how these activities are conducted are included. This paper builds upon the previous two by examining the role of non-state actors in competition and conflict in the modern era. This issue is a serious one for those concerned with national security because the goal of the terrorists is to undermine and unseat established governmental structures. Their use of the communications infrastructure is so far relatively benign, if one can consider raising and funding an army benign, but the potential enormous. Through these actions, the terrorists show an appreciation for the technological infrastructure and a fairly sophisticated imagination of how to use these technologies for their various goals. Should these goals and capabilities turn towards acts of armed aggression in cyberspace in the future, it may well be within their capabilities.

11. <u>Building an Ontology for Cyberterrorism</u>	
Author:	N Veerasamy, M Grobler, S von Solms
Date	5 July 2012
Type	Conference European Conference on Information Warfare and Security (reviewed and published)
ISBN	978-1-908272-56-0
Abstract	Cyberterrorism and the use of the Internet for cyberterrorism is an emerging field. Often cyberterrorism activities overlap with traditional hacking and Information and Communication Technology (ICT) Infrastructure exploitation. As a result, the defining and differentiating characteristics of cyberterrorism can easily be misunderstood. The use of an ontology specifically developed for cyberterrorism, will provide a common framework to share conceptual models. By using an ontology, the internal and external environment of a field (in this case, cyberterrorism) can be captured together with the relationships between the environments. This paper proposes an ontology to identify whether a cyber event can be classified as a cyberterrorist attack or a support activity. The role of the cyberterrorism ontological model will be to provide a better structure and depiction of relationships, interactions and influencing factors by capturing the content and boundaries in the field of cyberterrorism. The ontology will be developed using a cyberterrorism framework covering influencing factors, together with a compiled network attack classification ontology. Classes will be drawn from research carried out on the use of ICT in the support of cyberterrorism. As defined in this research, a cyberterrorism attack consists of a high-level motivation that is religious, social or political. The individual/group can furthermore be classified as having a specific driving force depending of the level of extremism or revolutionary thinking. Thus, the ontology will take into consideration the motivating characteristics that play a significant role in contributing towards the definition of cyberterrorism. Overall, this paper promotes the understanding of the field of cyberterrorism and its relation to ICT manipulation, together with the use of the Internet to support terrorism in general. Ontologies enable a common view on a specific domain to generate knowledge that can be shared and reused. Ontologies can further be populated with specific dynamic instances of information and therefore can be used to generate real-world scenarios. In this paper, the proposed ontological model will form a knowledge base for the field of cyberterrorism and will provide instances that aim to convey realistic cyberterrorism situations and support examples.

12. Towards a Cyberterrorism Life Cycle (CLC) Model	
Author:	N Veerasamy and M Grobler
Date	16 August 2012
Type	Workshop 4th Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2012 (IWSP 2012)
ISBN	978-1-86840-727-7
Abstract	Cyberterrorism has emerged as a new threat in the Information and Communication Technology (ICT) landscape. The ease of use, affordability, remote capabilities and access to critical targets makes cyberterrorism a potential threat to cause wide-scale damage. Cyberterrorism is often incorrectly perceived as encompassing all cybercrimes. However, cyberterrorism differs from cybercrime in various ways including motivation, attack goals, techniques and effects. Motivations for cyberterrorism, which is similar to terrorism in general, stem from religious, social and political views. Cyberterrorists generally would seek to have high impact in order to gain publicity for their cause, whereas cybercriminals often prefer to have their acts undetected in order to hide their financial theft, fraud or espionage. Therefore, there are various factors that drive the development of a cyberterrorist. This paper proposes a model for the development of cyberterrorism in order to show the various influential forces. The Cyberterrorism Life Cycle (CLC) model presented in this paper is composed of five phases: Prepare, Acquaint, Choose, Execute, and Deter (PACED). In addition the paper looks at various factors, including social, practices, objectives, targets and countermeasures, which are mapped onto the PACED phases in order to show the interaction and dynamic nature during the life cycle development

13. Cyberterrorism versus Cybercrime	
Author:	N Veerasamy and M Grobler
Date	15 October 2012
Type	Science Talk Presentation at Council for Scientific and Industrial Science Published on CSIR news http://intraweb.csir.co.za/news/articles/2012/11/CyberSecurity.php

13. Cyberterrorism versus Cybercrime

Abstract

Attacks in cyberspace are often publicised as cyberterrorism. However, in many cases the incidents are merely cyber criminals or hackers penetrating systems. Cyber-terrorism represents an emerging wave of cyber-based attacks in which cyberspace is now used as the battleground to promote political or ideological terrorism. Cyber-terror – like any other form of terror – involves the promotion of personal, social or political agendas. The tools and targets are merely reaching into cyberspace and IT-based devices and infrastructure. The acts may not be as violent as an explosion, but from a basic point of view the fear that is generated remains. Immense anxiety and concern can stem from the possibility of imminent attacks. The malicious parties can thus create great apprehension in the hearts of a nation with warnings of violence or disruptions to critical services. Thus, the underlying goals of fear creation and publicity may still be achieved. Terrorism may have moved into the Digital Age, but the fundamental principles of violence, fear and promotion of objectives still prevail.

In this talk, the fundamental aspects of cyber-terrorism will be discussed in order to distinguish between cybercrime and cyber-terrorism. The talk will also look at typical techniques used by cyber terrorists and cyber criminals, as well as preventative measures. This discussion will provide key factors that contribute to the field of cyber-terrorism. This includes the motivating forces, together with the technical means of carrying out an attack. Overall, the talk will provide insight into common attack methods that can form part of both cybercrime, as well as cyber-terrorism.

In addition, the talk will cover an overview of carrying out an attack to show the approach of an offensive perpetrator. This aims to educate users on the dangers of poor cyber-security practices. Furthermore, the talk will cover the description of a few terrorist groups and examples in order to show the links between the motivations discussed to actual events. This talk aims to create awareness of cyber safety, as well providing information relating to the field of cyberterrorism.

15 Citations

Countermeasures to consider in the combat of cyberterrorism	
Citation 1	
Paper	A dynamic cyberterrorism framework
Author:	Rabia Ahmad and Zahri Yunos
Date	2012
Type	Journal International Journal of Computer Science and Information Security Vol 10, No 2
ISSN	1947-5500
Citation 2	
Paper	Collaboration as protective measure against cyber warfare in South Africa
Author:	Marthie Grobler and Joey Jansen van Vuuren
Date	21 June 2012
Type	Journal African Security Review, Vol 21, Issue 2
Digital Object Identifier (DOI)	10.1080/10246029.2012.654803

Motivation for Cyberterrorism	
Citation 3	
Paper	A dynamic cyberterrorism framework

Motivation for Cyberterrorism	
Author:	Rabia Ahmad and Zahri Yunos
Date	2012
Type	Journal International Journal of Computer Science and Information Security Vol 10, No 2
ISSN	1947-5500
Citation 4	
Paper	Understanding cyberterrorism: The grounded theory method applied
Author:	Rabia Ahmad, Zahri Yunos Sahib
Date	2012
Type	Conference (Peer Reviewed) International Conference on Cyber Security, Cyber Warfare and Digital Forensics (CyberSec)
ISBN	978-1-4673-1425-1 (Print)
Citation 5	
Title	Culture and Computer Network Attack Behaviours
Author	Charmaine Sample
Date	April 2013
Type	Dissertation (Capitol College, USA)
Available	Google Books

Introduction to emerging threats and trends to create user awareness	
Citation 6	
Paper	Broadband broadens scope for cyber crime in Africa
Author:	Marthie Grobler and Joey Jansen van Vuuren
Date	2-4 August 2010
Type	Conference Paper (Peer reviewed) Information Security South Africa (ISSA) 2010
ISBN	978-1-4244-5493-8
Citation 7	
Paper	Fostering content relevant to information security awareness through extensions
Author	M Potgieter, C Marais, M Gerber
Date	2013
Type	Journal (Peer reviewed) Information Assurance and Security Education and Training IFIP Advances in Information and Communication Technology Volume 406
ISBN	978-3-642-39376-1 (Print) 978-3-642-39377-8 (Online)
Citation 8	
Title	Comprehensive legal approach to cyber security
Author	E Tikk
Date	2011

Introduction to emerging threats and trends to create user awareness	
Type	Dissertation
Available	http://dspace.utlib.ee/dspace/handle/10062/17914

High-level mapping of cyberterrorism to the OODA loop	
Citation 9	
Paper	Comparing models of offensive operations
Authors	T Grant, I Burke, R van Heerden
Date	March 2012
Type	Conference (Peer reviewed) International Conference on Information Warfare and Security
ISBN	978-1-908272-30-0 (CD) 978-1-908272-29-4 (Printed)

16 References

Ahmad, R. & Yunos, Z. 2012, "A dynamic cyber terrorism framework", *International Journal of Computer Science and Information Security*, vol. 10, no. 2, pp. 149-158.

Ahmad, R., Yunos, Z. & Sahib, S. 2012, "Understanding cyber terrorism: The grounded theory method applied", *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* IEEE, pp. 323.

Answers.com. 2013*, Information*, Answers.com, [Online]. Available: http://www.answers.com/topic/information, Accessed 2013/12/12.

Anylogic.com 2013, AnyLogic Multi-method Simulation Software. Available: http://www.anylogic.com/overview, Accessed 2013/11/12.

Armistead, L. 2004, *Information operations: Warfare and the hard reality of soft power,* Potomac Books Inc, Dulles, VA, USA, pp. 93.

Arquilla, J. & Ronfeldt, D.F. 2001, *Networks and Netwars: The future of terror, crime, and militancy,* Rand Corporation, Santa Monica, California, USA, pp. 41-45.

Ashenden, D. 2011, "Cyber security: Time for engagement and debate", *Proceedings of the 10th European Conference on Information Warfare and Security*, Tallinn, Estonia, pp. 11-16.

Atwan, A. 2006, *The secret history of Al Qaeda,* 1st edn, University of California Press, California, pp. 122-256.

Australian Government 2002*, Australia Security Legislation Amendment (Terrorism) Act*, Comlaw.gov.au, [Online]. Available: http://www.comlaw.gov.au/Details/C2004C01314, Accessed 2013/12/14.

Bass, R. & Ho, S.M. 20070313 2007, "AP: 1M archived pages removed post-9/11", USA Today, Section News, Available: http://www.usatoday.com/news/washington/2007-03-13-archives_N.htm, Accessed 2010/06/23.

Biersteker, T.J. & Eckert, S.E. 2007, *Countering the financing of terrorism,* Routledge, United States and Canada, pp. 139.

Boyd, J. 1987, *A discourse on winning and losing*, Maxwell Air Force Base, AL: Air University Library Document No. M-U 43947.

Brachman, J.M. 2006, "High-tech terror: Al-Qaeda's use of new technology", *Fletcher Forum of World Affairs*, vol. 30, pp. 149.

Bright, P. 2011, "Anonymous speaks: The inside story of the HBGary hack", Ars Technica, vol. 15.

Bronskill, J. 2001, "CSIS on alert for cyber saboteurs: spy agency monitors threat to computer networks", *Ottawa Citizen*, vol. 9, pp. A3.

Brunst, P.W. 2010, "Terrorism and the Internet: New threats posed by cyberterrorism and terrorist use of the Internet" in *A war on terror?*, ed. P.W. Brunst, Springer, pp. 51-78.

Carr, J. 16 August 2007, "Anti-forensic methods used by Jihadist web sites", E Security Planet, Available: http://www.esecurityplanet.com/trends/article.php/3694711/Anti-Forensic-Methods-Used-by-Jihadist-Web-Sites.htm, Accessed 2010/05/13.

Cashell, B., Jackson, W.D., Jickling, M. & Webel, B. 2004, "The economic impact of cyber-attacks", Congressional Research Service, Library of Congress .

CERT 2002*, CSIRT Services*. Available: http://www.cert.org/csirts/services.html, Accessed 2010/05/13/.

Charmaz, K. 2003, "Grounded theory", *Strategies of qualitative inquiry*, vol. 2, pp. 249.

Charvat, J. 2010, "Radicalization on the Internet", *Defence Against Terrorism Review*, vol. 3, no. 2, pp. 75-86.

Clarke, R.A. & Knake, R.K. 2011, *Cyber war,* HarperCollins, New York.

Clauset, A. & Gleditsch, K.S. 2012, "The developmental dynamics of terrorist organizations", *Plos One*, vol. 7, no. 11, pp. e48633.

Colarik, A.M. 2006, *Cyber terrorism: political and economic implications,* Idea Group Inc (IGI), USA, pp. 7-10.

Coll, S. & Glasser, S.B. 2005, "Terrorists turn to the Web as base of operations", *The Washington Post*, vol. 7, pp. 77–87.

Collin, B.C. 1997, "The future of cyberterrorism: The physical and virtual worlds converge", *Crime and Justice International*, vol. 13, no. 2, pp. 14-18.

Compact Oxford English Dictionary 2008*, Knowledge*, Compact Oxford English Dictionary, [Online]. Available: http://www.askoxford.com/concise_oed/knowledge?view=uk, Accessed 2008/02/12.

Conway, M. 2006, "Terrorist use of the Internet and fighting back", *Information and Security*, vol. 19, pp. 9.

Conway, M. 2012, "From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a new form of violent radical Milieu", *CTX: Combating Terrorism Exchange*, vol. 2, no. 4, pp. 12-22.

Cronin, A.K. 2002, *The diplomacy of counterterrorism lessons learned, ignored and disputed*, International Research Group on Political Violence (IRGPV), [Online]. Available: http://www.usip.org/pubs/specialreports/sr80.pdf, Accessed 2012/01/10.

Curts, R.J. & Campbell, D.E. 2005, "Building an Ontology for Command & Control", *10th International Command and Control Research Technology Symposium* DTIC Document .

Cyber Security Strategy Committee 2008, *Cyber Security Strategy*, Ministry of Defence, [Online]. Available: http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf, Accessed 2013/12/10.

Cyberterrorism Defense Initiative 2010, *CDI: Cyberterrorism First Responder (CFR)*, Cyberterrorism Centre, [Online]. Available: http://cyberterrorismcenter.org/cfr.html, Accessed 2010/05/11.

Davis, J. 2007, *Hackers take down the most wired country in Europe*, Wired Magazine, [Online]. Available: http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all, Accessed 2012/09/15.

De Borchgrave, A., Sanderson, T. & Harned, J. 2007, *Force multiplier for intelligence,* Centre for Strategic and International Studies, Washington, D.C., pp. 17.

Denning, D. 2000, *Cyberterrorism*, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, Georgetown University, vol. 18.

Denning, D.E. 2009, "Terror's web: How the internet is transforming terrorism" in *Handbook on Internet crime*, eds. Y. Jewkes & M. Yar, Routlege, United Kingdom, pp. 194-205.

Denning, D.E. 2012, "Stuxnet: What has changed?", *Future Internet*, vol. 4, no. 3, pp. 672-687.

Desouza, K.C. & Hensgen, T. 2003, "Semiotic emergent framework to address the reality of cyberterrorism", *Technological Forecasting and Social Change,* vol. 70, no. 4, pp. 385-396.

Dizard, W.P. 8 March 2006, "Internet "cloaking" emerges as new Web security threat", Government Computer News, Available: www.gcn.com/online/vol11_no1/40075-41.html, Accessed 2012/03/12.

Dunn Cavelty, M. 2010, *The future and reality of cyberwar*, Parliamentary Brief, [Online]. Available: www.parliamentarybrief.com/2010/03/the-future-and-reality-of-cyberwar, Accessed 2013/08/14.

Elmusharaf, M.M. 2004*, Cyber Terrorism: The new kind of terrorism*, Computer Crime Research Center, [Online]. Available: http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism, Accessed 2008/10/06.

Elrom, S. 2 December 2007, "The dark web of cyber terror- the threat that got lost in traffic", Global Politician, Available: http://www.globalpolitician.com/default.asp?23820-cyberterror, Accessed 2011/04/16.

Embar-Seddon, A. 2002, "Cyberterrorism: Are we under siege?", *American Behavioral Scientist*, vol. 45, no. 6, pp. 1033.

Epstein, J.M. 2008, "Why model?", *Journal of Artificial Societies and Social Simulation*, vol. 11, no. 4, pp. 12.

Eriksson, H.E. & Penker, M. 2000, *Business modeling with UML,* John Wiley & Sons, New York, pp. 1.

Farwell, J.P. & Rohozinski, R. 2011, "Stuxnet and the future of cyber war", Survival, vol. 53, no. 1, pp. 23-40.

FBI 2002, *Code of Federal Regulations*, 28 CFR.Section 0.85 on Judicial Administration, FBI.

Federal Ministry of the Interior 2011, *Cyber Security Strategy for Germany*, Federal Ministry of the Interior, Berlin Germany.

Foltz, C.,Bryan. 2004, "Cyberterrorism, computer crime, and reality", *Information Management & Computer Security*, vol. 12, no. 2, pp. 154-166.

Fornell, C. & Bookstein, F.L. 1982, "Two structural equation models: LISREL and PLS applied to consumer exit-voice theory", *Journal of Marketing Research*, pp. 440-452.

Frantz, A. & Franco, M. 2005, "A semantic web application for the air tasking order", *10th International Command And Control Research And Technology Symposium*, McLean, Virginia, 13-16 June 2005.

Garthwaite, P.H. 1994, "An interpretation of partial least squares", *Journal of the American Statistical Association*, vol. 89, no. 425, pp. 122-127.

Gearson, J. 2002, "The nature of modern terrorism", *The Political Quarterly*, vol. 73, no. 1, pp. 7-24.

Ghosh, T.K., Prelas, M.A., Viswanath, D., S. & Loyalka, S.K. *2010, Science and technology of terrorism and counterterrorism, CRC Press.*

Giacomello, G. 2004, "Bangs for the buck: A cost-benefit analysis of cyberterrorism", *Studies in Conflict and Terrorism*, vol. 27, no. 5, pp. 387-408.

Glaser, B.G. & Strauss, A.L. 2009, *The discovery of grounded theory: Strategies for qualitative research,* Transaction Books, USA, pp. 95.

Goodman, S.E., Kirk, J.C. & Kirk, M.H. 2007, "Cyberspace as a medium for terrorists", *Technological Forecasting and Social Change*, vol. 74, no. 2, pp. 193-210.

Gordon, S. & Ford, R. 2002, "Cyberterrorism?", *Computers & Security*, vol. 21, no. 7, pp. 636-647.

Grobler, B. 2009, "What is cyber terrorism and what is at risk?" in *Cyber Terrorism 2009 Seminar*, Ekwinox.

Gruber, T.R. 1993, "A translation approach to portable ontology specifications", *Knowledge Acquisition*, vol. 5, no. 2, pp. 199-220.

Haenlein, M. & Kaplan, A.M. 2004, "A beginner's guide to partial least squares analysis", *Understanding statistics*, vol. 3, no. 4, pp. 283-297.

Hansen, J.V., Lowry, P.B., Meservy, R.D. & McDonald, D.M. 2007, "Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection", *Decision Support Systems*, vol. 43, no. 4, pp. 1362-1374.

Heickero, R. 2007, "Terrorism online and the change of modus operandi", *Swedish Defence Reseach Agency*, Stockholm, Sweden, pp. 1.

Henseler, J., Ringle, C. & Sinkovics, R. 2009, "The use of partial least squares path modeling in international marketing", *Advances in International Marketing (AIM)*, vol. 20, pp. 277-320.

Ho, S.M. 2008, "A framework of coordinated defense", *Proceedings of the Second International Conference on Computational Cultural Dynamics*, Maryland, USA, 15–16 September, 2008, pp. 39-44.

Holt, T.J. & Kilger, M. 2012, "Examining Willingness to Attack Critical Infrastructure Online and Offline", *Crime & Delinquency*, vol. 58, no. 5, pp. 798-822.

Horridge, M., Knublauch, H., Rector, A., Stevens, R. & Wroe, C. 2004*, A practical guide To building OWL ontologies using the Protégé-OWL plugin and CO-ODE Tools Edition 1.0*, The University of Manchester, [Online]. Available: http://130.88.198.11/tutorials/protegeowltutorial/resources/ProtegeOWLTutorialP3_v1_0.pdf, Accessed 2013/08/14.

Hulland, J. 1999, "Use of partial least squares (PLS) in strategic management research: a review of four recent studies", *Strategic Management Journal*, vol. 20, no. 2, pp. 195-204.

Hutchinson, W. & Warren, M. 2001, Information Warfare: Corporate attack and defence in a digital world, Butterworth-Heinemann.

Ilvonen, I. & Virtanen, P. 2013, "Preparing for cyber threats in companies with information security policies", *Proceedings of the 12th European Conference on Information Warfare and Security*, Jyväskylä, Finland, 11-12 July 2013, pp. 120.

Industrial Control Systems Cyber Emergency Response Team (IS-CERT) 2005*, Cyber threat source descriptions*, US Government, [Online]. Available: http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions, Accessed 2013/10/01.

Internet World Stats 2013*, Internet usage statistics - The Internet big picture: World internet users and population stats*. Available: http://www.internetworldstats.com/stats.htm, Accessed 2014/01/21.

*I*nternational Standards Organisation (ISO) 2012*, Information technology — Security techniques — Guidelines for cybersecurity,* ISO/IEC FDIS 27032:2012(E), ISO/IEC JTC 1/SC 27/WG4, Geneva.

Jackson, D. 2003, System and method for internal network data traffic control, US20040146006 A1, Google Patents, United States.

Jacobson, M. 2009, "Terrorist financing on the internet", *CTC Sentinel*, vol. 2, no. 6, pp. 17-20.

Janczewski, L. & Colarik, A.M. 2008, *Cyber warfare and cyber terrorism,* Idea Group Reference, New York, USA, pp. 475.

Jenkins, B.M. 2006, "The new age of terrorism" in *McGraw-Hill Homeland Security Handbook*, McGraw-Hill, New York, pp. 118–119.

Joint Chief of Staff 1996, *Joint Doctrine for Command and Control Warfare (C2W)*, Joint Publication 3-13-1, United States of America.

Jones, D., Bench-Capon, T. & Visser, P. 1998, "Methodologies for ontology development", *Proceedings of the 15th IFIP World Computer Congress on IT and Knowledge Systems* Citeseer , pp. 20.

Kamien, D.G. 2006, *The McGraw-Hill homeland security handbook,* McGraw-Hill, New York, pp. 821-836.

Kimmage, D. & Ridolfo, K. 2007, *Iraqi insurgent media. The war of images and ideas. How Sunni insurgents in Iraq and their supporters worldwide are using the media*, Radio Free Europe/Radio Liberty, Washington DC, USA.

Knublauch, H., Horridge, M., Musen, M., Rector, A., Stevens, R., Drummond, N., Lord, P., Noy, N.F., Seidenberg, J. & Wang, H. 2005, "The Protégé OWL Experience", *Proceedings of OWL Experiences and Directions Workshop*.

Kosterman, R. & Feshbach, S. 1989, "Toward a measure of patriotic and nationalistic attitudes", *Political Psychology*, pp. 257-274.

Kramarenko, D. 2004, *Terrorism and high technologies*. Available: http://www.crime-research.org/news/04.14.2004/211/, Accessed 2010/03/08.

Labi, N. 2006, "Jihad 2.0", *The Atlantic Monthly*, vol. 102 (Issue and page no not available).

Lachow, I. 2008, *Cyber security: A few observations*, National Defense University, Washington.

Lachow, I. & Richardson, C. 2007, "Terrorist use of the Internet: The real story", *Joint Force Quarterly*, vol. 45, pp. 100.

Lappin, Y. 2010, *Virtual caliphate: Exposing the Islamist State on the internet,* Potomac Books, Inc., Washington DC, pp. 2-9.

Laqueur, W. 1996, "Postmodern Terrorism", *Foreign Affairs*, vol. 75, pp. 24.

Lau, S. 2003, *An analysis of terrorist groups' potential use of electronic steganography* , SANS Institute, [Online]. Available: http://www.sans.org/reading-room/whitepapers/stenganography/analysis-terrorist-groups-potential-electronic-steganography-554;, Accessed 2011/11/25.

Lehto, M. 2013, "The ways, means and ends in cyber security strategies", *Proceedings of the 12th European Conference on Information Warfare and Security*, Jyväskylä, Finland, 11-12 July 2013, pp. 182.

Lemos, R. 2002, *What are the real risks of cyberterrorism*, ZDnet, [Online]. Available: http://zdnet.com/2100-1105-955293., Accessed 2011/05/26.

Lewis, J.A. 2002, "Assessing the risks of cyber terrorism, cyber war and other cyber threats", *Center for Strategic and International Studies*, pp. 1-12.

Lyons, J. 1977, *Semantics. vol. 2,* Cambridge University Press.

Matusitz, J. 2013, "The Networks That Fight Cyberterrorist Networks", *Journal of Human Behavior in the Social Environment*, vol. 23, no. 5, pp. 616-626.

Matusitz, J. & Breen, G. 2011, "A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism", *Journal of Human Behavior in the Social Environment*, vol. 21, no. 2, pp. 109-129.

Merriam-Webster 2013, *Driver*, Encyclopedia Britannica, [Online]. Available: http://www.merriam-webster.com/dictionary/driver, Accessed 2013/08/22.

Merriam Webster Dictionary 2013, *Simulation*. Available: http://www.merriam-webster.com/dictionary/simulation;, Accessed 2013/11/12.

Michael, G. 2003, *Confronting Right Wing Extremism and Terrorism in the USA,* Routledge, New York and London, pp. 88.

Mirkovic, J. & Reiher, P. 2004, "A taxonomy of DDoS attack and DDoS defense mechanisms", *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53.

Mortman, D. 2009*, Disaster recovery risk assessment for cyberterrorism attacks*. Available: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1507807,00.html;, Accessed 2009/11/06.

MyBroadband.co.za. 2010*, Cyber terrorism on the rise*. Available: http://mybroadband.co.za/news/Internet/11673.html, Accessed 2013/10/10.

Nagpal, R. 2005*, Defining Cyber Terrorism*, Webmaster Digest, no 369, [Online]. Available: http://www.webmasterdigest.com/news/369.html;, Accessed 2011/05/14/369.

Nakashima, E. 26 January 2008, "Bush order expands network monitoring", The Washington Post, Section Technology - Special Reports, Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter, Accessed 2010/05/13.

National Institute of Standards and Technology 2013, *Glossary of Information Security Terms*, NIST IR 7298 Revision 1, NIST, USA.

Nelson, B., Choi, R., Lacobucci, M., Mitchell, M. & Gagnon, F. 1999*, Cyberterror prospects and implications*, Centre for the Study of Terrorism and Irregular Warfare, [Online]. Available: http://www.nps.edu/Academics/Centers/CTIW/files/Cyberterror%20Prospects%20and%20Implications.pdf;, Accessed 2011/05/14.

Noguchi, Y. & Goo, S. 13 April 2006, "Terrorists' web chatter shows concern about Internet privacy", The Washington Post, Available: http://www.washingtonpost.com/wp-dyn/content/article/2006/04/12/AR2006041201968_pf.html, Accessed 2013/10/13.

Nordeste, B. & Carment, D. 2006, " Trends in terrorism series: A framework for understanding terrorist use of the internet ", *ITAC*, vol. 2006-2, pp. 1-21.

Noy, N.F. & McGuinness, D.L. 2001, *Ontology Development 101: A Guide to Creating Your First Ontology*, KSL-01-05, Stanford Knowledge Systems Laboratory Technical Report.

Olson, K.B. 1999, "Aum Shinrikyo: Once and future threat?", *Emerging Infectious Diseases*, vol. 5, no. 4, pp. 513.

Onions, P.E. 2006, "Grounded theory applications in reviewing knowledge management literature", *Proceedings of the Postgraduate Research Conference on Methodological Issues and Ethical Considerations* Citeseer , Leeds, 24 May 2006.

Oxford Dictionary 2014, Logic. Available: http://www.oxforddictionaries.com/definition/english/logic, Accessed 2014/02/28.

Oxford Dictionary 2013, Definition of dimension in English. Available: http://oxforddictionaries.com/definition/english/dimension, Accessed 2013/08/22.

Palmer, C.C. 2001, "Ethical hacking", *IBM Systems Journal*, vol. 40, no. 3, pp. 769-780.

Phillipines 2003, *Anti-Terrorism Act*, S540, Senate Bill 1353.

Piper, P. November/December 2008, "Nets of terror: Terrorist activity on the internet", *Searcher*, vol. 16, no. 10, Available: http://www.infotoday.com/searcher/nov08/Piper.shtml.

Pollitt, M.M. 1998, "Cyberterrorism - fact or fancy?", *Computer Fraud & Security,* vol. 1998, no. 2, pp. 8-10.

Post, J.M. 2005, "The new face of terrorism: Socio-cultural foundations of contemporary terrorism", *Behavioral Sciences & the Law*, vol. 23, no. 4, pp. 451-465.

Prieto-Díaz, R. 2003, "A faceted approach to building ontologies", *IEEE International Conference on Information Reuse and Integration (IRI)*, pp. 458-465.

Public Safety Canada 2012*, Cyber Security Strategy.*, Government of Canda, [Online]. Available: http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx;, Accessed 2013/11/02.

Puran, R.C. 2003, *Beyond Conventional Terrorism… The Cyber Assault*, GIAC Security Essentials Certification (GSEC) v1.4b, SANS.

Rosipal, R. & Krämer, N. 2006, "Overview and recent advances in partial least squares" in *Subspace, Latent Structure and Feature Selection*, Springer, pp. 34-51.

Rowley, J. 1998, "What is information?", *Information Services and Use*, no. 18, pp. 243-254.

Rrushi, J. 2006*, SCADA Intrusion Prevention System*, Telecom-paristech.fr, [Online]. Available: http://perso.telecom-paristech.fr/~legrand/CI2RCO-conf/Article/scada_rrushi.pdf, Accessed 2010/06/06.

RSA 2011, *Cyber Security Awareness Month Fails to Deter Phishers*, Report No. 1011, RSA, United States of America.

Ruby, C.L. 2002, "The definition of terrorism", *Analyses of Social Issues and Public Policy*, vol. 2, no. 1, pp. 9-14.

Sanchez, G. 2013a*, PLS Modelling*, Creative Commons, [Online]. Available: http://www.plsmodeling.com/pls/pls-introduction, Accessed 2014/01/08.

Sanchez, G. 2013b*, PLS Path Modelling with R*, Creative Commons, [Online]. Available: www.gastonsanchez.com/PLS_Path_Modeling_with_R.pdf, Accessed 2013/08/20.

Schmorrow, D. 2011, *Sociocultural Behavior Research and Engineering in the Department of Defense Context*, Office of the Secretary Of Defense (Research And Engineering), Washington DC, USA.

Schneier, B. 2003, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World,* Copernicus Books, New York.

Schudel, G., Wood, B. & Parks, R. 1999, "Modeling behavior of the cyber-terrorist", *National Security Forum on International Cooperation to Combat Cyber Crime and Terrorism* Hoover Institution , Stanford University, 6 December 1999.

Seib, P. 2011, "Public Diplomacy, New Media, and Counterterrorism", *CPD Perspectives on PD*, no. 2, pp. 1-37.

Sevcenko, M. 2003, "Online presentation of an upper ontology", *Proceedings of Znalosti 2003* , Ostrava, Czech Republic, 19-21 February 2003.

Shaw, E.D. 2006, "The role of behavioral research and profiling in malicious cyber insider investigations", *Digital investigation*, vol. 3, no. 1, pp. 20-31.

Sidanius, J. & Pratto, F. 2001, *Social dominance: An intergroup theory of social hierarchy and oppression,* Cambridge University Press, Cambridge, UK, pp. 61-67.

Singel, R. 2010*, Richard Clarke's Cyberwar: File Under Fiction*, Wired, [Online]. Available: http://www.wired.com/threatlevel/2010/04/, Accessed 2010/06/25.

Smarr, L. 1985, "An approach to complexity: Numerical computations", *Science Journal*, vol. 228, no. 4698, pp. 403-408.

Song, S., Ryu, K. & Kim, M. 2010, "Ontology-based decision support for military information systems", *IEEE Long Island Systems Applications and Technology Conference (LISAT)*, pp. 1-5.

Squitieri, T. 5 May 2002, "Cyberspace full of terror targets", USA Today, Available: http://www.usatoday.com/tech/news/2002/05/06/cyber-terror.htm., Accessed 2013/08/14.

Stohl, M. 2006, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?", *Crime, law and social change*, vol. 46, no. 4-5, pp. 223-238.

Strauss, A. & Corbin, J. 1994, *Grounded theory methodology,* Denzin N.K. & Lincoln Y.S, Sage, London, pp. 273-285.

Supercourse lectures 2008*, Cyber terrorism (When the hackers grow up)*, Bibalex.org, [Online]. Available: www.bibalex.org/supercourse, Accessed 2011/04/16.

Talihärm, A. 2010, "Cyberterrorism: in Theory or in Practice?", *Defence Against Terrorism Review*, vol. 3, no. 2, pp. 59-74.

Targ, H.R. 1988, "Societal structure and Revolutionary Terrorism: A preliminary investigation", *The Politics of Terrorism*, pp. 127-152.

Taylor, M. 1988, *The terrorist,* Brassey's Defence Publishers, London.

The Free Dictionary 2013*, Factor*, Farlex, [Online]. Available: http://www.thefreedictionary.com/factor, Accessed 2013/08/22.

The Government Gazette 2002, *Electronic and Communciation Act (ECT)*, 23708 vol 446, Republic of South Africa, Cape Town, South Africa, Available: http://www.info.gov.za/view/DownloadFileAction?id=68060, Accessed 2013/08/14.

Tibbetts, P.S. 2002, "Terrorist Use of the Internet and Related Information Technologies", *Army Command and General Staff Coll Fort Leavenworth KS School of Advanced Military Studies*, pp. 1-67.

Traynor, I. 2007, "Russia Accused of Unleashing Cyberwar to Disable Estonia", The Guardian, Section World News, Available: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, Accessed 2011/05/27.

Ulph, U. 2010*, Towards a curriculum for the teaching of jihadist ideology*, Jamestown Foundation, [Online]. Available: http://www.jamestown.org/uploads/media/Ulph_Towards_a_Curriculum_Part1.pdf, Accessed 2014/03/06.

United Kingdom Cabinet Office 2011, *The UK Cyber Security Strategy*, Gov.uk, London, United Kingdom, Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, Accessed 2013/08/12.

United Kingdom Government 2000, *Terrorism Act*, Part 1, (1)-(3), Legislation.gov.uk, United Kingdom, Available: http://www.legislation.gov.uk/ukpga/2000/11/contents, Accessed 2013/08/12.

United Nations Security Council (UNSC) 2004, *Resolution 1566*, UN.org, Available: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement.

US Army Training and Doctrine Command 2006, *Critical infrastructure threats and terrorism,* 1.02nd edn, US Army Training and Doctrine Command, Fort Leavenworth, Kansas.

US DoD 2008, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23*, NSPD-54/HSPD, United States of America.

US Government 1983, *US Code Title 22 Section 2656f*, United States of America.

Uschold, M. & King, M. 1995, "Towards a methodology for building ontologies", *Workshop on Basic Ontological Issues in Knowledge Sharing*.

Vamosi, R. 20 May 2008, "The Estonia Cyberwar: One Year Later", Cnet, Section Security, Available: http://news.cnet.com/8301-10789_3-9948720-57.html, Accessed 2011/05/27.

Van Heerden, R.P., Irwin, B. & Burke, I.D. 2012, "Classifying network attack scenarios using an Ontology", *Proceedings of the 7th International Conference on Information Warfare and Security*, ed. V. Lysenko, Academic Conferences , Seattle, USA, 22-23 March 2012.

Vatis, M.A. 2001, *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, DTIC Research Report ADA395300, Available: http://www.ists.dartmouth.edu/projects/archives/cyber_attacks.html, Accessed 2011/06/29.

Veerasamy, N. 2009a, "A high-level conceptual framework of cyberterrorism", *Journal of Information Warfare*, vol. 8, no. 1, pp. 42-54.

Veerasamy, N. 2009b, "Towards a conceptual framework for cyberterrorism", *Proceedings of the 4th International Conference on Information Warfare and Security*, ed. L. Armistead, Academic Conferences , Cape Town, South Africa, 26-27 March 2009, pp. 129-137.

Veerasamy, N. & Grobler, M. 2011, "Terrorist use of the Internet: Exploitation and support through ICT infrastructure", *Proceedings of the 6th International Conference on Information Warfare and Security*, ed. L. Armistead, Academic Conferences , Washington, USA, 17-18 March 2011, pp. 260-267.

Ventre, D. 2009, *Information warfare,* Wiley-IEEE Press, London UK, pp. 40.

Von Solms, B. 2008, "Critical Information Infrastructure Protection- Essential during war times, or peace times or both?", *IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace*, eds. J. Phahlamohlaka, N. Veerasamy, L. Leenen & M. Modise, Council for Scientific and Industrial Research , 24 July 2008, pp. 36.

Von Solms, R. 1996, "Information security management: the second generation", *Computers & Security*, vol. 15, no. 4, pp. 281-288.

Von Solms, R. & Van Niekerk, J. 2013, "From information security to cyber security", *Computers & Security*, vol. 38, pp. 97-102.

Webb, K. 2009, "Considerations for management from the onset of Information Terrorism", *Proceedings of the 4th International Conference on Information Warfare and Security*, ed. L. Armistead, Academic Publication Limited , Cape Town, South Africa, 26-27 March, pp. 138.

Weimann, G. 2004, *Cyberterrorism: How real is the threat?*, Report No 119, United States Institute of Peace, Washington, United States, Available: http://www.usip.org/pubs/specialreports/sr119.pdf, Accessed 2011/07/25.

Weimann, G. 2005a, "Cyberterrorism: The sum of all fears?", *Studies in Conflict & Terrorism*, vol. 28, no. 2, pp. 129-149.

Weimann, G. 2005b, "How modern terrorism uses the internet", *The Journal of International Security Affairs*, vol. Spring 2005, no. 8.

Weimann, G. 14 May 2014, "Social media key for terror groups-study", News24.com, Section Tech, Available: http://www.news24.com/Technology/News/Social-media-key-for-terror-groups-study-20140514, Accessed 2014/05/14.

West, D. & Latham, C. 2010, "The extremist edition of social networking: The inevitable marriage of cyber jihad and Web 2.0", *Proceedings of the 5th International Conference on Information Warfare and Security*, ed. L. Armistead, Academic Conferences , Ohio, USA, 8-9 April 2010.

Whelpton, J. 2009, "Psychology of Cyber Terrorism" in *Cyberterrorism 2009 Seminar*, Ekwinox.

Whitman, M.E. & Mattord, H.J. 2010, *Principles of information security,* Cengage Learning.

Williers, C.J., Voster, C.J., van 't Wout, A., Venter, J.P., Naude, S.J. & van Buuren, R. 2005/06, *IW Basic Course*, DEFT-IW-00200, Council for Scientific and Industrial Research, Pretoria, South Africa.

Williers, C.J. 2007, *Agent Based Modelling Report*, DPSS-SM-EDERI-IW-003, CSIR, Pretoria, South Africa.

Wilson, C. 2008, *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress*, Library of Congress Washington DC Congressional Research Service, Washington DC, Available: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA477642, Accessed 2012/05/23.

Wilson, G.I., Wilcox, G. & Richards, C. 2005, "4GW and OODA Loop implications of the Iraqi insurgency", *16th Annual AWC Strategy Conference*, 12-14 April 2005.

Wilson, G.I., Wilcox, G. & Richards, C. 2004*, Fourth Generation Warfare and the OODA Loop implications of the Iraqi insurgency*, Smartpei.typepad.com, [Online]. Available: http://smartpei.typepad.com/robert_patersons_weblog/files/4gw_ooda_iraq.ppt, Accessed 2010/05/07.

Winsberg, E. 2003, "Simulated experiments: Methodology for a virtual world", *Philosophy of Science*, vol. 70, no. 1, pp. 105-125.

Winsberg, E. 1999, "Sanctioning models: The epistemology of simulation", *Science in Context*, vol. 12, no. 2, pp. 275-292.

Wood, B.J. & Duggan, R.A. 2000, "Red Teaming of advanced information assurance concepts Defence Advanced Research Projects Agency (DARPA)", *Information Survivability Conference and Exposition*, vol. 2, pp. 112-118.

World Population Prospects 2008a*, Crude birth rate*, UN Data, [Online]. Available: http://data.un.org/Data.aspx?q=world+population&d=PopDiv&f=variableID%3A53%3BcrID%3A900, Accessed 2012/08/14.

World Population Prospects 2008b*, Crude death rate*, UN Data, [Online]. Available: http://data.un.org/Data.aspx?d=PopDiv&f=variableID%3A65;, Accessed 2012/08/14.

Yau, J. 2008*, Russia engaging in cyberwarfare, says Georgia*, SiliconRepublic.com Ireland's Technology News Service, [Online]. Available: http://www.siliconrepublic.com/news/article/11184/cio/georgia-russia-waging-cyber-war, Accessed 2011/09/13.