4th Workshop on ICT Uses in Warfare and the Safeguarding of Peace

2012

Proceedings of the 4th Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2012 (IWSP 2012)

Protea Hotel Balalaika, Sandton

16 August 2012

Edited by Dr Brett van Niekerk, Dr Louise Leenen, Trishana Ramluckan, and Prof. Manoj Maharaj

A conference managed by CSIR and UKZN, South Africa

Proceedings of the 4th Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2012 (IWSP 2012)

School of Management, IT, and Governance
University of KwaZulu-Natal

and

Defence, Peace, Safety and Security
Council for Scientific and Industrial Research

Protea Hotel Balalaika, Sandton

16 August 2012

Edited by:
Dr. Brett van Niekerk, Dr. Louise Leenen, Trishana Ramluckan, and Prof. Manoj Maharaj

Papers have undergone a double peer review process before final submission.

Many thanks to the reviewers and the organising committee who helped to ensure the quality of the papers.

Further copies of the proceedings can be obtained from DPSS, CSIR or the School of Management, IT, and Governance, UKZN.

ISBN: 978-1-86840-727-9

Proceedings of the 4th Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2012 (IWSP 2012).

Published by:

Defence, Peace, Safety and Security
Council for Scientific and Industrial Research
www.csir.co.za

School of Management, IT, and Governance
University of KwaZulu-Natal
www.ukzn.ac.za

Preface

The Workshop on ICT Uses in Warfare and the Safeguarding of Peace is a note-worthy initiative that follows on three previous workshops: London (2007), Pretoria (2008), and Bela-Bela (2010). After the success of the workshops held in South Africa, the organising committee will be joining up with the annual ISSA (Information Security for South Africa) conference to provide a unique opportunity to interact with key researchers in the field. ISSA enables key players to review sustainable practice that have been developed by South Africans in order to meet the challenges delivered by globalisation in terms of information security.

The workshop will be hosted by the CSIR Defence, Peace, Safety and Security's (DPSS) Command, Control, and Information Warfare (CCIW) competency area and the School of Management, IT and Governance at the University of Kwazulu-Natal (UKZN). The CSIR is one of the leading scientific and technology research, development and implementation organisations in Africa. Its DPSS unit provides technology, advice and solutions in defence and security. The UKZN School of Management, Information Technology & Governance offers a wide range of undergraduate and postgraduate programmes in the disciplines of Marketing; Management and Entrepreneurship; Human Resources and Labour Relations; Supply Chain Management; Information Systems and Management; Information Systems and Technology; and Public Administration. The School conducts a number of innovative research projects in the areas of ICT for Development, Security, ICT in Education, Medical Informatics, eGovernment and Green IT.

The Programme Committee includes various international members that serve on IFIP Committees, UKZN, the CSIR, the South African National Defence Force (SANDF), and other research institutes. The Program Committee thus spans academia, industry and the military. This will provide theoretical, operational and practical viewpoints at this gathering.

The field of ICT security and its uses in warfare and the safeguarding of peace are wide and include various technical, legal, managerial, social, operational and even ethical issues. Therefore, the aim of this workshop is to focus the efforts of academia, military, industry and government to promote creative thinking in this field and the promotion of viable solutions to unanswered questions.

We want to express our gratitude to IFIP (International Federation for Information Processing) for the continued support they have offered this workshop from its first event in 2008.The South African local workshop will in future be organised by the CSIR and other interested parties in conjunction with willing and related conferences. A first regional version of this workshop was held in 2011 in Botswana and an international version is to be held in conjunction with the annual IFIP TC9 HCC conference in Amsterdam in September 2012. The regional and international events will be organised in partnership with IFIP.

Contents

Key Note Address: An Information Warfare Perspective on Entropy Warfare

Lt Col Jacques Théron
South African National Defence Force (SANDF), Pretoria, South Africa
jacques01.theron@gmail.com

The views expressed here are the author's own and do not necessarily reflect those of the SANDF or the South African Department of Defence.

Abstract: The term Entropy has been borrowed from thermodynamics. Entropy measures the disorderliness with which energy is stored in a system. This paper reviews the possible use of Information Warfare (IW) within the information sphere (infosphere) to achieve Entropy Warfare. This is not to indicate on the "how" or to prove that IW is Entropy Warfare. It is rather to indicate that the application of IW can lead to Entropy within the Information Sphere, thus contributing towards Information Superiority and the winning of skirmishes, battles or campaigns (military operations). Furthermore the paper strives to open an area for research within the Infosphere to apply Entropy Warfare through IW. To give a different approach of Entropy-Based Warfare away from the utilisation of precision guided kinetic weapons to create chaos. The creation of chaos can be non-kinetic of nature and within the cognitive domain forcing chaos within the decision making and command and control system of the enemy, breaking their will to fight.

Keywords: C4I3RS, Information Sphere (Infosphere), Land- Air-, Maritime-, Space Domains, Electromagnetic Spectrum (EMS), Network Spectrum (NS) or Cyberspace, Cyber Warfare (CW), Human Domain(HD), Information Warfare, Entropy.

1. Introduction

The rapid development of technology has considerably increased the significance of information within the Operational Battle Space (OBS). From the advent of the Personal Computers (PC) and the birth of the public version of the Internet, communication and information capabilities have exploded [2]. The advances in computer technologies, especially the Internet, network enablement, have made the world a village. Everything and everyone is connected to some degree, either by telephone, smart phone (cell phones), Internet etc. This is also prevalent within the military OBS. In the military it is known as network-centric.

Anyone with access to the Internet can visit foreign countries, their historical places, their national parks and even their military without a visa, passport or physically being there. One can purchase anything from any store or company anywhere in the world without leaving your home or having that country's currency, all done via the Internet. The Internet (Cyberspace) has paved the road for positive and negative use i.e. commerce, crime, warfare and even terrorism.

In the global village everything and everyone is within walking distance – finger walking distance over a keyboard.

2. Entropy

Entropy measure the disorderliness with which energy is stored in a system: the greater the disorder, the greater the entropy. The term entropy has been borrowed from thermodynamics to denote the average information content of messages. [9]

Entropy can also be explained as follow: [9]

- *Increasing Entropy*
  As the sun sets what you see becomes more obscure until such a stage where you do not see any more.
- *Decreasing Entropy*
  As the sun rises random obscurity becomes clearer more discernible.

Entropy can be understood intuitively as the amount of "disorder" in a system. This is an area that can be exploited by IW within the Cyber domain by applying malicious software into this environment to disrupt and/or to corrupt the enemy's Information Based Processing - thus creating entropy within the decision making process – cognitive entropy.

The principle of entropy can be expanded to include more than just energy stored in a system as shown below:

Table 1: **The Information Movement Towards Entropy [9]**

	Information Measures	
Information	→	**Entropy**
Order		Disorder
Signal		Noise
Music		Cacophony
Cosmos		Chaos
Design		Randomness

A lot of energy and effort are needed to keep order. Clocks unwind, batteries become flat, and vehicles need constant maintenance and upkeep to ensure they remain operational. On all levels a lot of energy is needed to move away from entropy, to keep order. This is where the key lies for IW to exploit this natural tendency toward entropy especially within the Infosphere and specifically in the Cyberspace. As Sun Tzu has observed: "disorder arises from order, cowardice arises from courage, and weaknesses arise from strength." [13]

Entropy-Based Warfare has the aim to ensure that the enemy force becomes disordered, and that they become cowards and weak as a military force. This is done by well planned, focused and coordinated efforts to create friction within the enemy leadership, to disrupt the enemy's plans and to degrade their firepower lethality.

3. Data, Information, Intelligence, Knowledge and Wisdom

A simplified definition of information within a military context: "information is history (history as in the past as well as current and present) - all recorded bits and pieces of information (i.e. activities) sensed or observed within the physical and/or information space regarding the enemy, terrain, weather, own- and friendly forces as well as their populace. Therefore information refers to "captured and managed" history (past and present), whereas Intelligence refers to the future. The collection, collation, processing and interpretation of information (history) give the ability to predict the future, hence the term Intelligence within the military.

Information Management (IM) (management of information throughout its life cycle – sensing to shooter cycle on strategic-, operational-, tactical- and weapon system levels), is arguably the most important activity for a military force. IM ensures that the correct information, in the correct format is available in-time for decision making at the correct place/person [4].

Information processing, including data, is also known as the Information Based Processing (IBP) environment. The IBP environment has a combination of automated (computer based) data fusion, information fusion and cognition. A substantial portion of IBP is made up by the human cognitive ability to process information into intelligence and knowledge [10,14].

Information is the start and the enablement of any military planning process where all relevant information is collated, analysed, processed and interpreted to predict the future. This prediction allows the commander and his/her staff to plan campaigns, operations or battles.

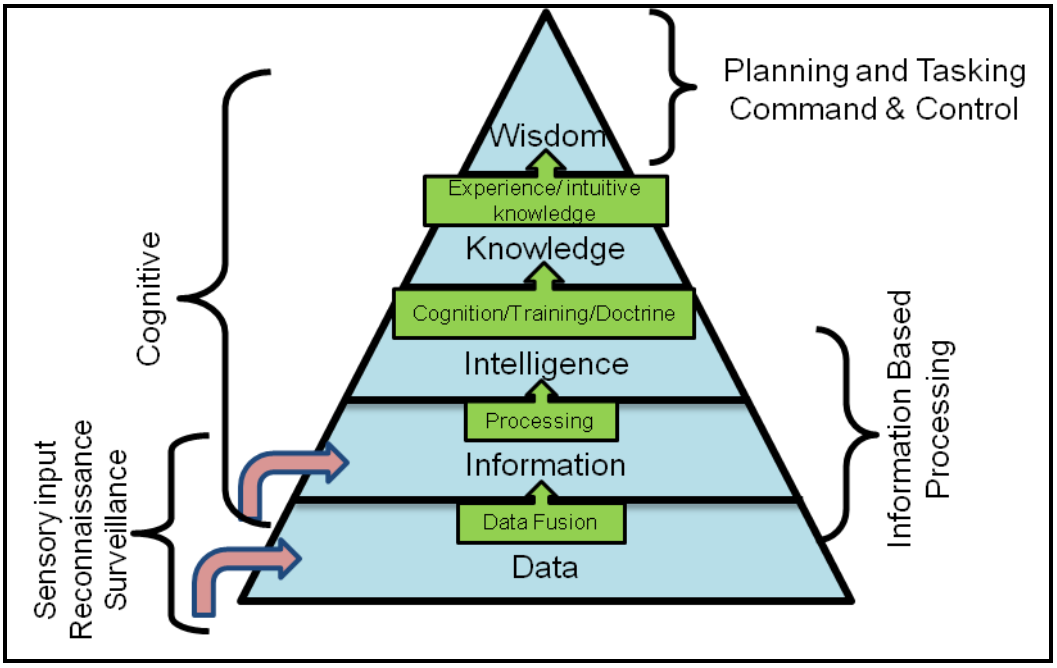

Figure 1: **Information Hierarchy: From Data to Wisdom [10]**

The processing of information is extremely important to ensure that the commander has the correct, relevant information on the right time in the right format for decision making.

3.1. Information Overloading

One need to note that there are three levels of information overloading that any military commander and his/her staff will face [1]:

3.1.1. Cognitive Overloading

The commander and staff cannot process the information fast enough to make a decision, and/or the information is of such a nature that no sense can be made from it. With 9/11 information was available but the nature and type of attack was not seen as executable thus possible "cognitive overloading".

3.1.2. Information Overloading

The commander and staff cannot find the correct and relevant information among the multitude of information.

3.1.3. Sensor Overloading

The commander and staff do not know which sensors to use for which information.

All the above overloading can be exploited by IW to create entropy (chaos) within the enemy's ability to collect and process information for decision making.

4. C4I3RS

The purpose here is not to delve deep into this, sometimes confusing and mostly misunderstood, C4I3RS - rather to set the scene for IW and Entropy. This is the centre of gravity of any military force / the hub of all power.

Table 2: **Explanation of C^4I^3RS**

C^4I^3RS	
First two C's of C^4	Command and Control (C^2). Command is the exercise of military authority by a designated commander for the planning, direction, coordination and control of a military force. Its ultimate aim is to generate and apply fighting power decisively. Control is a supporting activity through which the commander, assisted by his staff, organises, regulates and coordinates the activities of the force allocated. C^2 is mainly a cognitive activity which is dependent on knowledge and wisdom. This is the environment where planning and tasking is made. C^2 will be explained in Table 3 below.
Communications	The key to command is the ability to communicate. The structure must ensure that systems are available to allow for communications. The forces must be able to communicate with adjacent units, supporting joint forces or coalition forces. All methods of communication – radio, microwave, cell phone, satellite, telecom, video conferencing etc.
Computers	Computing stands at the centre of virtually all operating systems. It has extremely good possibilities to enhance the capabilities of resources available to the commander at all the levels of war, especially if the intelligence function is taken into account. Computers used for retrieval of data/information, for planning and/or for communications. This includes the computer networks (LAN and WAN) wire as well as wireless networks.
Information	As mentioned – also the collection thereof. This includes data fusion – data from various sensors, and the processing of all information (information based processing).
Intelligence	The processing of information to enable accurate intelligence for planning.
Infrastructure	The infrastructure needed for the communication networks that are the carriers of the information, which could be either physical or wireless that are within the Global, National and Defence networks or a combination thereof. Typical physical infrastructures include computers, a wire network connecting computers or a repeater mast. The wireless environment presently includes the satellite, radio and microwave networks, cell phone, global positioning systems, and other related technologies. This can also be referred to as the *Information Infrastructure Network* also known as net centric – interconnectivity with the purpose of enabling the flow of information from sensor through decision making up to the shooter (effecter).
Reconnaissance	Collection of information on military targets.
Surveillance	Collection of information wider that the military targets – terrain, weather, politics, population, infrastructure, etc.

C2 (the hub of all power) can be divided further and explained in Table 3. Note that the Communications, Computers, Information, Intelligence, Infrastructure, Reconnaissance and Surveillance enable C2, it is not C2.

Table 3: **Description of C^2**

C^2	
Situational Awareness	Being aware of one's surroundings and identifying potential threats and dangerous situations [12]. These are all inputs received from all sensors deployed (reconnaissance and surveillance) not only regarding knowledge of location and order of battle of the adversary also regarding own forces (including own deployment, higher, flanks and rear forces), friendly forces as well as own population (societies) and that of the adversary, including the state and location. Sensors could be deployed within the Electromagnetic Spectrum (EMS), Network Spectrum (Cyberspace) and/or Human Domain (physical observations).
Planning	The processing of the information received via (OBS) situational awareness. Planning operation – proactively on the enemy's/adversary's sensed and/or observed actions, movements, deployments, intentions, order of battle, etc.
Tasking	The physical tasking of subordinate commanders according to the plan.
Controlling	This includes the constant tasking, monitoring and feedback loop from higher command to lower command – ensuring the operation is on track and conducted according to plan. Consequently ensuring that the subordinate commanders are executing their tasks as commanded.

The most important part of C4I3RS is the Cognitive ability of the commander and staff. The C2 (Planning and Tasking part thereof) is mainly cognitive based. To do effective planning and tasking on accurate sensed/observed data/information one needs intelligence, knowledge and wisdom. Knowledge is obtained through intelligence linked to training and the application of doctrine (see figure 1 above). Applying this knowledge with experience and intuitive knowledge, wisdom is achieved, consequently the ability to command and control [10]. A simplified explanation is: "Knowledge is to know that tomatoes are fruit. Wisdom is to know not to use tomatoes in a fruit salad."

5. Information Sphere (Infosphere)

Since classical times, two domains of operation dominated military and civilian operations: Land and Sea. The advent of powered flight in 1904 initiated the opportunity for a third domain [3] namely the Air domain. As technology in propulsion improved and the introduction of crafts (rockets, space shuttles etc.) that are capable of space flight, and the consequent deployment of satellites in space a fourth domain was added, namely the Space domain.

This led to the notion that strategic power can only be projected over the known four dimensions such as sea, land, air and space. However, there is a fifth dimension or domain over which strategic power can be projected according to Lonsdale and it is described as the Infosphere [7].

The Infosphere is the environment that includes the land, sea, air and space domains. All of these domains operate within this sphere. It is also the domain where command and control takes place [7]. The Infosphere, according to Lonsdale, consists of the Electromagnetic Spectrum (EMS), Network Spectrum (NS also known as the Cyberspace) and the Human Domain (HD cognitive domain) see Figure 2 below [7].

5.1. Electromagnetic Spectrum (EMS)

The EMS is made up of the continuum of radiant energies that span from gamma and x-rays, through ultraviolet, the optical or visible wave band, infrared waves, microwaves, radio waves and up to extremely low frequency radio waves [7]. This is the environment in which Electronic Warfare (EW) is conducted.

5.2. Network Spectrum (NS)

The NS is made up of various technologies that enable the transportation (movement) of data packages in the form of bits and bytes (ones and zeros) resulting in the creation of information systems and networks that enable electronic interaction to take place. The bits and bytes (ones and

zeros) have physical manifestation in the state of electrons in a semiconductor gate or the waveforms of light passing through fibre-optic cable thus the medium in which this occurs are communication cables (copper or optic fibre) [7]. This spectrum is also known as the Cyberspace and where Cyber Warfare (CW) is conducted.

5.3. Human Domain (HD)

This domain relates to knowledge and wisdom acquired through thoughts, experience and senses, resulting in a perception, sensation or intuition. It is also the place where understanding, beliefs, norms and values reside, and where decisions are made. This is the domain of intangibles; leadership, morale, unit cohesion, level of training and experience. The significance of the human domain lies in its ability to influence the perceptions, cognitions, attitudes and behaviour of specific targets (other humans) [7]. "Cognitive Domain is the domain of the mind of the warfighter and the warfighter's supporting populace" [2]. This is the domain in which Psychological Operations (PO) are conducted.

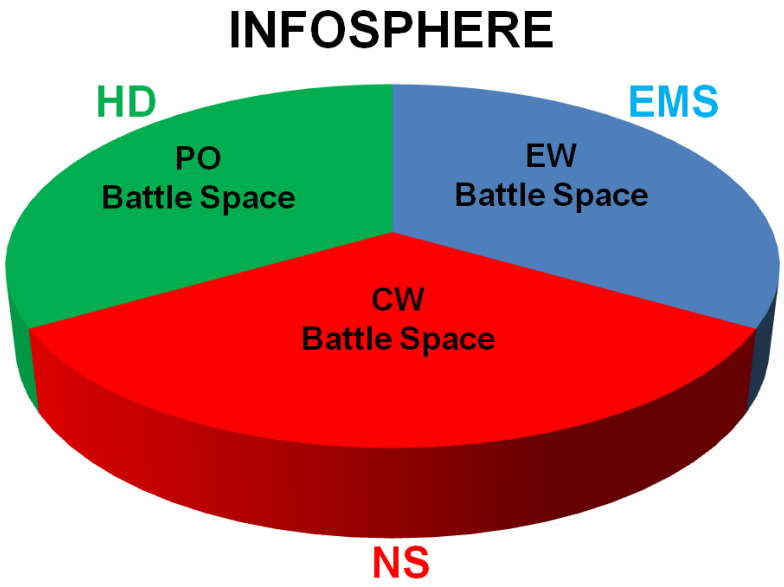

Figure 2: **The Domains (Battle Spaces) of the Infosphere**

6. Cyberspace

Recent discussions regarding the emerging field of CW have focused on the term "cyberspace", and have included cyberspace as being considered its own war fighting domain, much like air, land, sea and space. [2]

According to Lonsdale [7] the Infosphere consist out of three domains/areas the EMS, NS and the HD, see Figure 2 above.

With the inception of computers and the linking of computers in the past mainly via direct interconnecting by cables (LAN) and the interconnection via land based telecom landlines (WAN) this was an easy definable "space". This interconnection of computers created the term "cyberspace", a term attempting to describe this "new manmade" space, where information is stored, shared and distributed. Initially it was an area (space) that mainly existed within computers and computers linked to each other and/or to servers by copper wire.

To pinpoint cyberspace is not that easy as in the past. Cyberspace is now within the EMS and the physical communication network landlines. Cyberspace is still, according to the author, the "space", the "environment" which enables the interconnection of computers also including the computer, routers, hubs, servers, gateways, couplers, bowties, smart phones, software defined radios, satellite

phones etc. All this is used and controlled by the HD. Humans need to be connected and to share information to enable them to plan on how to conduct business, economics, politics and warfare.

Table 4: **Operational Capabilities and Effects within the Infosphere Domain/Areas**

Domain	War Fighting Capability
EMS	Electronic Warfare (EW): This include, but is not limited to, jamming of communications, interception of communications, direction finding and Electronic Pulse (EMP) weapons with the aim to disrupt, exploit, deny or corrupt the enemy's use of the EMS.
NS	Cyber Warfare (CW): The injection of malicious software into a computer network (whether physical or wireless) to intercept or map the network, with the aim to disrupt, exploit, deny or corrupt the enemy's use of the cyberspace (its computers and computer networks).
HD	Psychological Operations (PO): The influencing of the hearts and minds of the enemy's commanders, troops and its population with the aim to break its will to fight/cohesion.

The EMS is now not only the environment for Radio communication (SLF, LF; HF; VHF; UHF), or for location of target by radars, or for range finding by laser beams but also includes the cyberspace. To affect the cyberspace with IW to create entropy warfare one needs to understand the EMS cyberspace make up as well. The implication hereof is that traditional EW Jamming will have a CW effect as well. Information connectivity seems to be Net Centric based with Net Centrism focusing on IP. With the development of software defined radios it seems that the Cyberspace has absorbed the EMS.

Modern militaries understand the impact of information importance, the synchronisation of databases that share that information across networks which will result in a knowledge advantage over its enemy. If an enemy could degrade this network timekeeping the force could be thrown off with a related impact on performance [6] thus creating entropy. This degrading of the network timekeeping can be done by IW by applying CW.

7. Information Warfare (IW)

The role that IW plays in the Infosphere is to affect or protect the Command and Control capability, as this is the centre from where planned strategies are executed and controlled.

IW weapons in the form of malicious software, electromagnetic pulse devices and human influencing methods can be directed to target the information of the land, sea, air and space domains within the EMS, NS and HD.

IW can influence the opponent's information integrity and the flow of information by projection of its offensive capability (EW, CW and PO) to create entropy within the enemy's Infosphere. Information is the fundamental weapon and also the target of IW within the Infosphere.

8. Entropy-Based Warfare

A physical metric known as entropy can be used to describe disorder imposed on a military system at a given moment. Broadly defined, this metric is the steady degradation, of a military system. It is thus the mechanism that measures enemy disorganisation and ineffectiveness. Entropy-Based Warfare is the macro expression for the combined effect of friction, disruption, and lethality [6].

9. Creating Entropy by IW

The aim here is not to determine the "HOW" IW will achieve entropy by applying EW, CW and PO. As mentioned it is to open the "thought" to apply IW artfully to achieve entropy within the Infosphere creating cognitive dissidence within the enemy's C2.

As an example: by employing EW jamming on the Global Positioning System (GPS) will create chaos within the enemy's ability to deliver precision guide munitions on a GPS coordinate – thus influencing their lethality. How many current soldiers have the skill to call in precision artillery bombardment on a target only using a compass and a map? The same holds for flight planning of strike or bomber aircraft to deliver their weapons on a specific pinpointed target by only using compass and maps?

Taking the example of above, the jamming of GPS within an area, another method could be used for example with CW employing spoofing of false GPS information within the Infosphere thus enhancing entropy further. The GPS device still receives GPS "information" but it is false. How does this influence the C2 psychologically? Planning is done according to technology driven instruments however the delivery of the precision guided munitions are off target. The commander does not trust his/her planning staff; the planning staff start to second guess each other. Furthermore they start to lose trust in their equipment and the ability of the "shooter" to deliver the weapons on target. The "shooter" does not trust the planning staff or the commander. Thus Maximum Entropy has been achieved within the enemy's C2 system by creating friction and disruption among its planning and command structures and diminishing the lethality of it physical firepower.

10. Conclusions

In this paper a brief overview were given regarding the dynamics of the modern information age (including the technology age) and highlighting the importance of information-for-warfare. By applying the principles of IW to target the enemy's Information-in-Warfare with EW, CW and PO entropy can be achieved within the enemy's C2. It is therefore possible, by applying the factors of Entropy-Based Warfare within the Infosphere by IW, to render the use of the land, air and maritime forces useless.

Without situational awareness, information, intelligence and knowledge no planning can be done and therefore no warfare can be conducted. Thus the war has been won without physical fighting within the land, air, sea and space domain by merely creating entropy with little physical effort. This said, little physical effort still implies a lot of precision planning from the IW environment.

One can argue that all forms of warfare are entropy warfare as any military action creates a degree of chaos (entropy). Warfare on any level, with or without kinetic energy, is to create chaos forcing your enemy to stop fighting. In itself warfare is to exploit the natural tendency towards entropy.

It can thus be concluded that the application of IW within the Infosphere will achieve Entropy Warfare.

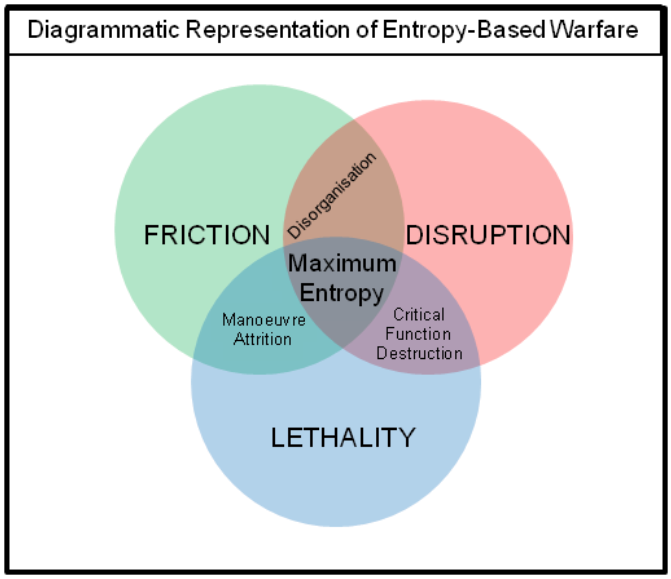

Figure 3: **Diagrammatic Representation of Entropy-Based Warfare [6]**

The three rings of the accompanying Venn diagram (Figure 3) represent the key factors that contribute to unit (military force) entropy. Friction comprises of those activities the unit performs that

increase its entropy level. Disruption includes those activities an enemy conducts to expand the unit entropy level. Lethality is the firepower a unit has to directly reduce an enemy through physical contact [6].

The Entropy-Based Warfare concept derives from the fact that a military force must maintain certain cohesive properties based on orderly construction and operation. As a unit (military force) loses cohesion, its entropy level increases until, at maximum entropy, it becomes a mob of individuals incapable of coordinating combat potential. The object of war has always been to bend an enemy to one's will, and a means to that end is to defeat an enemy's ability to resist [6] by breaking its cohesion and moral. A unit with no entropy can realise its full physical potential [6].

The components of fighting Power as defined by the SANDF are, Conceptual (the thought processes needed to develop the ability to fight), Moral (the ability of people to fight together irrespective of gender and/or individual traditions, needs and ethnicity) and Physical (the means to fight) (see Figure 4). These are the areas which need to be maintained and protected to ensure a cohesive fighting force.

These are also the areas of an enemy that could be targeted by applying the Entropy-Based Warfare factors. IW could play a major role in "attacking" any of these areas to create entropy within the enemy unit.

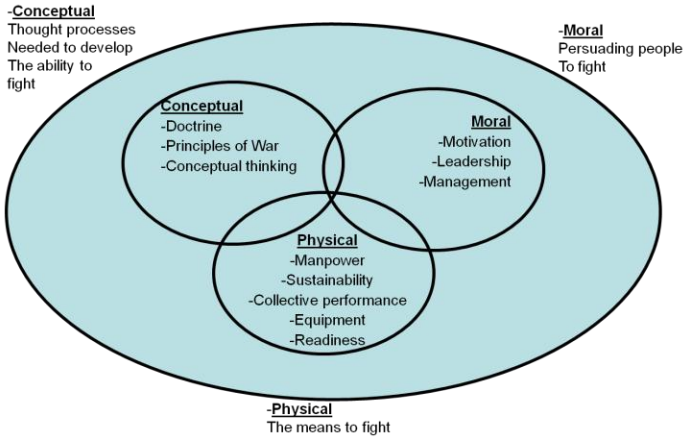

Figure 4: SANDF Components of Fighting Power

"Therefore those who win every battle are not really skilful – those who render other armies helpless without fighting are the best of all." [13]

References

[1] D. S. Alberts, J.S. Gartska, F.P. Stein. Network Centric Warfare, Developing and Leveraging Information Superiority – *DoD C4ISR Cooperative Research Program*, 2nd Edition (Revised), 2000.

[2] D.A. Patrick, D.P Gilbert, The information Sphere Domain Increasing understanding and Cooperation. *Cryptology and Information Security Series*. Vol. 3, 2009.

[3] H.B. De Czege. Systemic Operational Design: Learning and Adapting in Complex Missions. Paper published in *the Military Review January – February 2009*, pp. 2-12, 2009.

[4] J. De Feiter. IM: From Policy to Practice. Paper: Initiatives (no 7) a Publication of the C2 Centre of Excellence April 2010, 2010.

[5] D.E. Denning. Information Warfare and Security. ACM Press Books: New York, 1999.

[6] Herman, Mark. Entropy-Based Warfare: Modelling the Revolution in Military Affairs. Paper published in the JFQ Autumn/Winter, pp. 85-90, 1998-99.

[7] D.J. Lonsdale. The Nature of War in the Information Age, Clausewitzian Future. Frank Cass: London – New York, 2004.

[8] Microsoft ® Encarta® 2007. © 1993-2006 Microsoft Corporation.

[9] C. Misslar. Seminar – The Bible in 24 Hours, 2008.

[10] Numerous interactions and work sessions with members of the CSIR (DPSS) regarding the subject of Information Warfare.

[11] W.E. Richter, Walter. The Future of Information Operations. Paper published in the *Military Review January – February 2009*, pp. 103-113, 2009.

[12]S. Stewart. A Practical Guide to Situational Awareness. Paper published by Stratfor – Security Weekly – March 15, 2012.

[13] Sun Tzu (translated by Thomas Cleary 2005). The Art of War. Shambhala Boston & London, 2005.

[14] J.T. Théron. Operational Battle Space: An Information Warfare Perspective. Workshop on ICT Uses in Warfare and the Safeguarding of Peace, Pretoria South Africa, 2008

[15] P. Yancey. Rumours of Another World, What on Earth are we Missing?. Struik Christian Books, 2004.

The Future of Command and Control: Determining Force Readiness at the Push of a Button

Marthie Grobler, Jaco Robertson
Council for Scientific and Industrial Research, Pretoria, South Africa
mgrobler1@csir.co.za
jrobertson@csir.co.za

Abstract: The ability to determine force readiness is an important requirement for commanding the military. Currently, force readiness within the military is not measureable, but is estimated based on manual reporting and subjective human perceptions. Due to the potential level of miscalculation, commanding officers often need to make decisions on the fly, with no clear methodology in determining the correct level of force readiness. Hypothetically, these human estimations can result in either under allocation of military resources if the force readiness estimation is deemed high, or over allocation of military resources if the force readiness estimation is deemed low. This paper illustrates how a common data model can contribute to the automation of force readiness determination. This is enabled by Information Communication Technology automation within the command and control domain. The proposed Information Communication Technology utilisation will provide the foundation for future command and control systems based on automated formulas and algorithms, to remove subjectivity and the potential for human error from determining the force readiness of the military.

Keywords: Force readiness, interoperability, common data model, command and control.

1. Introduction

Command and control (C2) can be defined as the exercise of authority and general direction by a commanding officer over subordinate forces. This authority is exercised towards the accomplishment of a common goal, whether defensive or offensive. C2 consists of situation assessment, planning, tasking and control [3]. Part of the situation assessment of the military is to know the readiness of the force at their disposal, for any given scenario. This readiness refers to availability, capability and dependability. For the purposes of this research, force readiness can be defined as the upholding of military forces in a state of preparation for immediate deployment (availability), without additional training (capability), reinforcement or provisioning (dependability) required [15]. Regardless of the motivation behind a military goal, those in governing roles should know the readiness of the forces under their command: throughout the military command structure, from the Chief of the Military down to the stick leader.

This paper introduces the concept of a common data model for greater interoperability as a basis to use Information Communication Technology (ICT) automation to determine force readiness. The premise of the paper is that an implemented common data model will provide an adequate platform for future use of automated formulas and algorithms to provide a computer calculated readiness figure at the push of a button. This automation should largely lessen the scope for human error in readiness estimation.

The paper will introduce the problem background and explain it based on a futuristic scenario. Thereafter, the concepts of force readiness and interoperability in C2 will be discussed. The common data model will be introduced, and guidance provided on enabling the future of C2 with current technology and models. The paper is investigative in nature, and proposes a proof of concept for an interoperability solution. Due to the nature and sensitivity of the research field, little concrete research results and extensive examples are available in literature. As a result, a futuristic scenario forms the foundation of this exploratory study.

2. Background and scenario

Imagine the Chief of the Military arriving at the office, with his morning cup of coffee in hand, sitting behind the computer. With the press of a button, the computer tells the Chief that his military is currently standing at 96% force readiness. This calculation is done automatically, using all available sources: determining available personnel by checking duty rosters, leave schedules and training

records; vehicle readiness by checking maintenance records; and available munitions (weapons and ammunition) by checking the logistics system. The Chief can even ask the computer to calculate force readiness based on specific scenarios. For instance, determining how ready the military would be in case of a nuclear emergency, border attack or a sudden influx of refugees. The Chief can now sit back and enjoy his coffee, knowing that the situation assessment of his military indicates a readiness to serve the country in terms of National Security.

Although this futuristic scenario is not the current reality in calculating force readiness, it is possible with the technology available today. One of the main obstacles in achieving this automatic force readiness calculation is system interoperability (other obstacles may exist, but falls beyond the scope of this paper). Currently, systems are running in isolation, not exchanging information. For example, three different administration systems may exist, one each for duty rosters, leave schedules and training records. The only difference between reality and the futuristic example sketched earlier is that these three systems each give a single view of current reality: i.e. the duty roster for August 2012, the leave schedules for August 2012 and all past training for a specific soldier. However, the systems in isolation do not automatically calculate the impact that each system has on another. To illustrate, John Smith is one of only 10 commanders that have had advanced nuclear training; he is scheduled for leave during August 2012. Should a nuclear emergency break out during his leave period, the military's force command readiness would potentially be reduced by 10%. Therefore, John Smith's leave has a direct impact on availability and will influence force readiness in terms of the operational concept to be implemented.

These risks do not only hold for the Chief of the Military but flows down through all command structures. The reality is that commanders have to rely on *sitreps* (situational reports). These reports are compiled by the commander's line staff, based on their interpretation of available information. Not only does the possibility exist that this information may be incorrect or subjective, but the human interpretation introduces lag time between information retrieved by staff and sitreps produced to commanders. As a result, often no direct, unequivocal answer can be given to a specific set of possibilities. In addition, commanders may be put in the unenviable position of potentially making incorrect decisions that can have an impact on warfare and the safeguarding of peace within the country.

By introducing interoperability of information systems within the C2 domain, the level of situational awareness for the military will be unprecedented [6]. Commanders will have an accurate view of their resources and readiness in the case of a National Security event. The next section explains the necessity of force readiness.

3. Force readiness

Force readiness is not a single static metric, but is defined differently for different scenarios related to availability, capability and dependability. For the Chief of the Military, force readiness might be required to determine the overall readiness of the entire force - how many staff is on duty, levels of munitions stockpiles, operable vehicles, etc. For the commander of the special task force an important readiness metric might be how quickly his force can be deployed in the event of a threat to National Security. For the regiment leader, force readiness might be to determine which supporting arms and services are allocated to the battalion below the regiment. Since these services can be either of an administrative or tactical nature, force readiness can be impacted drastically. The validity and probability of the different scenarios is not the subject of this paper but deserves research in its own right.

Force readiness is an important metric within the military, used to determine aspects such as force deployment, budget allocation and capability development. The next sub sections introduce the importance of force readiness as driver in specific instances.

3.1 Force readiness as driver in force deployment

Force readiness can be broken down to unit resource assessment: each measured unit will report to an overall resource assessment. Force readiness therefore reflects the status of the selected resources measured against the resources required to undertake the missions for which the unit is organised or designed. For example, if twelve Petty Officers, six Browning machine guns and six dual

purpose guns are required to patrol a specific portion of the South Atlantic Ocean bordering Saldanha, but only nine Petty Officers, six Browning machine guns and two dual purpose guns are available, the naval force is not ready for the specific mission. Force deployment and resultant readiness is thus dependent on the condition of available equipment and personnel.

Another factor that can potentially have a debilitating impact on force readiness as driver in force deployment is the mental and physical health consequences of service in acts of war. It has been shown that rates of post-traumatic stress disorder vary between 4% and 31% in soldiers returning from war [7]. In addition, multiple deployments can also potentially have a debilitating effect on soldiers [7]. These figures can have a drastic impact on the readiness level of a force, if acts of war continue for prolonged periods of time. When put in perspective, this means that although the military's administration system may indicate that there are sufficient soldiers to call upon for active duty, these systems do not take into consideration that potentially only between 69% and 96% of the registered staff may be healthy and well enough for duty. In addition, these systems also do not take operational experience of soldiers into consideration. This example clearly illustrates the relation between availability, capability and dependability.

The latest available statistics from 2005 show that a total of 43.2% of active duty military personnel reported past-month binge drinking [11]. The study further showed that deployed soldiers were two and a half times more likely in need of emotional counselling; four times more likely to report needing help with sleeping problems; six times as likely to have received substance abuse treatment, and three and a half times as likely to have been prescribed an antidepressant. In addition, deployed soldiers reported more physical pain, requiring more medical care visits [7]. Although dated, the statistics show the importance and influence of multiple factors in determining force readiness.

Due to the sensitivity of the information, detailed personal information is generally not reflected in the military's personnel administration system. However, the implications of the mental and physical health statistics in terms of military readiness are considerable: a high number of medical visits, sick leave, early retirement, and loss of productivity have an impact on force deployment and the military's budget [5], as discussed in Section 3.2. These possibilities and the impact thereof on military readiness are difficult to calculate manually. However, with interconnected (interoperable) ICT systems, the military could utilise automated formulas and algorithms based on statistics to determine force readiness, at a push of a button. Although appropriate training and operational experience are a bigger driving force than the mental and physical health of soldiers in terms of calculating force readiness, an interoperability solution will allow the inclusion of non-tangible drivers into the decision making process. It is hypothesised that this will contribute to the calculation of a more realistic real time level of force readiness.

3.2 Force readiness as driver for budget allocation

Current calculation of force readiness is very subjective – commanders required to do the readiness estimation do so based on sitreps from their line staff. These reports can by interpreted inaccurately, either due to a lack of training or experience, or on purpose to mask a unit's specific inability or shortcomings. In addition, force readiness calculation requires a great deal of data, whilst the collection and processing of the data can take a great deal of time. This introduces the potential for lag between data collection, situation reports and decision making. Manual force readiness estimation based on a specific set of information does not always provide the most appropriate answer.

For example, according to the logistics' information system, the mechanised battalion may seem to be at full strength, with enough tanks, armoured vehicles, troop carriers, etc. for any incident, emergency or contingency. However, the information system do not necessarily take into consideration that many of these vehicles can be in a state of disoperation, either due to a lack of parts or a lack of skilled personnel able to perform maintenance duties. Therefore, in this scenario, the military budget will be better utilised on improving the delivery line for parts with the identified infrastructure supplier, or on the training of specialised vehicle maintenance mechanics. In this scenario, it would not be improving the long term force readiness if the budget is applied to buy more armoured vehicles, or by arranging more firing exercises. In the short term, the armoured vehicles will definitely make an impact, but as soon as it is scheduled for its first maintenance service, the vehicle will require

specialised mechanics to perform the necessary service. Force readiness is therefore an essential part of preparing the full military force in terms of budget allocation.

3.3 Force readiness as driver in capability development

Force readiness could be the single most important metric for the military during peace time. During non-active war time, the military's focus is generally on training and capability management; this is a time during which the nation can focus on rebuilding depleted resources, and recruiting and training more soldiers and staff as reserves for future war activities. However, it is imperative that the correct type of skills and capabilities are built.

To illustrate, the South African Border War lasted for 23 years (1966 to 1989), making it one of Africa's longest conflicts [2]. If an active recruitment campaign was launched before the war commenced, it is possible that most of the young soldiers started their military career during the war, and advanced through the ranks for the remainder of the war. Accordingly, it is possible that a large number of military personnel might retire after the war has ended. As a result, a large gap in military capability may have surfaced if the large group of military personnel retired at about the same time. Another example, after World War II, the main drivers behind warfare was nuclear weaponry. Although still a valuable tool, modern electronics and the advent of network centric warfare have now moved the focus of warfare into the digital age [14]. Accordingly, it could be postulated that staff with an Information Technology capability is more in demand than nuclear physicists. Knowing the discrepancy between required capability and actual capability is vital in capability development.

Both these examples have a definite impact on the variety of skills and capabilities required within the military. Therefore, it is imperative that the military accurately identifies what skills are lacking and what capabilities are required. It will not benefit either the military or the country if the recruitment focus is on foot soldiers, when a new type of advanced weaponry is available, but no soldiers are trained in using it. The answer lies in calculating real time force readiness as driver in capability development.

4. Interoperability in C2

Traditional approaches to C2 are not up to the challenge of modern warfare and are deemed to lack the agility required in the 21st century [1]. However, it is reasoned that ICT can enable the military to do things never done before, towards the betterment of C2. For example, real time blue force tracking, troop movement forecasts, as well as warfare at a distance using remote controlled unmanned aerial vehicles. In addition, modern electronics has greatly advanced precision in warfare. By using laser guided and GPS-guided bombs and missiles, it is possible to use one or two fighter planes to perform a task that once required the combined effort of twenty to thirty planes armed with dumb bombs to do [14].

Interoperability as such can be defined as the property that allows systems to work together independent of who created them, or how or for what purpose they were implemented. *"Data that is interoperable can be reliably read, written, and interpreted by a broad range of tools and databases, independent of who produces and who consumes the data"* [12]. Within the current military environment, the information advantage often decides the outcome of military missions. Accordingly, the interoperability of C2 systems can have a direct impact on the success of a mission. Unfortunately, it seems that many nations and even national units have each developed and maintained their own C2 systems based on information requirements relevant to that specific unit. As a result, there are numerous systems with different, incompatible interfaces [3]. Systems should be interoperable in order to provide constant feedback.

4.1 Interoperability vs. integration

The main premise of this paper is to institute interoperability of military systems, and not the integration of military systems. Where interoperability can be defined as the ability to exchange and use information in a large network [16], integration refers to combining existing parts to create a single new entity. The military already have a number of existing systems that were each designed to perform its own function. These systems are physically separated as a result of system design (refer to Figure 1).

In the military environment, interoperability is a much needed capability to facilitate automated, timely communications between different parts of the military. By introducing interoperability between these systems, additional functionality will be gained, without redeveloping existing systems (refer to Figure 2). This will allow other systems to leverage the work already done. In contrast, integration will require that each system will have to develop an interface with every other system, leading to a proliferation of difficult to manage interfaces.

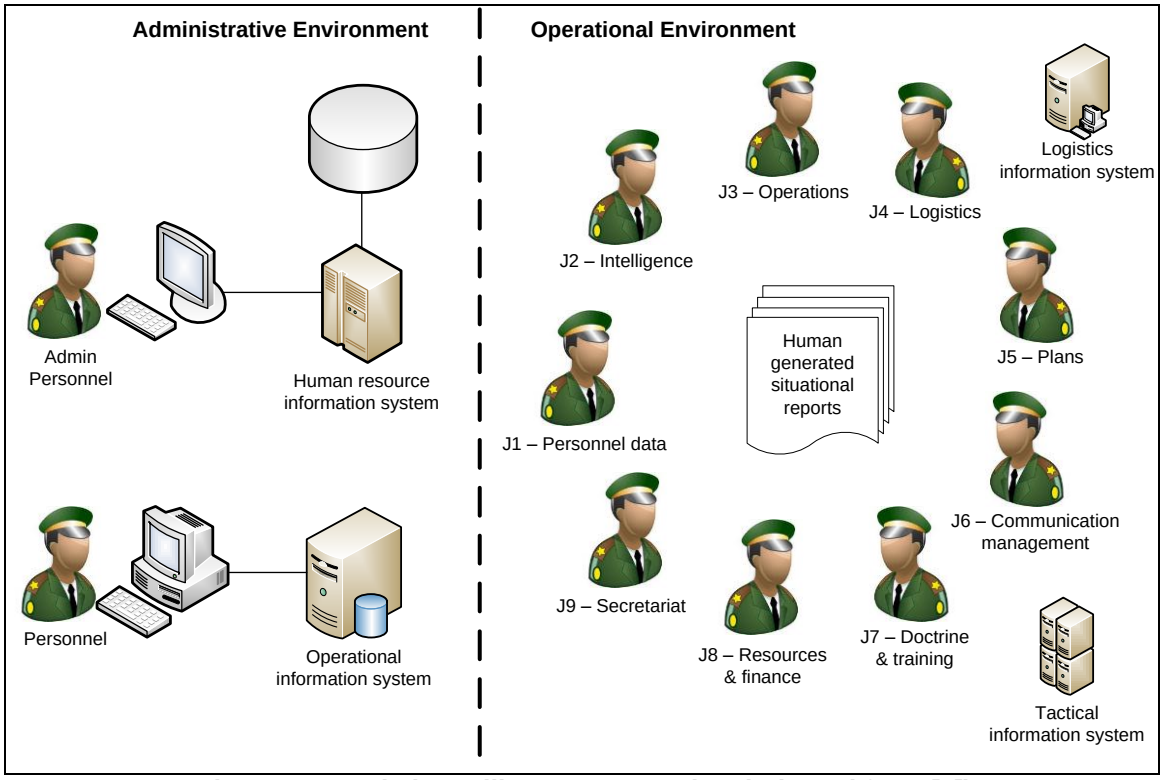

Figure 1: Existing military systems view (Adapted from [9])

Interoperability can further be sub divided into syntactic and semantic interoperability. If two or more systems are capable of communicating and exchanging data through specified data formats and communication protocols, the systems are exhibiting *syntactic interoperability*. XML and SQL standards, as well as ASCII formats are among the tools of syntactic interoperability. Syntactical interoperability is a necessary condition for further interoperability. Beyond the ability of two or more computer systems to exchange information, *semantic interoperability* is the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results as defined by the end users of both systems. To achieve semantic interoperability, both sides must refer to a common data model. The content of the information exchange requests are unambiguously defined: what is sent is the same as what is understood [8]. In working towards determining force readiness at the push of a button, it is recommended that the military have semantic interoperability. By introducing a common data model, already available information, computing power and skills are used to facilitate required information exchanges.

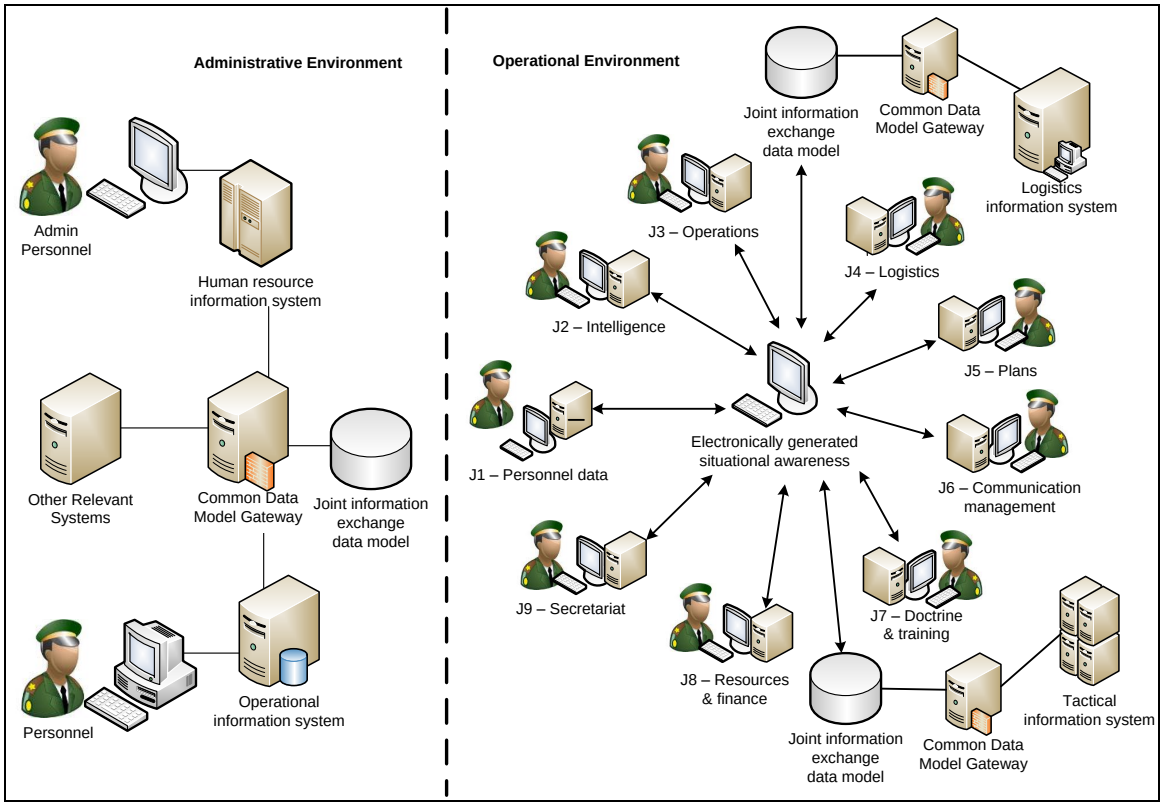

Figure 2: Proposed military systems view (Adapted from [9])

4.2 Command chain

There are four main levels in the command chain: strategic, operational, tactical and platform (weapon system). Although working towards solving the same overarching problem, the commanders at each of these levels will have a different view of the same situation. For example, on the strategic level the commander may be concerned with the allocation of national resources. On the operational level the commander may be concerned with the application of military resources. The commander on the tactical level's main concern may be the allocation of domain resources to the given task, whilst the concern on the platform level may be the application of the weapon to the target.

Traditionally, C2 systems focus on situation awareness of a specific operation. On different levels of command, different decisions are being made, thus the situation assessment will necessarily be different. However, information is already being collected and contained within operational and administrative systems. If these systems are made to be interoperable, then the military can harness the capability of all of these systems, and extract the appropriate views (data sets) required for the level of command where a decision is required. In terms of force readiness, a commander cannot have proper situation assessment if he does not also have a clear assessment of the readiness of the forces available to him. Furthermore, it does not help to know exactly how the commander will defend a strategic position, but he does not have the manpower or specialised equipment to execute the plan. Accordingly, determining force readiness is vital to C2. Figure 3 shows the military command levels, with the overlap of the C2 primary functions (refer to Section 1).

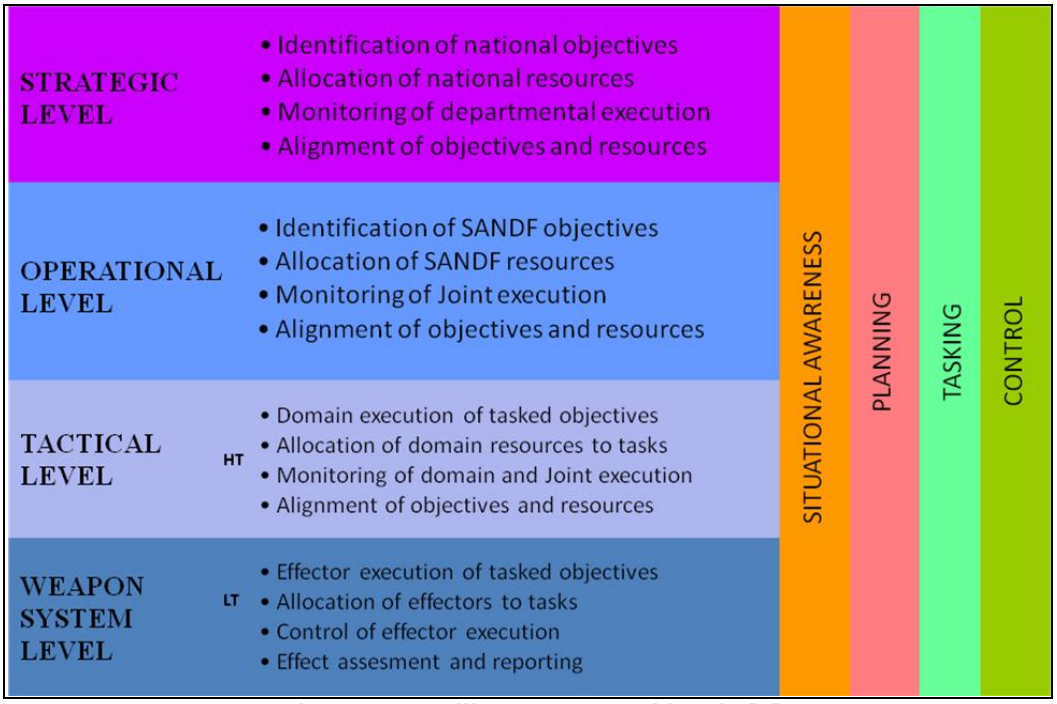

Figure 3: Military command levels [8]

5. Common data model

The complexity of data exchange requires/dictates the use of a common data model to enable full ICT system interoperability. A data model is required to describe the structure and semantics of data that is exchanged between systems, i.e. by understanding what information is most essential for decision making, the required information can accurately be communicated, processed or displayed [4].

A common data model is analogous to a dictionary, or a common interface between different languages. For example, two entities want to communicate. The one entity (in this case, the human resource information system) speaks only English, whilst the other entity speaks only German (the tactical information system). By using an English-German dictionary (the common data model), the two entities are able to communicate with each other, by translating words as necessary into the common language that can be understood by both entities. Without the dictionary, the two entities can only guess what information the other entity has. This is analogous to the current reality of subjective estimations when military personnel interpret information collected from a single information system.

The solution is therefore the introduction of the common data model. This allows the flow of information between interoperable entities, allowing both entities to benefit from the value gained through a holistic systems view. If this common data model is a well-defined, understood and agreed upon model, semantic interoperability is possible. All the information required for force readiness calculation is readily available, in disparate systems, varying data formats and different levels of granularity. If these systems are made to be interoperable and make use of a common data model, then different views for the different command levels can be applied to the data. The commanders can then have the correct force readiness calculated for their level of decision making.

Literature investigation and consultation with knowledgeable resources show that the Joint Consultation Command and Control Information Exchange Data Model (JC3IEDM) is regarded as the most well established and supported common data model available at the time of writing [8]. This model is developed and maintained internationally by the Multilateral Interoperability Programme (MIP), an organisation established to develop specifications for a data model that can be used to share C2 information in a multilateral or coalition environment [9]. The implementation of JC3IEDM internationally testifies to the success of a common data model as interoperability solution [10].

Although the benefits of interoperability systems are widely accepted, it is not always practical to move to interoperable system architecture. In many cases, the development and implementation of a new interoperability system is costly and takes time. In addition, many of the existing systems used by the military are incompatible with each other, as depicted in Figure 4. Although the requirement for interoperability has been identified, the systems involved are not physically able to interoperate with each other. For example, the Navy might have a customised personnel deployment system in place that is different to the Airforce personnel deployment system. These two systems may not be directly compatible to exchange information.

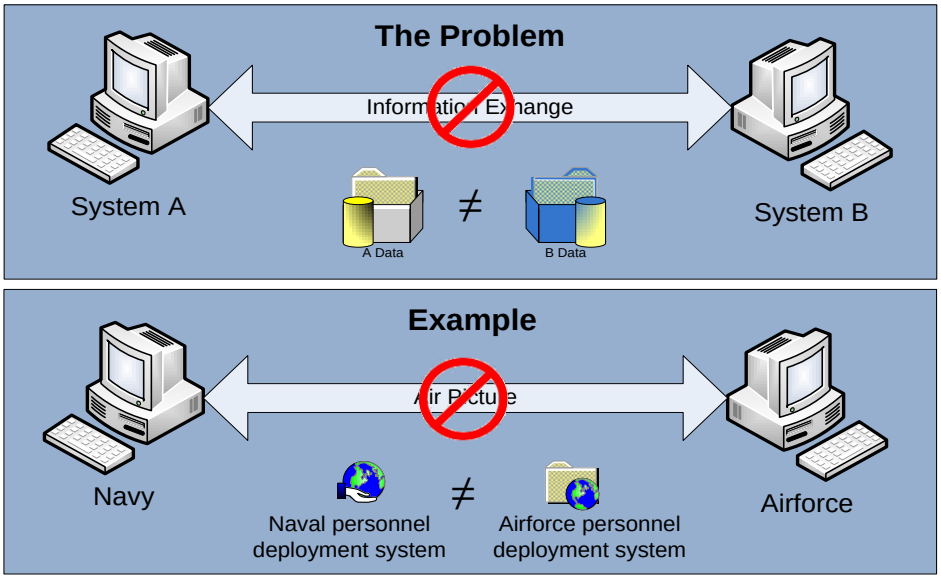

Figure 4: Problem with existing interoperability efforts

This problem can be addressed by introducing a translator function between the two participating systems. This translator will translate the respective systems to a common data exchange model able to translate both participating systems, enabling different parties to communicate with each other, irrespective of the details used by the systems. In keeping with the analogy, the common data exchange model would perform the role of the person creating the dictionary.

6. Enabling the future of C2

In a concept document published in April 2012, it is reported that the South African Army's (SAA) performance has deteriorated drastically. It is estimated that even immediate government intervention is not sufficient, and that it may take up to ten years to reinstate a basic defence ability. In addition, it is reported that the SAA does not adequately protect South African borders, and that awareness in terms of maritime and air-based activities are not sufficient to protect the country during an attack [13]. To address this deteriorating capability, and to ensure the future of C2, interoperability in the military by means of a common data model is imperative.

The operational needs that constitute the basis for the existence of the interoperability solution are that several command posts are supposed to operate together in a coordinated way to perform military operations. To do so, C2 information systems (refer to Figure 1) and user-to-user communication is used to exchange information. The future of these exchanges, through the interoperability solution is supposed to provide value added services to operational users on top of these existing communication networks. The interoperability solution is intended to be used to allow interoperability between units that share a C2 relationship of any kind (operational, technical or administrative) [9].

At the time of writing, the South African National Defence Force's Interoperability Development Environment is developing an experimental programme to help create and manage a common data model for the military systems. This programme is based on JC3IEDM [9] and aims to manage the

common data model as a standard. The programme has, amongst others, the following objectives [10]:

- To become the principal operator-led multinational forum to promote international interoperability of C2 information systems at all levels of command.
- To further develop and improve interface specifications in order to reduce the interoperability gap between different C2 information systems.
- To deliver a C2 interoperability solution in a net-centric environment focused initially on the Land operational user in a Joint environment.

By addressing the incompatible systems and working towards achieving an ability to successfully exchange and use information between systems, consensus can be obtained on international system-independent specifications to achieve semantic interoperability among distributed and diverse C2 information systems. This endeavour supports information exchange across national domains in combined and joint operations, as well as automated analysis workflow construction and discovery [9].

7. Conclusion

Calculating force readiness is not a trivial task; it requires complex algorithms with large real time data sets. This investigative paper established the importance of force readiness in commanding the military, taking availability, capability and dependability into consideration. The paper showed the drawbacks of the current manual reporting based on sitreps and information retrieved from isolated information systems, as well as the potential for subjective force readiness calculations. It introduced the function of interoperability within the environment, and the possibilities that ICT automation holds for the future of C2.

Determining force readiness at the push of a button is a viable reality within the military environment. The only missing component is a common data model to serve as translator between currently disparate military information systems. This paper proposed a proof of concept on the introduction of a common data model to contribute to the automation of force readiness determination, minimising the decision making risk of either under allocation or over allocation of military resources as a result of skewed readiness estimations.

The challenge of automated force readiness calculation lies in the collation of data. By introducing a common data model for the military, it will ensure that data across disparate systems has the same meaning allowing for data fusion. A common data model will also have the benefit of increasing interoperability amongst systems, and increasing each system's functionality. It will also ensure the integration of multiple systems as only one interface is required; for example a system to data model and not multiple system to system integrations. In an agile, network centric military data should be collected timeously and force readiness calculated in real time, allowing commanders to make informed decisions before it is too late. This not only holds for war time scenarios but doubly so for peace time. In war time, the focus is on winning the war; in peace time the military needs to be ready for any likely eventuality.

References

[1] D.S. Alberts & R.E. Hayes, *Power to the edge*. Washington, DC: CCRP Publication Series. 2003. Available online at: http://www.dodccrp.org/files/Alberts_Power.pdf (Accessed 27 June 2012).

[2] Anonymous. *A site about the South African Bushwar/Border War.* ND. Accessed 20120501. Available online at: http://sites.google.com/site/sabushwarsite/interesting.

[3] N. Bau, M. Gerz M. Glauer, Ensuring interoperability of command and control information systems – new ways to test conformance to the MIP solution. *Journal of Telecommunications and Information Technology.* Volume 2, pp. 5 – 13. 2008.

[4] C.H. Builder, S.C. Bankes, & R. Nordin, *Command concepts - A theory derived from the practice of command and control.* National Defense Research Institute. Santa Monica: RAND. 1999.

[5] K.L. Cameron, S.W. Marshall, R.X. Sturdivant & A.E. Lincoln, Trends in the incidence of physician-diagnosed mild traumatic brain injury among active duty U.S. military personnel between 1997 and 2007. *Journal of Neurotrauma,* pp. 29:1-9. 2012.

[6] M.R. Endsley, Toward a theory of situation awareness in dynamic systems. *Human Factors*, vol. 37, no. 1, pp. 32-64. 1995.

[7] A. Kline, M. Falca-Dodson, B. Sussner, D.S. Ciccone, H. Chandler, L. Callahan, & M. Losonczy, Effects of repeated deployment to Iraq and Afghanistan on the health of New Jersey Army National Guard troops: Implications for military readiness. *American Journal of Public Health,* vol. 100, no. 2, pp. 276-283. 2010.

[8] J. Robertson, ND. *IDE – Strategic and operational interoperability strategy.* Internal document. DPSS-CCIW-IDE-1132.

[9] SDMP. *SANDF SDMP Governance document.* SANDF SDMP Unpublished Report, DPSS-CCIW-IDE-1111. 2012a.

[10] SDMP. *SANDF SDMP Standard briefing and best practices.* SANDF SDMP Unpublished Standing Document SD6. 2012b.

[11] M.A. Stahre, R.D Brewer, V.P. Fonseca, & T.S. Naimi, Binge drinking among U.S. active-duty military personnel. *American Journal of Preventive Medicine*, vol. 36, no. 3, pp. 208-217. 2009.

[12] A. Stoltzfus, K. Cranston, H. Lapp, S. McKay, E. Pontelli, R. Vos, & N. Cellinese, *EvoIO: Community-driven standards for sustainable interoperability*. 2010. Accessed 20111110. Available online at: http://hdl.handle.net/10101/npre.2010.4588.1.

[13] J.B. Styan, *Weermag kan SA nie beskerm.* 2012. Accessed 20120424. Available online at: http://www.beeld.com/Suid-Afrika/Nuus/Weermag-kan-SA-nie-beskerm-20120418.

[14] E. Thomas, *Military weapons throughout history.* 2012. Accessed 20120501. Available online at: http://www.ehow.com/about_5059386_military-weapons-throughout-history.html.

[15] US Military Dictionary. *Force in readiness*. The Oxford Essential Dictionary of the U.S. Military, Oxford University Press. ND. Accessed 20120627. Available online at: http://www.answers.com/topic/force-in-readiness.

[16] Wordnetweb. *Interoperability.* 2012. Accessed 20120502. Available online at: http://wordnetweb.princeton.edu/perl/webwn.

Mobile Devices and the Military: Useful Tool or Significant Threat?

Brett van Niekerk, Manoj Maharaj
University of KwaZulu-Natal, Westville, South Africa
vanniekerkb@ukzn.ac.za
maharajms@ukzn.ac.za

Abstract: Smart mobile devices are becoming more prevalent in the military, not only for personal use, but as a battlefield tool. This paper discusses the introduction of smart mobile phones into a military environment, and the possible benefits and risks thereof. The paper will also investigate what these devices mean for information warfare. Throughout the paper, specific examples will be provided of military application of mobile devices, and the threats they pose.

Keywords: Mobile phones, information warfare, mobile malware, mobile security

1. Introduction

Mobile devices are becoming more prevalent in society; in South Africa it is estimated that there is approximately 11 mobile subscriptions to every fixed-line subscription for both data and voice [1]. Despite dedicated military communications, smart mobile devices with increased functionality are appearing in this context, and are even surfacing on the battlefield [2].The United States Army was even building its own transportable mobile phone network in Afghanistan [3].Whilst there are advocates for using mobile devices in the military, there are those that are concerned with the threat it poses [4]. This paper discusses the threats due to mobile devices, their potential beneficial applications, and what they mean in an information warfare context. It should be noted that mobile devices also include portable media players and e-book readers, many of which have wireless and USB connectivity.

Section 2 will provide examples of the threats introduced by mobile devices, and Section 3 will focus on the beneficial applications. The role of mobile devices in information warfare is discussed in Section 4, and Section 5 provides recommendations and Section 6 concludes the paper.

2. Threats related to Mobile Devices

This section will discuss the myriad of threats that smart mobile devices face and their use presents. As smart phones have increased in processing capability, malicious software writers have begun targeting these platforms. Mobile wireless signals can be jammed and intercepted, and it is also possible to intercept the communications in the infrastructure. Using mobile devices for emails and documents may expose sensitive information to unauthorised persons should they gain access to the device; in many cases targeted attacks seek to steal the mobile phones of influential people. Mobile phones have also been used for controlling improvised explosive devices (IEDs) and in instigating violence and uprisings. Due to the various integrated technologies, commercial mobile devices are equivalent to the sensor and communications capability of militaries a decade ago, and therefore can pose a military threat [4].

2.1 Malware

A growing threat due to prevalence of smart mobile devices is that they are increasingly being targeted by malware [5]. Currently there is mobile malware that floods the network with illegitimate SMS messages; however the majority appear to focussed more towards generating income illegally, such as having the infected device call or message premium rate numbers [5]. Mobile malware is following the same trend that traditional PC-based malware followed, in that the most common platform is targeted the most; initially this was Nokia's Symbian platforms, however there has been a dramatic shift towards Google Android devices [6].

Mobile malware primarily appears to be for illegal money-making. The phone dials or sends messages to false premium rate numbers and the attacker receives the amount charged to the unsuspecting owner of the infected device [5]. Some malware is known to transmit the user's information [7], and another was installed on a PC when the phone was connected by USB [8]; these are equivalent to the PC-based malware that targets users for their login details to email and bank

accounts [5]. There are variants of malware that flood the mobile network with spam SMS messages; however these are small minority [9]. Researchers are concerned about a potential mobile worm, which will propagate over the mobile network and result in service outages due to the sheer amount of illegitimate traffic, similar to the Sasser and SQL Slammer worms that infected PC networks in 2003 and 2004 [5].

The malware may disrupt the ability to communicate using the mobile devices. This will not be as severe with other means of communication, however there will be some hindrance of the mobile phones are relied upon. A large threat is that infected mobile devices could be connected to computers on a sensitive network, thereby infecting the network. It should be mandatory for any mobile device entering a networked environment to have anti-virus applications installed. System or network administrators should prevent devices from connecting to the wireless access points unless they have been checked to meet the minimum security requirements [10].

2.2 Jamming

The wireless channels used by mobile communications could be jammed. Whilst military electronic warfare solutions are sometimes designed specifically for this purpose, home-made solutions and commercial devices are also able disrupt mobile signals in a localised area. An example of this is a disgruntled traveller using a jammer to disrupt signals on busses [11]. It is also believed that insurgents with sympathisers in mobile phone networks force the networks to shut down to prevent their operations from being tracked [3].

2.3 Interception

The wireless channels used by mobiles to communicate to the base stations could be intercepted. Researchers assessed the security of the encryption for GSM networks, and found that the encryption could be broken [12]. It is also likely that military electronic warfare communications intelligence solutions can intercept and eavesdrop on commercial mobile communications.

In Greece, attackers managed to penetrate the mobile infrastructure hardware and eavesdrop on senior political and corporate figures. It was not clear if the initial system compromise was an inside job or an attack via the network; however, the attackers were able to manage the attack through the Internet connections where they were able to add or remove targeted mobile phone numbers from those being intercepted [13]. Some of the war logs released by Wikileaks indicated that the United States commanders in Afghanistan were concerned that insurgents had collaborators in the national mobile infrastructure, which was also used by the soldiers and diplomats for communications. Their calls could therefore be intercepted at the central mobile switching stations, and sensitive information could then be leaked to the insurgent groups [14]. The Israeli military is also reported to have gained access to mobile networks in the Middle East, and left messages on voice-mail or sent SMS messages [15]; this level of access also implies an ability to listen to messages or conversations. Vulnerabilities in the Blackberry servers were also rapidly patched after it was found that even a link to a malicious image could result in the server being hijacked [16].

The threat of interception mitigated through the use of additional encryption of messages (text, multimedia, and email) and voice communications. This will protect the communications in both the wireless channels and when transiting through the physical infrastructure. In the United States, government and military personnel are being provided with secure mobile devices to work with classified documents over cellular networks [17].

2.4 Information Leaks

Mobile devices are susceptible to being lost or stolen. Often executives are targeted at airports, where there laptops are stolen when going through the airport security scanners; this can also apply to mobile phones. Any information contained on these devices could be breached if there is no password set [10]. It is possible to delete information remotely; however, if a laptop or mobile device is stolen from a car or pick pocketed the information may be compromised before the user realises it has been stolen [10]. Using mobile devices to access emails and sensitive networks increases the probability of sensitive information being stored on the mobile device; this increases the risk of severe information leaks. In addition to being lost or stolen, information can be leaked through devices with open wireless connectivity; research has shown that it is also possible to monitor the magnetic fields

of the device circuitry to access information on the device [18]. Therefore measures should be taken to prevent files and email being accessed in the event a device is lost or stolen by protecting the device with a password or PIN, encrypting the contents, and having the ability to remotely disable the device.

Should a mobile device with open wireless or Bluetooth settings be connected to a computer inside the network, it forms what is similar to a rogue wireless access point. It is therefore possible to gain access to the network by connecting through the open wireless. This effectively subverts all the networks perimeter security controls [10]. Malware on mobile devices may also be used to install backdoors on corporate networks when the device is connected to a PC, subverting the network perimeter security [19]. System administrators should prevent email or network access until the device has been checked to ensure it meets the minimum security requirements; this will aid in preventing any leaks due to lost devices or unintended network access.

2.5 IEDs

One method used for detonating improvised explosive devices (IEDs) is by using mobile phones; these devices account for the majority of casualties in Afghanistan and Iraq [20]; however they have also been used in the bombing campaigns in Cape Town in the 1990s [21]. The use of cellular phones and other wireless devices for detonating IEDs has resulted in billions of Dollars being spent on research and procurement to counter these threats [20].

2.6 Mobile Devices in Uprisings and Inciting Violence

Mobile devices have played a large role in many instances of popular uprisings and civil unrest; the most noticeable are the Arab Spring events and UK riots in 2011; SMS services were also used in a popular uprising in the Philippines in 2003, to incite racial violence after the Kenyan elections in 2008, in unrest in Iran, Moldova, and China in 2009, and in the Mozambique food riots of 2010 [10], [22]. Combined with social media, mobile devices can become an impromptu command and control system for mass demonstrations and civil disobedience. Due to the integrated cameras, social media connectivity and other communications, they may also be a useful intelligence tool; photos can be taken and uploaded quickly; this can be used by protestors or insurgents to keep track of troop and police movements. In a military context, this may prevent a surprise attack, as images of troop movements can be uploaded onto the public internet.

3. Mobile Devices as a Tool

Many applications are available for smart mobile devices; there is a move to produce military-oriented applications to allow soldiers to access cultural intelligence and phrasebooks, technical manuals, and maps [23], [24]. It is reported that popular devices can withstand combat scenarios [25] and that some existing devices and applications are already being used by the military [2]. It is therefore apparent that mobile devices may have benefit to the military; with minor modifications commercial equipment may provide a platform to perform multiple functions. This section discusses the potential benefits of mobile devices to the military.

3.1 Peacekeeping and Disaster Response

Mobile phones have proved effective in crowdsourcing information in conflict and the response to natural disasters [26]. Mobile phones played a major role in the recovery after the 2004 Indian Ocean Tsunami [27]; the gathering of information in the 2008 post-election violence in Kenya and in the aftermath of the Haiti relied heavily on mobile communications [26]. An advantage of mobile phones is the ability to geo-locate devices; this has resulted in the inclusion of mobile communications in early the warning systems [27]. Mobile phones will therefore be crucial to any military emergency response teams or peacekeeping forces for gathering information. A mobile infrastructure that is transportable, such as the one being developed by the United States military [3], can be deployed to the affected area to replace damaged infrastructure and provide a dedicated mobile network for emergency workers.

During deployments on peacekeeping operations, troops require some contact with their families at home. In some instances, satellite communications are provided for this purpose. A disadvantage of using satellite communications is the long logistic support lines required for specialist spares and technicians [28]. Integrated military mobile communications may have the advantage that the majority

of the components are available in the host infrastructure, possibly making spares easier to source. The devices will also be able to operate with any existing national infrastructure. The only specialist component of the mobile communications is the additional encryption and security; as these can take the form of mobile applications, they will be easily transportable on removable storage media.

3.2 Command, Control, Communications, and Intelligence (C3I)

The use of mobile phones and social media applications to coordinate mass demonstrations illustrates the potential for their use in command and control. Useful applications and the variety of integrated technologies and communications abilities make mobile devices versatile. Whilst these technologies have been cited as a military threat [4], they may be a military asset if employed effectively. Integrated GPS and geo-location can be used for navigation and remote tracking of forces, and the photographic, video, and sound recording capabilities will be beneficial for gathering intelligence from the front-lines. A project to use mobile phones as a sensor grid is described in [29]. Portable towers and infrastructure which can be rapidly deployed to forward operating bases will provide a convenient C3I platform. It will also be more secure than utilising the local infrastructure [3], and additional security measures can be introduced into the design.

4. Mobile Infrastructure and Information Warfare

Sections 2 and 3 have described some threats and benefits related to mobile devices. As the mobile infrastructure is a major component of civilian communications, and now with its introduction into the military environment, it may become a target and tool for information warfare operations. As mentioned in Section 2.6 and 3.2, mobile communications is a useful tool for command and control, and has been used successfully in mass demonstrations; the vulnerability to interception and information leaks also provides the ability for intelligence gathering, as discussed in Sections 2.3 and 2.4. This section discusses the relevance of network warfare, psychological operations (PSYOPs), and electronic warfare to the mobile infrastructure.

4.1 Network Warfare

As is evident from Section 2, mobile infrastructures have been penetrated through network connectivity in order to both broadcast and eavesdrop on messages. As the mobile network and mobile infrastructure are essentially the same, network warfare operations against the mobile networks can also be considered as information infrastructure warfare.

Due to Web-based SMS services and integrated Web browsing and social networking, the mobile infrastructure is susceptible to denial-of-service attacks. Web SMS platforms can be compromised and used to flood the mobile network with illegitimate traffic, or mobile malware can transmit large quantities of illegitimate requests or messages. The capacity of the wireless control channels may be overwhelmed, or the capability of the switching centres could be overloaded [10]. Researchers have specifically raised concern that the prevalence of mobile devices in Africa will contribute to the growing information security problems on the continent, increasing the vulnerability of Africa to cyber-attacks [10], [30].

As discussed in Sections 2.1 and 2.4, malware can be installed on PCs and networks through mobile devices. Therefore the mobile device itself becomes a propagation vector for computer-based network warfare. This malware can be used for compromising information of conducting denial-of service attacks.

4.2 PSYOPs

As Middle Eastern mobile infrastructures were reportedly penetrated on multiple occasions by the Israeli military in order to distribute messages via SMS and voicemail [15], and mobile devices were used in Kenya to incite racial violence, the Arab Spring events, the Mozambique food riots [10] and the London riots [22], the possibility of the mobile infrastructure as a PSYOPs tool is apparent. Messages can be sent by using legitimate systems or by compromising existing services.

4.3 Electronic Warfare

Due to the wireless channels mobile communications are susceptible to electronic warfare, as discussed in Sections 2.2 and 2.3. Mobile infrastructure in the vicinity of the frontline can be easily targeted by adversary electronic warfare operations; however civilian infrastructures at home would

be out of range for troops deployed long-distance [10] (such as coalition forces in the Middle East and South African forces in Central Africa). Electronic warfare has also been employed to combat the threat of wirelessly detonated IEDs [20], illustrating the relevance of electronic warfare and the mobile infrastructure.

4.4 Summary

A number of aspects of information warfare are directly relevant to mobile devices and the mobile infrastructure. The role of mobile infrastructures and devices play in information warfare can be considered as both a threat and a tool; these techniques can be used by friendly forces, or by an opponent against your own forces. Some aspects of the relevance to information warfare are a direct result of the possible threats presented by mobile devices; in particular, the vulnerability to malware which allows for network warfare, and the vulnerability to interception, allowing for intelligence gathering. Figure 1 provides a summary of the relationship between information warfare and mobile infrastructure and devices. The figure follows the six functional areas or pillars of information warfare that are defined by the South African National Defence Force [30], where network warfare and information warfare have been combined due to their similarities in this specific case.

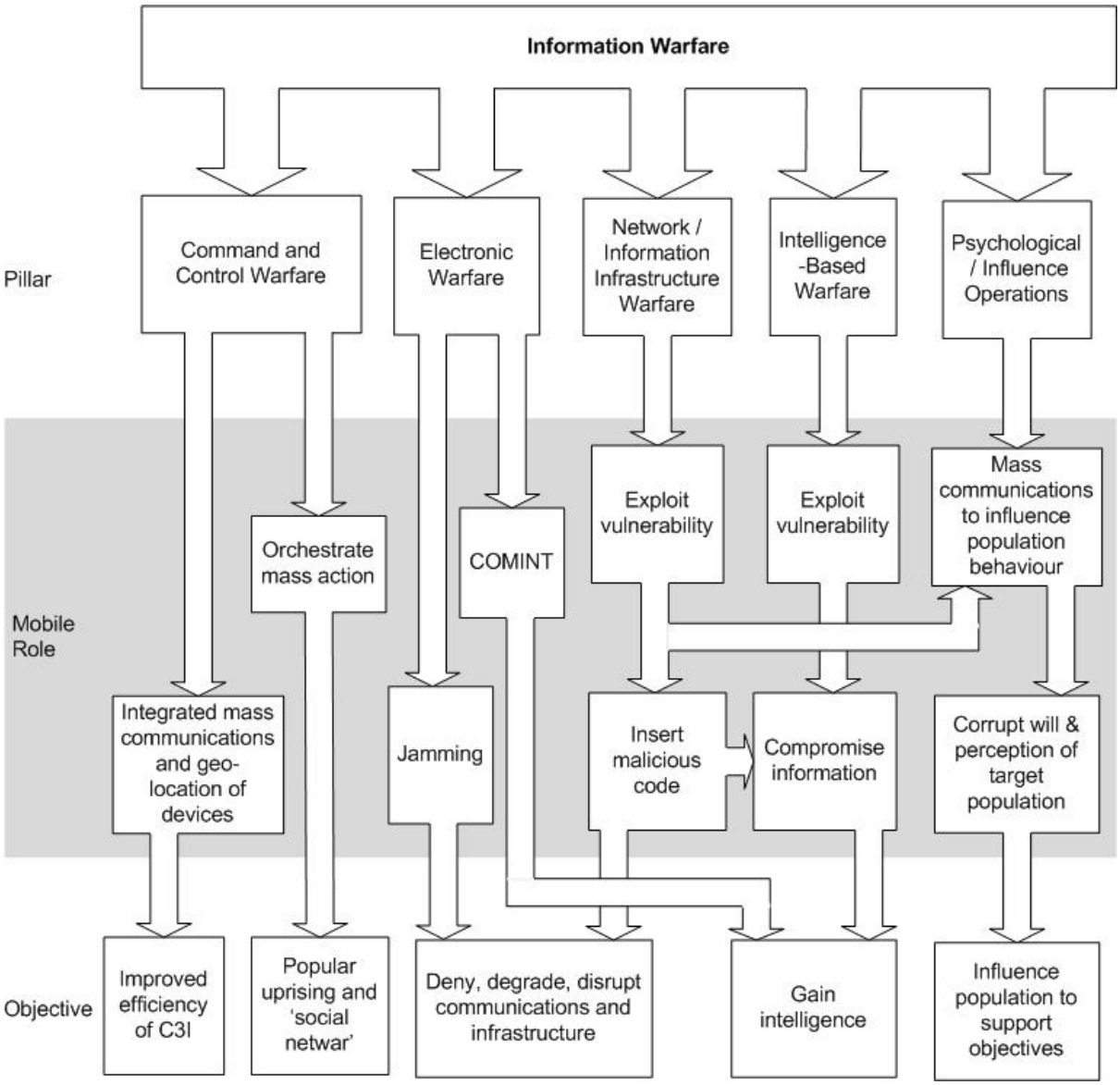

Figure 1: Mobile Devices in Information Warfare [10]

Due to the variety of threats, security concerns, and benefits of mobile devices, it is advisable that all military personnel undergo awareness training, and clear policies are in place regarding mobile device usage, reporting of potential security incidents, and ethical considerations for use in information warfare. The policies will provide a solid platform to govern the use of these devices, and the awareness training ensures that the personnel are aware of the policies and prevalent threats.

5. Recommendations

This section recommends a course of action for the South African Department of Defence and National Defence Force. Wolfswinkel presented on the importance of a desktop strategy for the South African Department of Defence [32]. Similarly, a mobile device strategy is required. This is evident from the United States Department of Defence introducing a mobile device strategy. Their strategy aims to [33]:

- Upgrade their infrastructure to support mobile devices;
- Introduce standards and policies for the use of mobile devices; and,
- Develop and implement defence applications for mobile devices.

Similarly, a strategic plan should be developed and implemented by the South African Department of Defence and Defence Force, should one not already exist. Initially the focus should be on implementing policies for the use and security of mobile devices. Policies should be designed to accommodate research, development, and implementation of mobile applications and their distribution. Research in the United States includes using mobile phones as a sensor grid [29] and adapting the Apple online application store's business model for application development and distribution in the armed services; this project has been implemented on a limited basis [34]. Where necessary, equipment should be requisitioned, particularly for counter-IED operations and surveillance of mobile communications in operational areas. Expertise should be developed to protect South African infrastructure from cyber-attacks.

Furthermore, existing funding mechanisms for postgraduate research projects can be used as an incentive for academia to develop mobile applications and investigate technical and social aspects of introducing mobile devices into the South African Defence Force for operational purposes.

6. Conclusion

Mobile communications is one of the most ubiquitous technologies. In a military environment, mobile devices can be viewed as both a threat or a potential tool for C3I, peacekeeping, and disaster relief. The mobile infrastructure and devices also have a relevance to information warfare. As this paper uses actual incidents to illustrate points, it is clear that the concerns are real. Therefore there is little question that mobile devices and the related infrastructure need to be considered from military and information warfare perspectives.

The internal threats due to the introduction of mobile devices can be managed by introducing additional security measures and processes. External threats, such as the use of mobile devices as a C3I tool by insurgents or another adversary might not be easily mitigated directly. By introducing such technology into one's own arsenal this threat is mitigated by reducing or nullifying the advantage the adversary gains from utilising the mobile communications. Therefore the benefits gained by formally integrating mobile devices into military doctrine and operations outweighs the risks, provided they are properly accounted for and managed. Through proper integration, these devices will provide both a useful tool, and mitigate the risks posed through ad-hoc allowance of devices or ignoring the issues. The introduction of policies and awareness training can be considered essential for the efficient and secure introduction and integration of mobile devices into the military environment.

Acknowledgements

This paper is related to the first author's PhD thesis, which was supported by grants from South African Department of Defence, and the Armscor Ledger Program through the Cyber Defence Research Group at the Council for Scientific and Industrial Research, Defence, Peace, Safety and Security (CSIR-DPSS), and the University of KwaZulu-Natal.

References

[1] International Telecommunications Union, ICT Data and Statistics, 2011. Accessed 20110531. Available online at: http://www.itu.int/ITU-D/ict/statistics/index.html

[2] StrategyPage.com, "Smart phones go to war," 13 July 2010. Accessed 20100714, Available online at: http://www.strategypage.com/htmw/htiw/articles/20100713.aspx.

[3] StrategyPage.com, "Mobile cell towers advance on all fronts," 5 November 2010. Accessed 20101105, Available online at: http://www.strategypage.com/htmw/htecm/articles/20101105.aspx.

[4] N. Shachtman, "Darpa warns: your iPhone is a military threat," Wired.com DangerRoom Blog, 29 February 2012. Accessed 20120308, Available online at: http://www.wired.com/dangerroom/2012/02/darpa-iphone/.

[5] M. Hyppönen, F-Secure mobile security review September 2010, FSecure News You Tube Channel, 11 October 2010. Accessed 20101213, Available online at: http://www.youtube.com/watch?v=fJMLr8BDQq8.

[6] McAfee Labs, McAfee threats report: third quarter 2011, 2012. Accessed 20120209, Available online at: http://www.mcafee.com/uk/resources/reports/rp-sda-cyber-security.pdf?cid=WBB048.

[7] N. Seriot, "iPhone privacy," Black Hat DC 2010, Arlington, Virginia, 2010. Accessed 20100626. Available online at: http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html.

[8] R. Charette, "First Energizer, now Vodaphone: more malware found in store bought consumer electronic products," IEEE Spectrum Riskfactor Blog. Accessed 20100503. Available online at: http://spectrum.ieee.org/riskfactor/computing/it/malware-found-in-store-bought-consumer-electronic.

[9] J.A. Morales, Timeline of mobile malicious code, hoaxes, and threats. In K. Dunham (Ed.), Mobile malware attacks and defense (pp. 35-70). Burlington: Syngress Publishing, 2009.

[10] B. van Niekerk, Vulnerability assessment of modern ICT infrastructure from an information warfare perspective, PhD thesis, University of KwaZulu-Natal, 2011.

[11] F. Van Allen, "Vigilante jamming cell phone calls on city buses to help preserve peace and quiet," www.Tecca.com, 1 March 2012. Accessed 20120308. Available online at: http://www.tecca.com/news/2012/03/01/cell-phone-jammer-philadelphia-buses/.

[12] S. Ragan, "GSM Alliance downplays seriousness of GSM Project," The Tech Herald, 28 August 2009. Accessed 20100406, Available online at: http://www.thetechherald.com/article.php/200935/4332/GSM-Alliance-downplays-seriousness-of-GSM-project

[13] V. Prevelakis, and D. Spinellis, "The Athens Affair," *IEEE Spectrum*, July 2007. Accessed 20100312. Available online at: http://spectrum.ieee.org/telecom/security/the-athens-affair/1

[14] S. Tisdall, "Afghanistan war logs: NATO feared Taliban could tap it mobile phones," The Guardian, 25 July 2010, Accessed 20110816, Available online at: http://www.guardian.co.uk/world/2010/jul/25/taliban-tapped-mobile-phones-afghanistan

[15] StrategyPage.com, "Gaza cellphones targeted," 2 January 2009. Accessed 20100407. Available online at: http://www.strategypage.com/htmw/htiw/20090102.aspx

[16] D. Goodin, "Smartphone images can hijack BlackBerry servers," The Register, 11 August 2011. Accessed 20110812. Available online at: http://www.theregister.co.uk/2011/08/11/blackberry_high_severity_bug/

[17] M. Milian, "U.S. government, military to get secure Android phones," CNN, 3 February 2012. Accessed 20120315. Available online at: http://edition.cnn.com/2012/02/03/tech/mobile/government-android-phones/index.html?eref=rss_mostpopular

[18] Technology Review, "Eavesdropping antennas can steal your smart phone's secrets," Blacklistednews.com, 6 March 2012. Accessed 20120323. Available online at: http://www.blacklistednews.com/Eavesdropping_Antennas_Can_Steal_Your_Smart_Phone%27s_Secrets/18319/0/38/38/Y/M.html

[19] E.B. Parizo, "Mobile device attacks to enable more enterprise network intrusions," TechTarget.com, 29 February 2012. Accessed 20120308. Available online at: http://searchsecurity.techtarget.com/news/2240118712/Mobile-device-attacks-to-enable-more-enterprise-network-intrusions

[20] D. Eshel, "Defeating IEDs," *Journal of Electronic Defence*, vol. 10, no. 12, pp. 28-42, 2007.

[21] A. Sabasteanski, Patterns of global terrorism 1985-2005: U.S. Department of State reports with supplementary documents and statistics, Berkshire Publishing, 2005.

[22] N. Potter, "London Riots 2011: protestors use Blackberry Messenger; hackers support them," ABC News, 2 August 2011. Accessed 20120229. Available online at: http://abcnews.go.com/Technology/london-riots-2011-protesters-blackberry-messenger-hackers-back/story?id=14264839

[23] N. Hodge, "A combat zone iPhone? Soldiers have an app for that," Wired.com, 2 March 2010. Accessed 20100303. Available online at: http://www.wired.com/dangerroom/2010/03/a-combat-zone-iphone-soldiers-have-an-app-for-that/

[24] R. de Silva, "Military smartphones: the information super iWay!" DefenceIQ, 15 March 2012. Accessed 20120315. Available online at: http://www.defenceiq.com/defence-technology/articles/the-information-super-iway/

[25] T. Devaney, "Soldiers in battlefield turn apps into arms," The Washington Times, 24 January 2011. Accessed 20110126. Available online at: http://www.washingtontimes.com/news/2011/jan/24/soldiers-on-battlefield-turn-apps-into-arms/?page=1

[26] J. Heinzelman, and C. Waters, Crowdsourcing crisis Information in disaster-affected Haiti, United States Institute of Peace, October 2010. Accessed 20120328. Available online at: http://www.usip.org/files/resources/SR252%20-%20Crowdsourcing%20Crisis%20Information%20in%20Disaster-Affected%20Haiti.pdf

[27] D. Coyle and P. Meier, New technologies in emergencies and conflicts, The United Nations Foundation and Vodafone Foundation, 2009. Accessed 20120419. Available online at: http://www.globalproblems-globalsolutions-files.org/pdf/UNF_tech/emergency_tech_report2009/Tech_EmergencyTechReport_full.pdf

[28] I.R. Fordred, Satellite communication strategy, Military Information and Communications Symposium South Africa (MICSSA) 2009, Pretoria, 20-24 July 2009.

[29] Peter J Young, A mobile phone-based sensor grid for distributed team operations, Master's thesis, Naval Postgraduate School, September 2010. Accessed 20120620. Available online at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA531740

[30] Seymour Goodman and Andrew Harris, The coming African tsunami of information insecurity, *Communications of the ACM, 53(12)*, 24-27, 2010.

[31] M.S. Brazzoli, Future prospects of information warfare and particularly psychological operations, in L. le Roux (ed.), South African Army Vision 2020, Institute for Security Studies, pp. 217-232, 2007.

[32] Johann Wolfswinkel, The importance of a desktop strategy in the Department of Defence, 5th Military Information and Communications Symposium South Africa (MICSSA 2011), Pretoria, July 2011. Accessed 20120620. Available online at: http://www.micssa.co.za/4.%20Presentation%20-%20MICSSA%202011%20DIAMOND/4.2%20Diamond%20Wednesday%2020-07-2011/2-01A-3%20Wolfswinkel-MICSSA11%20Desktop%20strategy%20Wolfswinkel%20v1.1.pdf

[33] Eric Chabrow, DOD outlines mobile device strategy, GovInfoSecurity.com, 18 June 2012. Accessed 20120619. Available online at: http://www.govinfosecurity.com/dod-outlines-mobile-device-strategy-a-4870

[34] Brad A. Naegle and Douglas E. Brinkley, Apple App Store as a business model supporting U.S. Navy requirements, Naval Postgraduate School, 25 October 2011. Accessed 20120620. Available online at: http://www.dtic.mil/dtic/tr/fulltext/u2/a555658.pdf

Using a Layered Model to place EW in Context within the Informationsphere

Francois Maasdorp, Warren Du Plessis
Council for Scientific and Industrial Research, Defence Pease Safety and Security, Pretoria, South Africa
fmaasdorp@csir.co.za
wduplessis@csir.co.za

Abstract: In recent years, a discussion on relationship between Electronic Warfare (EW), Information Warfare (IW), Cyber Operations, Net-Centric Warfare, Command and Control, Information Operations (IO) and other constructs has emerged. This paper proposes a layered model, similar to the Open Systems Interconnection (OSI) model in an attempt provide a new perspective on this discussion. A number of layers are defined and the roles and relationships between EW, IW, IO etc. are considered with respect to this new model. This approach is extremely powerful as it emphasises the complementary natures these fields should have, rather than highlighting rivalry between these fields as often happens. An attack on an 802.11g (WiFi) link is used as an example to display the value this layered approach can offer by emphasising the complementary, yet unique roles of EW and Cyberspace.

Keywords: Electronic Warfare (EW), Information Operations (IO), Information Warfare (IW), Cyberspace, Electro Magnetic Spectrum (EMS), Informationsphere.

1. Introduction

In recent years, a common trend within the Electronic Warfare (EW) community involves debates on the rightful place of EW among other constructs such as Cyberspace [1]-[4], IW [5], Net-Centric Warfare [5] and Information Operations (IO) [6], [7]. The latest trend in this regard includes the involvement of physics into arguments that defend the rational for involving EW in categories such as Cyberspace, Information Operations (IO) [1], [8] etc. Therefore, as observers to this debate and with a background in the telecommunications industry, we would like to propose an alternative perspective which we believe will help simplify the discussion.

We start by defining some concepts that are key to this discussion. Cyberspace is defined in [1] as

> "*A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers*."

From this definition, one can see that Cyberspace cannot exist without physical networks to connect systems to form networks. These physical connections rely on the Electromagnetic Spectrum (EMS) to convey data. The EMS is thus a key component of physical networks, and by extension, Cyberspace. In [9], the EMS is defined as

> "*EMS refers to the range of frequencies of the electromagnetic radiation from zero to infinity. The spectrum is divided into bands ranging from radio frequencies at the low end to x-ray and gamma frequencies at the high end*."

Although not directly stated in the quote, the electro-optical region is also part of the EMS and is situated between the radio frequency region and the x-ray region. EW traditionally refers to a military action involving the use of electromagnetic (EM) and directed energy to control the EMS in by means of sensing, attack, and protection. These abilities are known as Electronic Support (ES), Electronic Attack (EA) and Electronic Protection (EP) and are the cornerstones of EW. EMS control (EMC) has lately been added to EW nomenclature to allow for a better effects-based emphasis.

A practical example is shown in Figure 1. A radar is deployed in the field to alert Head Quarters (HQ) of air activity in the vicinity. Upon the radar detecting a target, the positional information is sent to HQ via a wireless link to allow a decision to be made by the commanding officer. Note that a land line or fibre optic cable could also have been used to communicate the information without affecting the principles.

In this scenario, the role of EW would traditionally be limited to the accurate detection of the target by the radar or prevention of such detection by an adversary as these processes are inherently based on the EMS. However, as the EMS is also used in the wireless link, EW applies to this network as well. For example, an adversary could use EW jamming at the EMS level to alter the target position information sent over the wireless link. If caution is not exercised, the HQ would never know about this deception/denial because the radar would report no jamming. Therefore, EW's capability to manipulate and exploit the EMS is a valuable capability in the communications aspects of this scenario.

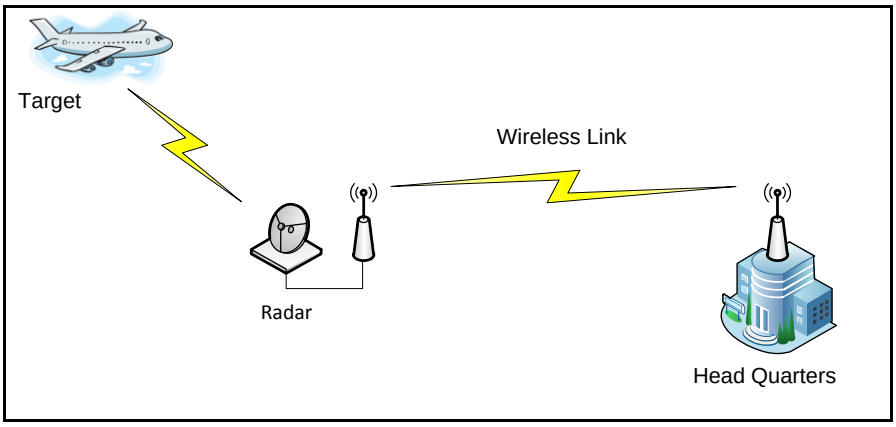

Figure 1: Utilisation of the EMS

2. OSI Model

As stated in the introduction, the main underlying principle of EW is its interface to the EMS. However, EW systems are increasingly required to provide input to and take instructions from other networks and systems in order to achieve the desired operational effect. Keeping this in mind, we now shift our focus to the computers/telecommunication domain.

In the early 1980s (the early days of the internet), the computer and telecommunications industries experienced a similar dilemma, i.e. defining protocols to connect multiple computers for the mass distribution of information, while exploiting different fields of expertise stretching from antennas to operating systems.

The solution to this problem came in the form of the development of an architecture for computer communications. This development was undertaken under the auspices of the International Organisation for Standardisation (ISO) and the result was the Open Systems Interconnection (OSI) model. The model, displayed in Figure 2 [10], consists of seven layers, namely the application, presentation, session, transport, network, data-link and the physical layers. The key to this model is the principle of abstraction whereby the intricacies of each layer are hidden (abstracted) in every other layer while still allowing relevant information about other layers to be communicated. This approach is extremely powerful because it allows engineers to focus on the issues related to each layer without requiring a detailed knowledge of every aspect of all layers. In this way, engineers working on the application layer (e.g. software running on a system) do not need detailed knowledge of the physical layer (the physical wires or EM waves connecting systems), but still have access to information they require (e.g. bandwidth, latency, etc.). Note that higher levels in the model do not imply additional or reduced complexity, or any kind of superiority or inferiority, merely a different view of the system.

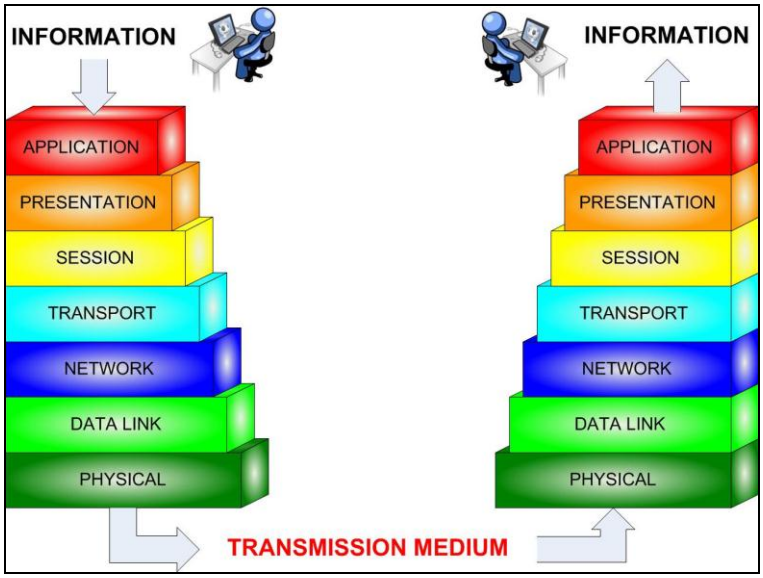

Figure 2: OSI model [3]

3. Proposed Model

In the case of the relationships between EW, Cyberspace, IW, IO, etc. within the defence domain, a similar architecture or model can be used, hopefully addressing many of the debates surrounding this topic. Therefore we propose the adoption of a similar approach to the OSI model for this purpose but define new layers. This is crucial as a lack of clear definitions is one of the underlying causes of confusion about the roles and responsibilities of each field.

With reference to Figure 3, we start by defining the bottom or first layer as the layer responsible for access to the EMS and label it the Access Layer. EMS systems, such as EW systems, communication systems, radars etc., operate at this layer as they all provide an interface to the EMS. In the light of a recent article published in the Journal of Electronic Defence (JED) [8], this seems reasonable as the article argued that every EW practitioner should have some knowledge of physics, including electromagnetic wave propagation, modulation types, etc. Thus, we see the Access Layer, in which EW resides, as the ability to manipulate and exploit the EMS and pass information to and from higher layers in the model.

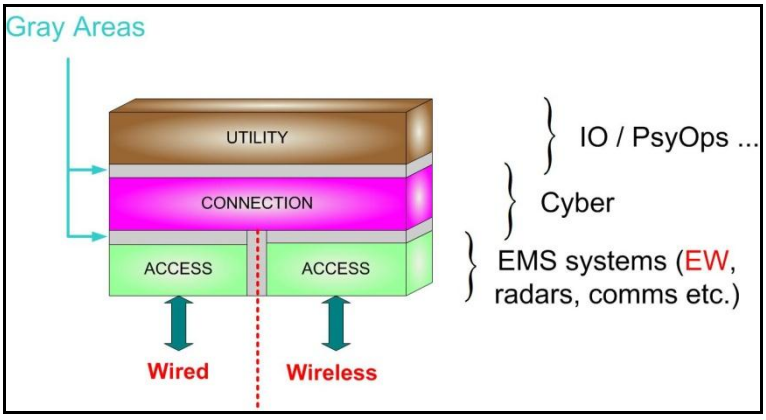

Figure 3: Proposed model to place EW in context

The second layer is labelled the Connection Layer and is defined as the layer responsible for the manipulation and transport of data within a network. At this point, data would be manipulated as bits or packets, rather than modulated signals as is the case in the Access Layer. This layer is also

commonly referred to as Cyberspace and is the region in which IW practitioners typically operate. Thus, IW practitioners are not required to have expert knowledge of interactions with the EMS – or even whether data are transferred via coaxial cable, fibre optic link or radio link – but rather to focus on the manipulation of data at bit or packet level to accomplish the appropriate objectives.

The third and final layer, labelled the Utility Layer is placed at the top of the model and is defined as the layer which exploits the lower layers to achieve a desired effect, again without requiring detailed knowledge of those lower levels. The Utility Layer is thus the level in which operations are conducted, for example PsyOps, IO, etc.

This approach demonstrates the differences between EW, Cyberspace and IO in a very natural way, emphasising both the importance and complementary nature of each of these fields. The grey areas displayed in Figure 3, illustrate that the interfaces between the layers are not intended as clear dividing lines and that subject matter expertise can overlap. For example, the interface between EW operating at the Access Layer, and Cyberspace operating at the Connection Layer could vary depending on the task at hand, but the for example the transition from modulation in the Access Layer to binary ones and zeros in the Connection Layer is seen as a common transition. However, this should be determined by the subject matter experts residing in the respective layers. Lastly, note the Access Layer has been split into two sections to emphasise the fact that EW focuses predominantly on the wireless scenario (though EW expertise can be relevant to the wired case). Furthermore, all layers in the model do not necessarily need to be present in every situation. For example, an EW protection system such as a Directed Infrared Countermeasures (DIRCM) system on board an aircraft would respond immediately to a missile fired on it without waiting for a command to be issued from the Utility Layer.

Quoting from David J. Lonsdale's book, titled "The Nature of War in the Information Age" [11]:

> "*Strategic power can be projected over the current known dimensions such as sea, land, air and space. A fifth dimension in which strategic power can be projected is also described as the infosphere. The infosphere is the environment where shapeless information exists and flows both in structured and or random ways. The infosphere is where facts or knowledge reside and is represented or conveyed by a particular sequence of symbols, impulses or characterisations. It is also the domain where command and control takes place. The Electromagnetic Spectrum, Network Spectrum and the Human Domain (cognitive domain) are the spine of the infosphere*."

With reference to this quotation, the information sphere is made up of the EMS, network spectrum and the human domain. The proposed model mirrors this approach with the Access Layer, which accesses the EMS, the Connection Layer, which is equivalent to the network spectrum, and the Utility Layer, which is the human domain in which operations are conducted. Therefore, this model is clearly supported by the infosphere approach presented in [11].

4. Jamming example on 802.11b

This section provides an example to illustrate the value of using the proposed model. Recent experimental results published by EW staff at the CSIR [12] have shown that an 802.11b wireless link is vulnerable to smart attacks.

The classic method of performing such an attack is to raise the RF noise floor to levels which prevent the wireless system from transferring data over the link. This attack is therefore aimed towards the Access Layer in Figure 3. However, since the 802.11b standard has built-in intelligence to compensate for RF interference, it senses the link interference and adjusts the link power to a level at which the system is able to re-establish the link and proceed with the data transfer. Therefore, the jammer and the 802.11b communication link enter into a power struggle in which each party aims to emit more power that the other. Furthermore, the user of the 802.11b system will be able to determine that such an attack is taking place from the information captured by the system.

Making use of a more intelligent attack, and aiming more towards the data-link layer of the OSI model, it was proven that an attack could be performed very efficiently (and covertly) without entering into a

power struggle [12]. This attack works by injecting signals at the Access Layer which exploit the access-control mechanism of the 802.11b protocol to cause the desired breakdown in the communications. Furthermore, it would not be easy for a user to determine that an attack was taking place, potentially increasing the value of the attack.

Using a simple noise jamming scheme would clearly reside in the Access Layer and be an EW task. A traditional Denial of Service (DoS) attack where the network is overwhelmed with synthetically generated data would equally clearly reside in the Connection Layer and be a Cyberspace task. While still predominantly working in the Access Layer, the approach used in [12] moves towards the Connection Layer because knowledge of the access-control mechanism is required. The value of the proposed model in this context is that is shows that we, as EW practitioners, need to enlist the help of our Cyberspace colleagues to take this work further because future extensions will rely on a knowledge of issues like authentication and encryption which clearly lie in the Connection Layer. In fact, the lack of such knowledge is one of the main factors which have meant that this work has not been continued.

6. Conclusion

In conclusion, an approach similar to the OSI model is proposed to clarify the relationships between EW, IW, Cyberspace, IO etc. This approach would allow debates surrounding EMS, and who takes responsibility for it, to be placed in context. We believe that this approach will go a long way towards clarifying the different, yet complementary roles of EW, IW, Cyberspace, IO and any other system or concept which interacts with the EMS. However, the OSI model is very seldom applied to specific systems without modification, so it is reasonable to expect the same will occur with the proposed model.

Acknowledgements

The authors wish to thank Jacobus Vlok for his assitance with the development of the 802.11b attack described above. The authors also wish to thank Christo Cloete and Joey Jansen van Vuuren for their insightful suggestions to this paper.

References

[1] R. Hahn, “Physics of the cyber-EMS problem, why we have the language wrong”, *Journal of Electronic Defense*, vol. 33, no. 11, November 2010, p. 44.

[2] J. L. Borque, "Why EW is not part of Cyberspace," *Journal of Electronic Defense*, vol. 31, no. 9, September 2008, pp. 38-40.

[3] J. L. Borque, "A (pragmatic) future for joint electronic warfare: does EW + CNO = cyber?" *Journal of Electronic Defense*, vol. 31, no. 9, September 2008, pp. 30-38.

[4] M. Kunkel, "New cyber definition excludes EW" *Journal of Electronic Defense*, vol. 31, no. 11, November 2008, p. 26.

[5] R. Smith and S. Knight, Applying electronic warfare solutions to network security. *Canadian Military Journal*, Autumn 2005. Accessed 20120713. Available online at: http://www.journal.forces.gc.ca/vo6/no3/doc/electron-eng.pdf.

[6] W. Wolf, "EW co-opetition for info ops," *Journal of Electronic Defense*, vol. 34, no. 6, June 2011, p. 12.

[7] W. Wolf, "21st century EM domain capabilities," *Journal of Electronic Defense*, vol. 34, no. 10, October 2011, p. 12.

[8] J. Clifford, “What electronic warriors should know about physics, language and concepts”, *Journal of Electronic Defense*, vol. 34, no. 3, March 2011, pp. 40.

[9] R.J. Elder, “21st Century electronic warfare”, Whitepaper, AOC, 2010.

[10] W. Stallings, Data and computer communications 6th Edition, Prentice Hall, New Jersey, 2000.

[11] D. J. Lonsdale, The nature of war in the Information Age, Kings College London, 2004.

[12] J.D. Vlok, “Control Jamming of WiFi 802.11b”, 5865-ESDE-00001, RPT, CSIR, Nov. 2010.

Social Recruiting: a Next Generation Social Engineering Attack

Adam Schoeman, Barry Irwin, John Richter
Department of Computer Science, Rhodes University, Grahamstown, South Africa
adam@closehelm.com
b.irwin@ru.ac.za
j.richter@ru.ac.za

Abstract: Social engineering attacks initially experienced success due to the general lack of understanding of the attack vector and resultant lack of remedial actions. Due to an increase in mainstream media coverage of this form of attack, corporate bodies have begun to address the need to defend their interests from this vector. This has resulted in a new generation of social engineering attacks that have adapted to the industry response. By focusing on people, not technology, and capitalising on vulnerable security policies in the higher echelons of a company, new forms of attack may be more effective than ever. These new forms of attack take into account the increased likelihood that they will be detected, rendering traditional defences against social engineering attacks moot. As a result, new forms of incident response processes must be proposed to pre-emptively combat this new generation of attack. In this paper I will highlight some of these new attacks and will explain why traditional defences fail to address them. I will then suggest new methods of incident response that can be used to defend against these attacks in the future.

Keywords: Social-engineering, awareness, training

1. Introduction

As the usage of computers and electronic infrastructure has moved from a fringe asset in corporations to an essential part of business profit generating processes [1], the darker side of information technology has grown in step. The increased use of various information technology systems has equated to a decrease in operating expenses and increased productivity, but has also increased the surface area onto which malicious parties can focus attacks. Faced with this, the discipline of information security was born out of a need to protect assets that have not previously been at risk, and has been quite successful in doing so by implementing an ever-expanding tool box of controls. But, as technical controls become stronger, devious minded groups and individuals have turned their attention toward the personnel that use the systems rather than the systems themselves, as there is often a higher probability of success associated with breaching an operator than breaching an operating system [2].

Social engineering, as it has become known, focuses on the human aspect of information security, but due to its deceptive nature it relies on the ignorance of the target to be successful. This has been addressed somewhat through training and general awareness in both mainstream media and focused training, but just as the nefarious elements within information technology shifted their focus to the easier human targets when technical controls proved resilient, the opportunity now exists for that shift to happen once again. This time, social engineers could capitalise on softer targets within the human element, and, given an awareness of the training that the target may have had, the ‘engineer’ could avoid many of the pitfalls associated with traditional social engineering. The following section offers a brief outline of the main differences between the traditional social engineering attack and its newer evolution, the social recruiting attack.

2.1. Social engineering: a low tech hack for a high tech environment

Social engineering is defined as the science of skilfully manoeuvring human beings to take action in some aspect of their lives [3]. Applied more directly to information security, and taking into consideration the actions that penetration testers use when testing the viability of social engineering against their targets, it can be seen as a collection of skills that target the human element of an organisation in an attempt to bypass technical controls. As an example, a classic social engineering attack would consist of the assailant convincing an employee to plug a flash drive into their workstation, which would then run a set of malware, attempting to exploit the workstation and bringing it under the control of the attacker [4]. The social engineering aspect of the attack is the act of convincing the target to insert the infected flash drive, which, under normal technical means, would

require the attacker to somehow bypass inline deep packet inspection [5]. Social engineering allows the attack to instead focus their attack on a person instead of the technical controls, a method which has proven very successful for famous hackers such as Mike Ridpath [6] and Kevin Mitnick [7].

2.2. Combating social engineering: knowledge is power

Social engineering relies on deception and misinformation, with the attack assuming a role that has been tailor made to suit the target and yield the greatest probability of success. But while these traits are essentially the cornerstone of social engineering, they are also its weakness. Security awareness training has been singled out as one of the most important initiatives when combating social engineering because it arms employees with the knowledge of what a typical social engineer will do [8]. Given this raised awareness, employees can more effectively detect a social engineer, limiting or completely negating potential data leaks.

Increased security awareness goes hand-in-hand with a solid, well defined, and easily interpreted security policy [8]. From the security policy a set of 'hard and fast' rules should be derived that can be used by perimeter facing personnel (receptionists, security guards and the like), as they are the most likely to be faced with possible situations that could jeopardise the security of the organisation. Having these two controls in place should allow staff to detect a social engineer and, in the best case scenario, block one from breaching the organisation. Looking at the increase in literature associated with the detection and prevention of social engineering at Defcon DC over the conference's 19 years, as per Figure 1, it's clear that social engineering awareness has enjoyed a drastic increase in later years, particularly from 2008 to 2010 [9]. The industry has targeted social engineering as a high risk area of security and has been trying to solve the problem, as shown by the increased number of research papers presented on the topic. As Allen points out, there is no effective way to fully protect against social engineering attacks [8], but this is true for all technical controls as well (defined as residual risk) [10]. However, with the increase in general awareness of the subject, the human link is not as fragile as it was when social engineering made its debut.

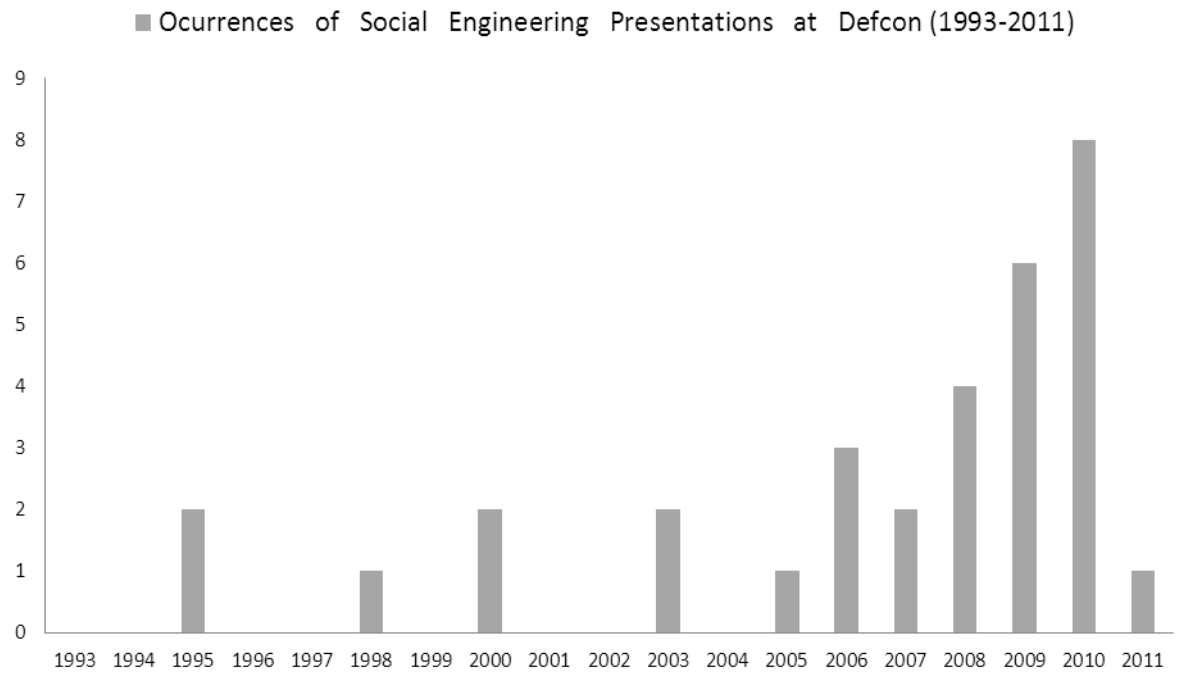

Figure 1: Number of social engineering references in Defcon presentations per year

3. The social recruituing attack: choosing the right target

Where social engineering relies on a distinct lack of widespread detection in order to succeed, social recruiting builds and improves upon the strengths of human hacking. It takes into consideration that detection will occur, and instead of letting its deception based attack collapse under those circumstances, it instead leverages it as part of the attack vector, hijacking the chain of command within a corporation and repurposing it for the attackers needs.

The process starts off as any other targeted social engineering attack, whereby an individual is chosen as a target based on his or her internal privileges and the potential for breaching network assets by taking control of their workstation. Research into the interests or hobbies of this person is paramount to the success of the attack, as it is this that will be used as the bait for a spear phishing campaign [11].

This attack's social engineering roots are quite clearly established in the first phase, which could be described as a traditional social engineering attack (spear phishing), but changes slightly from the next step. In the first case, the social engineer builds a dummy website that looks like a web shop front end: a shop that the target would likely want to visit based on their interests and hobbies. However, in the second (social recruiting) case, the social recruiter would spend more time building the reputation of the website, with special attention being paid to a fictitious Help section. The website would have the illusion of a strong user base to help convince the target of its legitimacy, and would require a prospective new member to install an application in order to utilise the site's functionality. A professional-looking installation guide would then clearly state that certain antivirus programs have been known to conflict with the installation process and would 'helpfully' offer ways to remedy that, usually by asking the user to simply turn them off. As this is the crux of the attack, these steps would need to be clearly visible.

This is what differentiates the social recruiter attack: social engineering relies on tricking a human, whereas social recruiting relies on tricking *and using* one. Knowing that the front-facing low-level employees are increasingly aware of attack vectors, social recruiting instead targets those higher up: it assumes that an upper-tiered executive will have enough influence within the organisation that he or she will be able to have a change made to the technical protections that would leave the company vulnerable to attack. It is assumed that upper managers have this heightened internal privilege and do not understand the potential harm that could come to the organisation by side stepping the security policy [12]. By creating a convincing installation process that tells the user that the antivirus blocking the program is normal, and shifting the nuance of fixing the problem onto the 'client', the target will hopefully instruct the security team to allow access and whitelist the application.

This form of attack overcomes the inadequacy of social engineering by exploiting two common flaws in organisational security policy: a weakening regard and understanding of the security policy amongst higher level employees in a hierarchical organisation [12] [13], and the common managerial assumption that information security is a barrier that prohibits legitimate business transactions [14].

4. Detection nulified: the difficulties of combating social recruiting

If both vulnerabilities exist within a corporation's environment, the social recruiting attack allows the attacker to subvert technical controls to infect a station, and uses the station-owner's managerial privileges to open up the technical controls that would prevent the malware from running. Upon a successful installation, the malware could then disable controls that could block a remote shell or similar malicious application from phoning home.

This creates a sizable problem for information security engineers because they could be faced with a situation where they could know very well that an attack is in progress, but be helpless to utilise their arsenal of technical controls to prevent it. This happens due to the weakened security policy posture as it applies to the targeted higher-tiered employee. An information security engineer that attempts to block the attack could put their job in jeopardy, as it could seem to the managerial target that the employee is not performing and not complying with management's requests.

It also means that most of the normal defences used to detect social engineering attacks are severely diminished because the social recruiting attack does not need to keep itself cloaked from security experts to succeed. By disguising the malware as a legitimate piece of software that is being hampered by the numerous security controls, the social recruiter creates an environment where the attack does not need to be changed based on any technical controls that may be protecting the victim. Therefore the attack does not need to know how the internal security landscape of the victim looks in order to craft this attack.

Social recruiting is also immune to the defensive security mantra of protecting against all known forms of attack (blocking predefined known bad ports, antivirus signatures, IPS signatures and the like) [15] because, even though the security department is aware of the attack, it is often powerless to act against it in an environment where the two human vulnerabilities exist.

5. Out of the box tactics needed to mitigate a social recruiting attack

Since the social recruiting attack exploits two human vulnerabilities in an organisation's security posture, a method that directly mitigates the risk associated with those two vulnerabilities would be best suited. This means that if procedures were in place that prohibited the altering of the security policy by individuals, regardless of their rank or power within the company, the social recruiting attack would be rendered useless.

However, the weakening of the security policy is not due to a lack of process and procedures, but instead is based on special case privileges that are granted through the hierarchical model and a lack of understanding regarding the reasoning behind the security policy. It is therefore impractical to defend against this attack by addressing the security policy head on.

Fortunately, while difficult to prevent, this form of attack's biggest weakness is that it is extremely easy to detect. This may sound paradoxical at first, given that the social recruiter makes the assumption that detection will occur, but for the defender, this ease of detection gives the information security department the opportunity to react to the attack, specifically by decompiling and disproving the authenticity of each piece associated with the overall deception.

For example, the domain name would probably only have been registered recently [16] (unless it was bought by the attacker from a parked domain store, but the resources required for this would normally be too large to justify or require an unrealistic amount of pre-planning), which could contradict statements made by the fake users on the website regarding how long they have been members. Any claims that relate to how long the website has been doing business are also worth investigating as timelines are relatively easy to dispute.

Depending on the amount of time that the attacker has put into the website and the overall back story, a general search for the website might render few or no links to it, which would be a another sign that it is not what it is posing as. If the attacker has gone to the trouble of building a reputable back story for the website (cross posting on other forums and so forth) it is unlikely that the attacker would have been able to correlate the posts with the website's date of establishment. A timeline of cross posts would reveal that a surge of activity appears around a certain date and continues forward, but very little before that, which shows that the posts have been fabricated.

While building a docket that disproves the attacker's platform is essential to countering the overall social recruiting attack, its ability to sway the victim is diminished unless the second vulnerability exploited by the attack has been addressed. Once sufficient evidence has been compiled a case needs to be made to a body within the organisation that, if persuaded that the website is malicious, could reliably convince the managerial target of the same, or simply possess sufficient power to override him or her.

The existence of a third party within an organisation that can be activated to aid the security department in breaking the traditional top-down hierarchical enforcement path is essential in the interim, while a mitigation process is put in place to address the difficult relationship between security and the general management of the organisation. Fixing this relationship defect is not achieved quickly or easily, and therefore it requires a stopgap in the form of the third party body to mitigate social recruiting attacks.

In the medium to longer term, the organisation should focus on instituting some form of social reform with the aim of improving the relationship between the security department and the rest of the company. This is not a focal point for this paper due to the amount of work required, but some areas that can be looked at are:

1 Actively marketing defensive security in the company by highlighting the attacks that have been prevented (possibly aided by showing the theoretical maintenance costs or data loss had those attacks been allowed to pass the control points).
2 Drawing on the incident response team's knowledge in this type of scenario, as they might have internal case studies of breaches that have occurred in the past that match this new attack's fingerprint. There is also value in forwarding the digital forensic education of the security team to management, arming them with the tools to successfully combat the social recruiting attack before it takes place.

6. Conclusion

Security has evolved over the years from simply applying ACLs on perimeter routers, to layering multi technical controls over each other, to a point now where deep packet inspection is required on both the in- and outbound paths of the organisation [5]. But as the technical controls increased in strength, attackers have redirected their efforts towards the easier targets: human operators.

Social engineering has gained momentum because of its ability to bypass many of the technical controls found in a typical corporation's network, but due to tactics based in deception, the infamy of social engineering is often a double edged sword. By exploiting the human element, it is humans who become personally motivated to encourage a greater level of education and response, thereby diminishing the probability of an attack successfully breaching an asset in the future.

While an environment of stronger technical security controls and heightened awareness is not conducive to traditional social engineering attacks, the social recruiting attack thrives in it by combining the most powerful aspects of social engineering with two common human and organisational vulnerabilities often found in companies.

Because of this attack's ability to shatter the technical controls of an organisation via managerial edict, there is no suitable technical platform that can be used to remedy the attack vector. Instead the information security team must employ non-traditional forms of security such as research and information gathering with the purpose of disproving the legitimacy of a seemingly honest website or piece of software.

The remediation strategies for the social recruiting attack are limited, resource intensive and require that the attacker has not covered his or her back story correctly, placing the security team on the back foot. But it also requires a lot of time and precise work from the attacker, who needs to make sure that the timeline of the website makes sense and is plausible, since it is the easiest portion of the attack to investigate.

Coupling this with the assumption that the company has a weakening security policy at the higher echelons (and that a negative attitude towards the security department exists), the possible attack surface and frequency of this attack can be viewed as relatively low compared to those that information security specialists face on a daily basis.

However, we live in a world where it has become worthwhile for a group of hackers to attack a security company, steal secrets from them and then use those secrets to successfully attack a military contractor [17]. That attack took patience, planning and out-the-box thinking, and while it could be classified as an unlikely occurrence on a daily basis, the truth of the matter is that it did happen and could happen again.

As the attack is so dynamic and time sensitive, the security team needs to focus on being able to quickly and efficiently label a social recruiter attack. They can then identify which parts of the deception need to be dissected and disproved, and finally have a predefined process in place to escalate the docket to a pre-formed body with both the technical and managerial power to address these types of attacks.

The steps required to combat social recruiting attacks have their difficulties, but they are not expensive from a capital expenditure point of view nor are they unrealistic, but they do not fall under the traditional armoury of the security specialist. While this might cause the responsibility of the attack

to be passed on to some other department, security personnel that defend a company's assets need to realise that a dynamic mind set needs to be used to combat dynamic attacks.

Unless security professionals realise that the trench-warfare style of defending needs to be abandoned, their prospects of being able to successfully protect their corporation's assets are bleak at best.

Acknowledgements
I would like to acknowledge and extend my gratitude to Haroon Meer for this tireless mentoring and positive encouragement, as well as Gavin Binge for his editing and proofing reading. Without your aid this paper could not have been completed.

References
[1] S. E. Black and L M. Lynch, "How to compete: The impact of workplace practices and information technology on productivity," The review of Economics and statistics, vol. 83, pp. 434–445, 2001. Accessed 20120710. Available online at: http://goo.gl/C2u3X

[2] I. S. Winkler, B. Dealy, "Information security technology?... don't rely on it. A case study in social engineering," in Fifth USENIX UNIX Security Symposium, 1995.

[3] C. Hadnagy, Social engineering: The art of human hacking. Wiley, 2010. Kindle Locations 481-482

[4] C. Hadnagy, Social engineering: The art of human hacking. Wiley, 2010. Kindle Locations 1255-1256

[5] R. Goss, R. Botha, "Traffic flow management in next generation. Service provider networks - are we there yet?" Information Security South Africa (ISSA), pp. 1–6, 2011. Accessed 20120710. Available online at http://goo.gl/OiiDR

[6] M. Ridpath, "Covert calling," in BsidesPDX Track 1, 2011. Accessed 20120710. Available online at: http://www.ustream.tv/recorded/17736407

[7] K. Mitnick, The art of deception: Controlling the human element of security, Wiley, 2003.

[8] M. Allen, "Social engineering: A means to violate a computer system," SANS Institute InfoSec Reading Room, pp. 1–13, 2006. Accessed 20120710. Available online at: http://goo.gl/7Rujh

[9] Defcon Communications Inc. Defon archives. 2012. Accessed on 20120525. Available online at: https://www.defcon.org/html/ links/dc-archives.html

[10] National Institute of Standards and Technology. (2002, July) Risk management guide for information technology systems. Special Publication. NIST. Accessed 20120710. Available online at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[11] A. J. Burstein, "Trade secrecy as an instrument of national security? Rethinking the foundations of economic espionage," Arizona State Law Journal, 2009. Accessed 20120710. Available online at: http://ssrn.com/abstract=1462319

[12] Gabriel Consulting Group, "2011 GCG Data Center security survey," 2011. Available online at: http://goo.gl/AZO2c

[13] InsightExpress, "Cisco research reveals common data loss mistakes," 2008. Accessed 20120710. Available online at: http://newsroom.cisco.com/dlls/2008/prod_093008.html

[14] E. Albrechtsen, "A qualitative study of users' view on information security," Elsevier, 2006, Norwegian University of Science and Technology. Accessed 20120710. Available online at: http://goo.gl/MUZLV

[15] S. Harris, CISSP all-in-one exam guide, Fifth, Ed. McGraw-Hill, 2010.

[16] E. Stalmans, B. Irwin, "A framework for dns based detection and mitigation of malware infections on a network," Information Security South Africa (ISSA), p. 3, 2011. Accessed 20120710. Available online at http://icsa.cs.up.ac.za/issa/2011/Proceedings/Full/44_Paper.pdf.

[17] J. Finkle. (2011, May) Exclusive: Hackers breached U.S. Defense Contractors. Reuters. Accessed 20120517. Available online at http://goo.gl/DIsE7.

Protecting E-mail Anonymity with an Anonymizer Bouncer

Mercia M. Malan, Francois Mouton
Dariel Solutions, Johannesburg, South Africa
CSIR, DPSS, Pretoria, South Africa
malan747@gmail.com
moutonf@gmail.com

Abstract: Communication between people has always been part of society. In the past, paper mail was frequently used for communication with a specific person. Letters were written and placed in an envelope, with the recipient address on the front and a return address on the back, unless the sender's identity was to be kept private. Technology has allowed for communication to develop to electronic mail (e-mail) sent using a computer, which is now used as an accepted way of communication. The problem is that keeping the sender's identity private is often a requirement, and unlike paper mail, it is not as easy to achieve anonymity when sending and receiving e-mails. This paper discusses ways of achieving anonymity when using e-mail as communication in a military environment whilst lodging complaints to the grievance department. Anonymity is defined as hiding the identity and personal information of an individual. Motivation for privacy enhancing technology and the need for anonymity is given, as well as some methods used to try and evade these technologies. The proposed model for this problem uses an anonymous re-mailer to show how the sender of an e-mail's identity can remain private and anonymous, and how the recipient can respond to the sender's e-mail without knowing the identity of the sender.

Keywords: security, e-mail, anonymity, privacy, re-mailer, privacy enhancement technology.

1. Introduction

Communication between people has always been one of the basic human instincts. There are various forms of communication, which can be categorised into two main categories: verbal and non-verbal communication [9]. Components of verbal communication include sounds and words and can be split into two categories: oral communication and written communication [2], [9]. Oral communication is when people talk to each other using their voice. Written communication can vary from paper mail to modern electronic mail (e-mail) [9]. Non-verbal communication is the sending and receiving of wordless messages such as gesture, body language and facial expressions [9].

Another common human characteristic is keeping personal, sensitive information private and secret. Keeping information private and secret can be done by making one's identity anonymous. If the individual's identity is anonymous, the associated, sensitive information cannot be linked to the individual. In the internet milieu it is difficult to maintain privacy and anonymity whilst sending e-mails, whereas paper mail allows one to send mail without a return address [7].

Gülcü and Tsudik [7] explain four main reasons for anonymity under the following subcategories: the discussion of sensitive data, information searches on a person's identity, freedom of speech in an intolerant environment and polling or surveying [7]. There are several other reasons why one would want to stay anonymous, from a secret valentine message to an e-mail containing military protected information. For purposes of this paper, anonymity is defined as the hiding of an individual's identity and personal information whilst using e-mail communication.

Consider an example where a military company is on a field training exercise. A company is defined as a group of soldiers. If a soldier has a grievance during or at the end of the training and wants to lodge a complaint against the training instructor, the complaint has to go through a number of people before the complaint reaches the correct department. The department then needs to respond to the soldier, which goes through another number of people before it reaches the soldier.

The problem is that anonymity of the soldiers is important when dealing with complaints towards a military official, like the training instructor as per previous example. Anyone in the line of people receiving the complaint can go to the training instructor directly and inform him of the complaint and whom it came from, even though this might be unethical and of poor standard of the individual. This

can reflect badly on the soldier as the training instructor can act negatively towards him. If the soldier can send an anonymous message to the correct department directly, and the department can respond without knowing who the sender is, it would cancel out the previously mentioned problem.
This paper initially investigates current available privacy enhancing techniques and ways to achieve privacy and anonymity. This research is then used to construct a model as a possible solution to the problem of achieving anonymity whilst using e-mail as a communication method.

The authors propose a model, the anonymizer bouncer model, which implements a basic "middle-man" principle. The model uses a "middle-man" anonymizer bouncer which manages all e-mails sent from a point A, the military soldier lodging a complaint, to a point B, the military grievance department, as explained in the previous example. The goal is for the soldier at point A to keep his/her identity hidden, thus to stay anonymous. The soldier at point A sends an e-mail to the anonymizer, which processes the relevant information and forwards the e-mail to the department at point B. The department at point B can then respond to the soldier at point A through the anonymizer, without knowing who the original sender was. It is the task of the anonymizer to process the relevant information, and forward the response from point B back to the soldier at point A. Figure 1 shows a basic overview of the model.

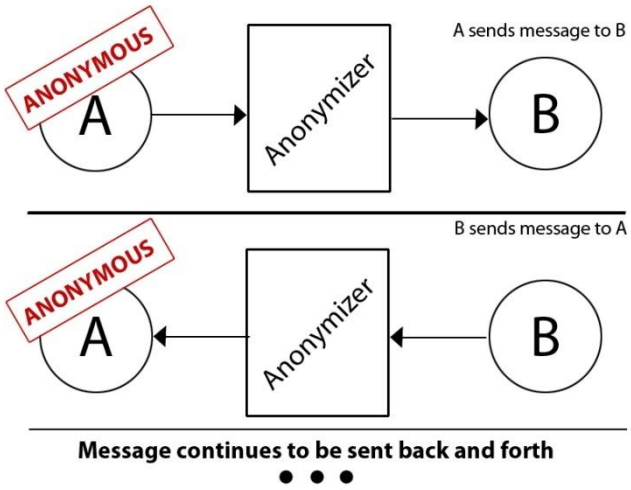

Figure 1: Basic overview of the anonymizer bouncer model

Furthermore, this paper describes the model using a call centre environment as it provides a simplistic way of explaining the model. The paper focuses on a scenario where the sender is an agent working in a call centre environment and the client is an individual requesting a task from the agent. When the client phones the call centre, the agent answers the phone and the client requests a task from the agent. In order for the agent to process the task, he/she requires documents from the client. In order for the agent to receive the documents, the agent sends an anonymised e-mail to the client. The client sends a response e-mail containing the required documents back to the agent.

The remainder of this paper is structured as follows. Section 2 discusses ways to achieve privacy and anonymity on the internet. This section also introduces the reader to passive attacks, which are ways to try and prevent anonymity, and previous work in the field of anonymity. Section 3 proposes the anonymizer bouncer model as a solution to the problem. This section is subdivided into four subsections. The first subsection provides an overview of the system. The second and third subsections explain the communication between the agent and the client and between the client and the agent, respectively. The last subsection discusses the advantages and disadvantages of the model. Section 4 concludes the paper with the advantages that this model brings to a call centre environment as well as future work.

2. Privacy and anonymity on the internet

This section is discussed in three subsections. Section 2.1 discusses privacy and anonymity and how they are linked. Section 2.2 lists and briefly explains three different passive attacks used against

anonymous re-mailers. The last section, section 2.3, discusses previous work in the field of anonymity.

2.1 Privacy and anonymity

Anonymity can be defined as the privacy of one's identity and can be divided into two cases: persistent anonymity where one uses a pseudonym instead of one's real name, and one-time anonymity where an online identity is created that only lasts for one session [4]. Paper mail allows for anonymity because adding a return address is not a necessity [7]. Modern day electronic mailing, however, is not that simple and many approaches have been followed to solve this problem [7].

A way to achieve privacy of an e-mail is to encrypt the message before sending it. Pretty Good Privacy, or PGP, is encryption software that can be used to encrypt the message in such a way that one can send it to multiple recipients [12]. The message is encrypted with a public session key and then this key and the public key of each recipient is encrypted and sent with the mail in a block [10]. The recipient then uses his / her private key to decrypt the session key and then decrypts the message [10].

Onion routing is another way of achieving anonymity. Onion routing is an infrastructure that allows for private communication over a public network [6]. The basic idea is that "onion" data, which is data layered into different encryptions, is sent through the onion route and each node decrypts one layer of the "onion" until the data is in clear text [6], [7].

The onion routing system that is currently being used is called Tor [11]. Tor is an anonymity tool where the client Tor application selects nodes from the Tor server [11]. The data to be sent is encrypted and sent through randomly chosen Tor nodes [11]. The last node then decrypts the message and sends it to the final recipient [11].

Achieving complete anonymity on the internet is an even more difficult task to accomplish, but there are systems available that partially accomplishes this. One of these systems is called the 'Anonymizer' which is an anonymity service keeping your entire system anonymous from the internet [1]. The Anonymizer masks the individual's IP address and assigns an alias IP to the system which is sent out to the public network. The following subsection discusses the different types of passive attacks and gives a brief description of how each attack works.

2.2 Passive attacks

There are three main ways to try and retrieve the private, anonymous information. These are called passive attacks, because these attacks occur by monitoring network traffic [7]. Passive attacks on re-mailer systems occur by monitoring e-mail communication between the sender, A, and the receiver B. The attacker first monitors the message before A sends it to B. The attacker then analyses the message after B received it. The differences between these two messages can either be monitored by the content of the message or by the time of sending and receiving the message. Assumptions are then made from the monitored differences.

The first type of attack is a Content (or size) correlation attack which takes the content and the length of the e-mail into account [5]. If the attacker can compare the content of the e-mail from the receiver's side as well as the sender's side, it can be assumed that it is the same e-mail. Assumptions can then be made and one can see who the sender and receiver are, which reveals the anonymous user's identity. The other method of content correlation attacking is the analysis of the size of the message before sending and after receiving the e-mail. If the size is more or less the same, the messages are assumed to be the same.

The second type of attack is a Time correlation attack which takes the time of sending and receiving the e-mail into account [5]. This is done by comparing when the e-mail was sent and received and then drawing conclusions of which e-mails was sent closest to each other and seems linked. The anonymous identities are revealed since the sender as well as the receiver is now known.

The third type of attack is called Message Replay which records and plays e-mail messages back. A legit message is recorded and then played back later in the message stream [7]. The same output

that was given for the original message is again given for the fake message, if the system does not account for message replay. Similarities and differences can then be drawn by comparing the first message and the second message in terms of content and times sent and received.

The following subsection discusses previous work which has been done in the field of anonymity.

2.3 Previous work

The first, most authoritative paper about anonymity and anonymous communication was published by D. Chaum in 1981 [3], [7]. Chaum produces an idea called a “mix” as a solution to obtain anonymity. This “mix” is based on a more primitive way of sending mail, which includes sending the mail to a friend who strips out all the identifying factors of the mail and then forwarding it to the right person [4]. The “mix” is basically a component acting as a re-mailer which forwards e-mails from the anonymous user to the proper recipient. The goal of the “mix” is to obfuscate the relationship between incoming and outgoing mail before forwarding the message to the recipient, so that the recipient is not able to identify the sender [7].

Most other anonymity systems are based on Chaum’s original idea. The IBM Zurich Research Laboratory wrote an anonymous re-mailer, called Babel. Babel is an e-mail filter, which filters out the identifying parts of the e-mail before forwarding it to recipient [7]. Babel caters for the different attacks and focuses on more detail than just stripping the mail of the identifying factors [7].

Anonymous re-mailers are classified according to four types [4], [5], [7]. The types are as follows.

1. Type 0 re-mailer, called the *Penet* re-mailer, is the oldest and currently still most used re-mailer [7]. The Penet re-mailer strips the mail of all header information, creates an alias for the sender, and then forwards the mail to the recipient. The recipient can then reply to this alias, which is connected to the real person [4], [5], [7].
2. The type 1 re-mailer was created by a group called the *cypherpunks* [8]. There are many different versions of this type of re-mailer and all are based on the type 0 re-mailer with slight variations [7]. This re-mailer addresses the issue of time correlation attacks by adding extra security features including message chaining, encryption and mixing [5]. Mixing is a method of batching up messages and then sending a whole batch out in a random order, instead of sending out one message at a time [5].
3. The type 2 re-mailer is called the *mixmaster* and its main focus is improving on the size correlation issue. This is done by sending out the mail in packets of the same size. The mixmaster does not assign a pseudonym (alias) to the sender [5].
4. The type 3 re-mailer is called the *mixminion* and is basically a type 2 re-mailer, but creates an alias for the sender as with type 0 and 1 [5].

The following section discusses the details of how the model proposed by the authors, called the anonymizer bouncer model, works.

3. The anonymizer bouncer model

The previous sections explained the different types of re-mailers that are available. Most of the re-mailers make provision for handling multiple recipients, and in the call centre scenario and military example, there will always be only one intended recipient: the client or the grievance department. The authors suggest a simple anonymous re-mailer model which handles incoming and outgoing e-mail in the call centre. The goal of the re-mailer is to hide the identity of the agent to the client, but still provides the client the ability to reply to the agent. A Gmail account was created to act as the anonymizer bouncer, with the e-mail address anonymizerbouncer@gmail.com.

The authors combine the techniques of Chaum and the original penet re-mailer into a simplistic re-mailer [3], [7]. This re-mailer improves on other techniques because it does not make use of pseudonyms and is completely separate from the person sending the e-mails. The re-mailer also has less complexity than ordinary chain re-mailers. Pseudonyms can be unravelled to reveal the original sender. As the anonymizer bouncer is separate from the person sending the e-mails, there is no way of tracing the e-mail back to the sender by using the passive attacks mentioned earlier. The other available re-mailers try to account for these attacks by sending the e-mails at random times and

keeping the sizes of the e-mails consistent, whereas with the anonymizer bouncer none of these extra complications are required.

This section is subdivided into four sub sections. The first subsection provides an overview of the system. The second and third subsections explain the communication between the agent and the client and between the client and the agent respectively. The last subsection discusses the advantages and disadvantages of the model.

3.1 Overview of the model

Figure 2 shows an overview of the model. The anonymizer in the image is the anonymizer bouncer.

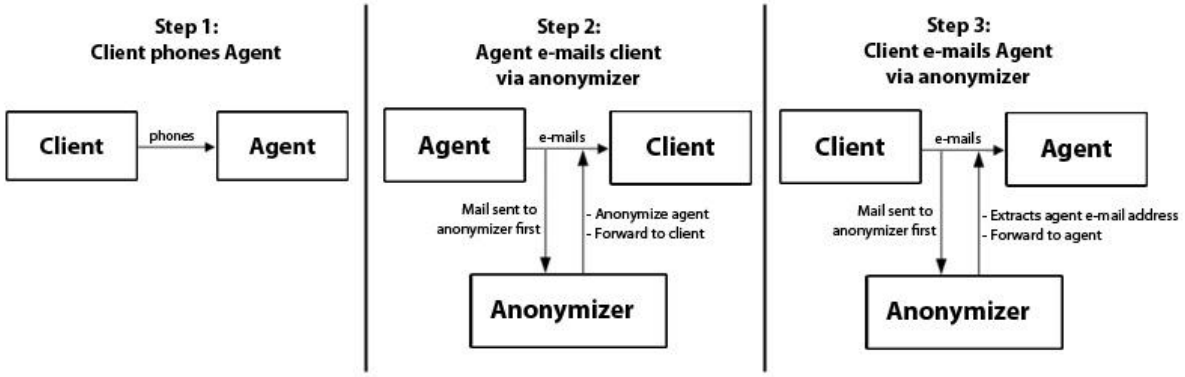

Figure 2: Overview of anonymizer bouncer model

The client phones the call centre and speaks to a specific agent. The agent then informs the client that there is a need for the agent to e-mail the client, for example there is a need for extra documentation. The client provides his/her e-mail address to the agent and the agent then e-mails the client requesting the additional documentation. The goal of the anonymizer is to be the middle man between the agent and the client, making the agent's identity obfuscated to the client.

The agent's e-mail is sent to the anonymizer, with parameters to specify where the e-mail should be forwarded to. The anonymizer processes the headers of the e-mail to retrieve all necessary information, encrypts the agent's e-mail address and forwards the e-mail to the client. The anonymizer also configures the e-mail in such a way that the return address would return to the anonymizer with the encrypted e-mail address as parameters. This is done so that when the client replies to the "agent", the anonymizer will know which agent to forward the reply to.

In the case where the client replies, the anonymizer retrieves the e-mail and extracts the header of the message. The anonymizer decrypts the agent's e-mail address and then forwards it to the agent, with the client's e-mail address as parameters.

The following subsection explains the e-mail communication originating from the agent to the client.

3.2 Agent to client

Figure 3 depicts the process that occurs when an agent communicates to the client.

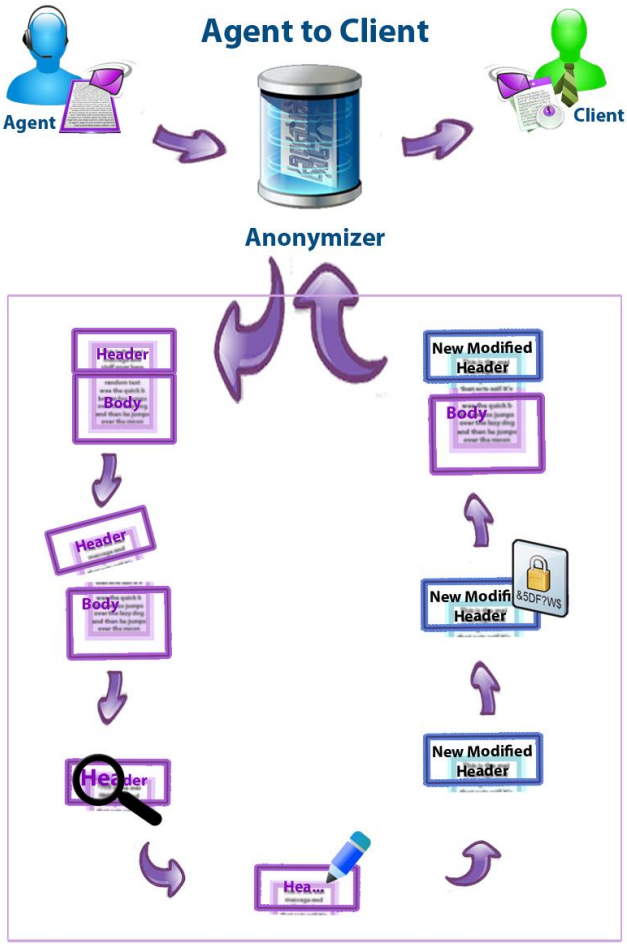

Figure 3: Agent to Client communication

The first step of the process is the agent from the call centre sending an e-mail to the anonymizer. The agent adds the client's e-mail address to the subject field in a specified format, and then the message to send to the client in the body as per a normal e-mail. Figure 4 shows the structure of the message sent from the agent to the anonymizer.

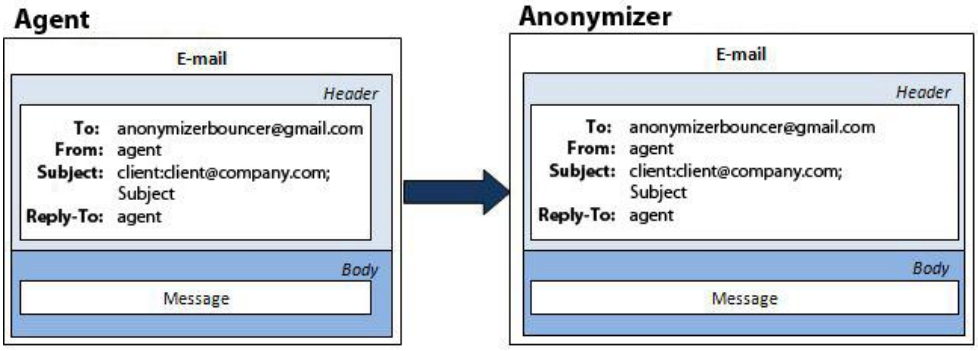

Figure 4: Message structure in communication from agent to anonymizer

The anonymizer analyses the header of the message and extracts relevant information from it. The subject field contains the client's e-mail address as well as the actual subject. The anonymizer also saves the "To" and "From" field of the original message, as this is used in the next step. Figure 5 shows the information stripped from the header, to replace in the anonymizer's header in the next step.

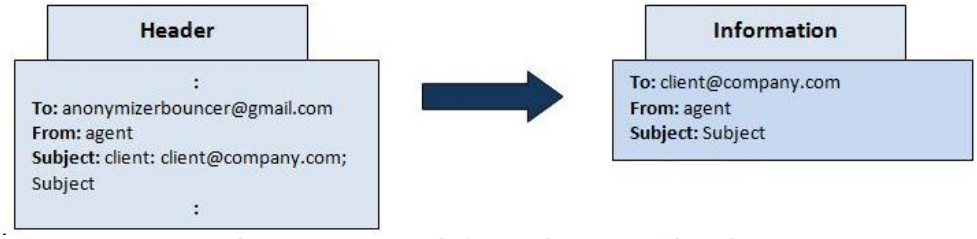

Figure 5: Extract information out of header

The next step is to strip the original message of its header and replacing it with the modified template header of the anonymizer. The anonymizer extracts relevant fields, as depicted in Figure 6, from the original message's header and replaces it in the template header. The relevant fields that are replaced are as follows. The "To" field gets replaced with the client's e-mail address contained in the subject. The "From" field is the anonymizer's e-mail address. The "Subject" field is replaced with only the subject out of the original message as the client's e-mail address is removed from the subject. The agent's e-mail address is encrypted and concatenated to the anonymizer's e-mail address to form the Reply-To field. The Reply-To field is in the format 'anonymizerbouncer+agentEncrypted@gmail.com'. The gmail server disregards any text after the plus sign in a gmail address and the e-mail is sent to anonymizerbouncer@gmail.com. The "To" field will still contain the entire formatted address, with the plus sign and text after the plus sign included.

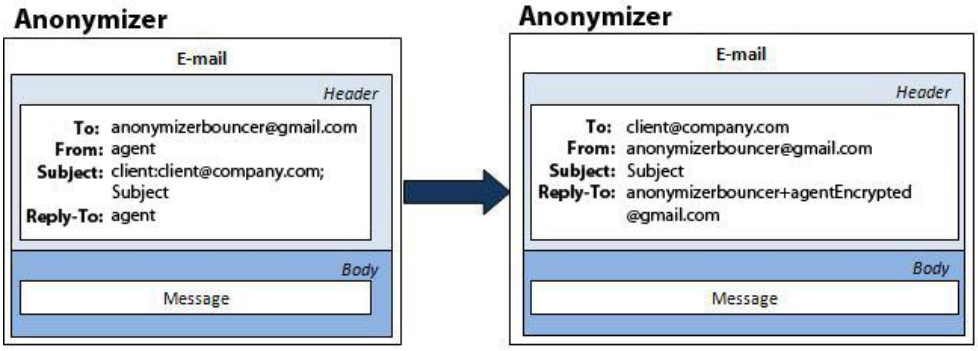

Figure 6: Construct new message

This e-mail is then sent to the client, who can now reply to the call centre agent without knowing the agent's identity as depicted in Figure 7.

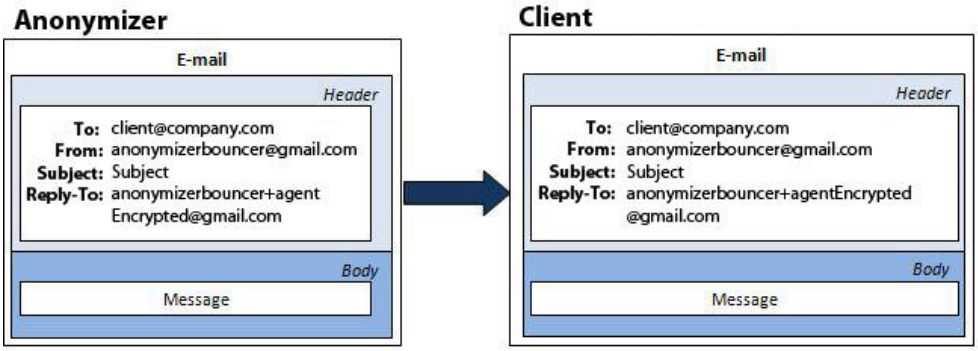

Figure 7: Anonymizer forwards e-mail to client

The following subsection explains the e-mail communication originating from the client to the agent.

3.3 Client to Agent

Figure 8 depicts the process that occurs when the client responds to the agent.

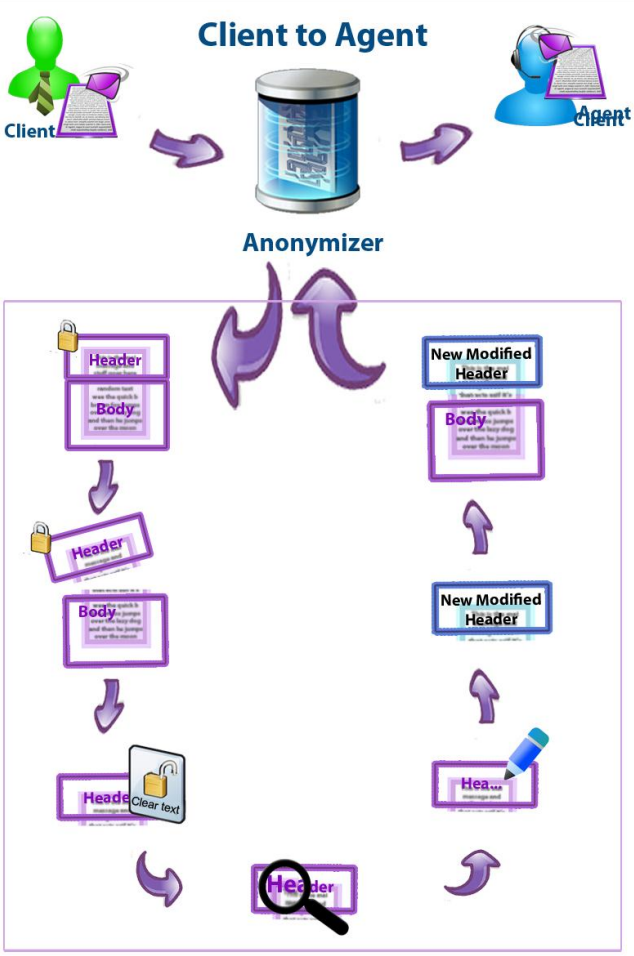

Figure 8: Client to agent communication

The client replies to the e-mail sent from the call centre agent. Since the "Reply-To" field has been populated as the anonymizer bouncer's e-mail address, the anonymizer receives the e-mail from the client. Figure 9 shows the message format sent from the client to the anonymizer.

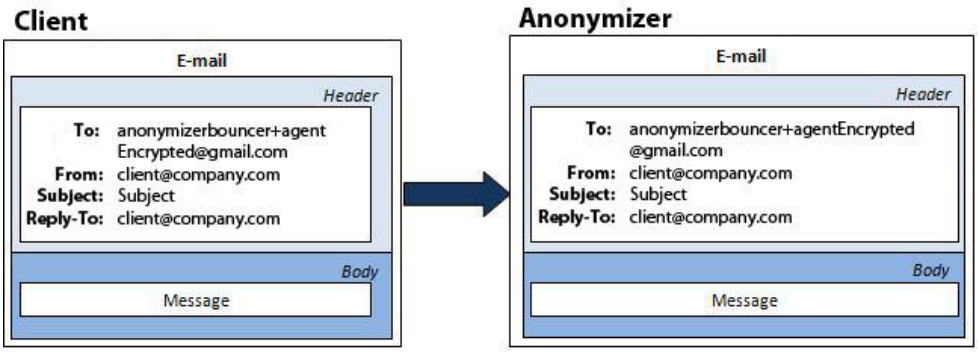

Figure 9: Message structure in communication from client to anonymizer

The anonymizer extracts the header from the e-mail and retrieves the relevant information from the e-mail, as shown in Figure 10. The "To" field contains the agent's encrypted e-mail address. The "From" field contains the client's e-mail address, and lastly, the "Subject" field contains the subject of the e-mail.

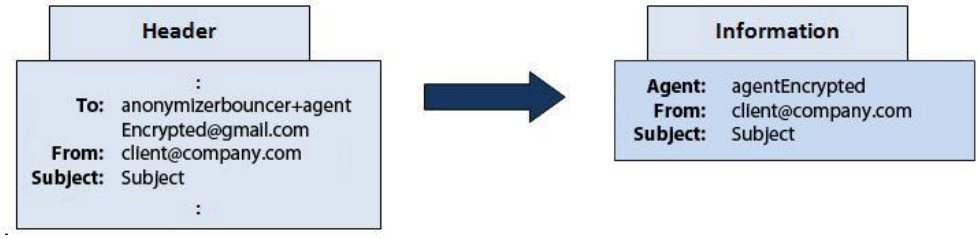

Figure 10: Extract information out of header

The next step is retrieving the agent's e-mail address and constructing the new message. This requires the anonymizer to decrypt the agent's encrypted e-mail address. The original message is completely stripped of its header and replaced with the anonymizer's header. The relevant information from the original header replaces the associated fields in the anonymizer's template header. The "To" field gets replaced with the decrypted agent's e-mail address. The "From" and "Reply-To" fields gets replaced with the anonymizer's e-mail address. The client's e-mail address is joined with the subject in the form "client:client e-mail; subject" and set as the "Subject" field. Figure 11 shows the original and modified messages.

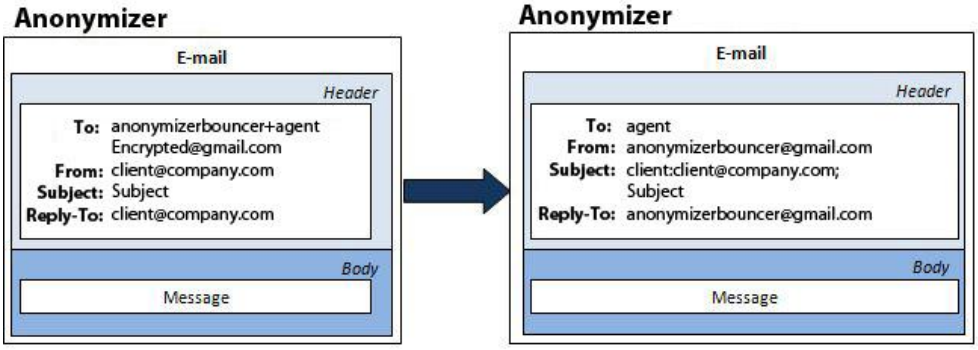

Figure 11: Construct new message

The final step of the anonymizer is to forward the message to the agent. The agent can reply to the anonymizer with the client's e-mail address as parameters as explained in section 3.2. Figure 12 depicts the final step.

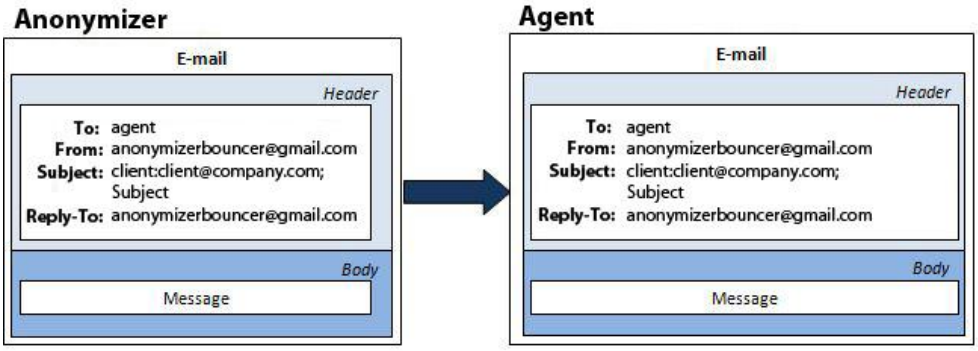

Figure 12: Anonymizer forwards e-mail to agent

The following subsection explains the advantages and the disadvantages of the proposed model.

3.4 Advantages and Disadvantages of the anonymizer bouncer model

The advantage of having an anonymous re-mailer in a call centre environment is that the agent can do his/her job safely, without having to worry about angry callers (clients) who might want to use the agent's e-mail address for malicious reasons. These reasons can vary from hacking the agent's computer, to extreme cases as doing information searches on the agent and stalking the agent. Angry

callers may be upset with the call centre and not with the agent specifically and may take it out on the agent.

Another advantage is that there is no favouritism involved when callers rate the call centre agent. If the caller knows the agent's identity, he/she might rate the agent unfairly if he/she has any previous experience with the agent.

In a military environment, the advantage of having an anonymous re-mailer is that the soldier can send a complaint to the grievance department without having to worry about anyone knowing that he lodged the complaint. If the soldier lodged a complaint against a military official in a higher rank than himself and the military official finds out about it, the military official might act negatively towards the soldier. This is very important in a military situation, as officials acting negatively towards the soldier can result in physical punishment or emotionally breaking down the soldier.

The anonymizer can also help prevent some of the passive attacks. Since the e-mails are sent from within the call centre, through the anonymizer, the only assumption that can be made is which message was sent by the client and received by the anonymizer. Thus, analysing the time of the message and size of the message cannot be accomplished as the attacker has no access to the data from the call centre to the anonymizer server. In the case of the message replay attack, the only problem that is foreseen is that the anonymizer can send duplicated e-mails to the agent. The identity of the agent will thus remain anonymous no matter which of the three mentioned attacks are used against the anonymizer bouncer.

The main disadvantage of the re-mailer is that the communication may take a bit longer. This is due to the fact that the agent has to configure the subject of the e-mail in a very specific way so that the anonymizer can process the e-mail correctly.

4. Conclusion

Communication is an important part of everyday life amongst human beings. People are also very secretive about private, sensitive information and sometimes want to keep this information secret and hidden. By making one's identity anonymous, one removes the value from sensitive information and can thus keep it secret. Keeping anonymity is not always an easy task and it is even more difficult to obtain anonymity on the internet.

In a military environment, sending e-mails to the grievance department, the sender sometimes needs to stay anonymous. The problem is that anonymity of the soldiers is important when dealing with complaints towards someone else in the military. The purpose of this paper was to find a simplistic solution, without causing extensive extra network overhead, in order to achieve anonymity within a military environment.

It has been shown that there are various privacy enhancement techniques available and research has been performed on different techniques of anonymity, but none of these apply directly to a military environment. Most of the techniques require extensive extra network overhead without providing much more benefits. The anonymizer bouncer re-mailer model, as proposed by the authors, is based on one of the first anonymous re-mailer concepts. This is performed by stripping the e-mail of its header and replacing it with a header created by the re-mailer. Encryption is used to make the agent's e-mail address anonymous so that the client cannot identify the agent. The type of encryption is interchangeable and this model does not constrain itself to a specific encryption algorithm.

The anonymizer bouncer re-mailer model improves the military environment, as the soldiers doing field exercise training can feel safe when lodging a complaint against a military official in a higher rank. By keeping the soldier's identity anonymous, the military officials cannot threaten the soldier in any way, whether by physical punishment or by breaking the soldier down emotionally.

In future research one can examine the effects it might have if one writes a customised client e-mail application which automatically formats the relevant parts of the e-mail so that the anonymous re-mailer can process it correctly. Further security enhancements can also be implemented to better prevent the spam effect of the message replay attack. In the military environment the soldier's identity

would need to be authenticated before the mail reaches the recipient, so that a non-military person cannot send false complaints. As this paper focuses on the anonymity of the sender, the current model does not cater for this type of authentication and needs to be investigated in future work.

References

[1] Anonymizer, "Anonymizer", Anonymizer, Inc. 2012. Accessed 20120505. Available online at http://www.anonymizer.com.

[2] College Of Business, "Verbal communication", University of Louisville, ND. Accessed 20120509, Available online at: http://cobweb2.louisville.edu/faculty/regbruce/bruce/mgmtwebs/commun_f98/verbal.htm.

[3] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[4] I. Goldberg, D. Wagner, and E. Brewer, "Privacy-enhancing technologies for the internet," in Compcon '97. Proceedings, IEEE, pp. 103 –109, 1997.

[5] I. Goldberg, "Privacy-enhancing technologies for the internet iii: Ten years later," in Digital Privacy: Theory, Technologies, and Practices, pp. 1 – 14, 2007.

[6] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing," *Communications of the ACM*, vol. 42, no. 2, pp. 39–41, 1999.

[7] C. Gulcu and G. Tsudik, "Mixing e-mail with babel," in Network and Distributed System Security, pp. 2 –16, 1996.

[8] E. Hughes, "The electronic privacy papers". A cypherpunk's manifesto, John Wiley & Sons, Inc, pp. 285–287, 1997.

[9] Your academic Encyclopedia, "Types of Communication", Notes Desk, 8 March 2009. Accessed 20120509, Available online at http://notesdesk.com/notes/business-communications/types-of-communication/.

[10] I. William F. Price, "Method and apparatus for facilitating secure anonymous email recipients," Patent US 6 851 049 B1, 02 01, 2005, Accessed 20120519, Available online at http://www.google.com/patents/US6851049.

[11] Tor, "Tor: overview", The Tor Project, Inc, ND. Accessed 20120508 Available online at https://www.torproject.org/about/overview.html.en.

[12] P.R. Zimmermann, The Official PGP User's Guide. MIT Press, 1995.

Towards a Cyberterrorism Life-Cycle (CLC) Model

N Veerasamy [1, 2], M Grobler [1, 2] S von Solms [2]
[1] CSIR, [2] University of Johannesburg, Pretoria, South Africa
nveerasamy@csir.co.za
mgrobler1@csir.co.za
basievs@uj.ac.za

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.

Keywords: cybercrime, cyberterrorism, life-cycle

1. Introduction

Terrorism brings with it a wave of potential devastation and uncertainty. Terrorism has thus entered a new arena in that Information and Communication Technology (ICT) has become both a prime target and weapon to perpetrate and cause onslaughts on innocent victims and high-profile points of interest.

The most cited definition for cyberterrorism comes from Denning which was given before the Special Oversight Panel. It 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” [15].

Desouza and Hensgen define cyberterrorism as “A purposeful act, personally or politically motivated, that is intended to disrupt or destroy the stability of organizational or national interests, through the use of electronic devices which are directed at information systems, computer programs, or other electronic means of communications, transfer, and storage” [8]. Overall cyberterrorism can be seen as the threat or act of causing harm in order to create fear and shock, targeting critical ICT infrastructures based on political, religious or social reasoning.

Janszewski and Colarik have stated that “The emergence of cyberterrorism means that a new group of potential attackers on computer and telecommunication technologies may be added to 'traditional' criminals" [17]. In some cases, when a cyberattack is carried out it is often labeled as cyberterrorism. However, all cybercrimes are not cyberterrorism acts. Cyberterrorists and cybercriminals may use the same underlying security and hacking skills to break into systems but the underlying motivation, objective and effects may differ. Lachow [20] has explained that whilst cyberterror tries to cause a political change and targets innocent victims through computer-based violence or destruction, cybercriminal activities aim to have an economic gain from individuals and companies by carrying out fraud, identity theft, blackmail, and other computer attacks and exploits. In order for a cyberattack to be considered cyberterrorism it should have a terrorist motivation like threatening, disturbing or destroying critical infrastructure based on a political, social or religious background. Terrorists would try to cause fear or the enforcement of demands and not just cause annoyance, carry out fraud or economic espionage.

In addition, terrorists may use very specific practices in order to create a disastrous effect. For example, after the Estonian government chose to move the war memorial in Tallinn honoring Russian-Estonians, the critical government websites were hit by a multitude of requests which caused the systems to fail [28][37]. Due to the large number of requests, the attacks were probably distributed, automated and carried out using a botnet. Furthermore, the conflict between Indian and Pakistan resulted in five megabytes of sensitive nuclear data at the Bahaba Atomic Research Centre being downloaded by unauthorized parties [9], [26], [27], [31]. From events categorized as cyberterrorism, it can be surmised that cyberterrorism would usually take the form of virus, bot or privilege escalation attacks to specifically infiltrate high-profile targets in order to achieve a maximum effect.

Various factors influence the development of a cyberterrorist. These include social factors, practices, objectives, targets, effects and motivation. In some cases, these factors are behaviourally based and in other cases technically based. The following questions therefore arise: How does one encapsulate the development of a cyberterrorist? How can cyberterrorism be deterred? This paper proposes the development of a Cyberterrorism Life-Cycle (CLC) model in order to address the raised questions. The next section looks at the motivation for modelling.

2. Motivation for Modelling

Epstein describes various reasons for modelling. Some of these reasons include [10]:

- Explain
- 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 helps in portraying a concise representation of a field that may have various complex components.

According to Eriksson and Penker, a model is a simplified view of a complex reality and provides a means of creating abstraction that allows one to eliminate irrelevant details and to focus on one or more important aspect at a time [11]. For this reason, as a means of portraying some of the most critical aspects of cyberterrorism, this paper proposes the CLC model. The next section presents the generic CLC model, based on the findings found in literature.

3. Overview Of Cyberterrorism Life-Cycle (ClC) Model

In order to develop a helpful model, it is important to include a number of far-ranging factors 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 factors are related in order to identify the best approaches of combating attacks. Literature was used as background to identify the core factors during the phases.

Figure 1 shows the proposed generic CLC model. It is composed of four main phases: Prepare, Acquaint, Choose, Execute, as well as specific countermeasures in the supplementary Deter phase. These phases are loosely based on steps in the Observe-Orient, Decide, Act (OODA) loop proposed by Col John Boyd [1].

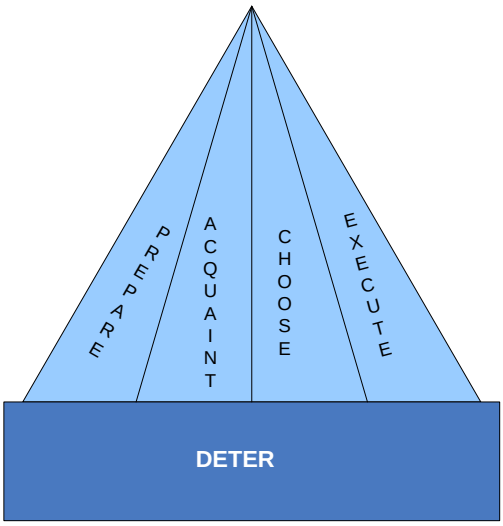

Figure 1: High-level CLC model

To illustrate, a cyberterrorist would identify the affordability and advantages of ICT during the preparation phase, then acquaint himself with the online presence of the targeted organization during the acquaintance phase. Thereafter during the choose phase he would make a selection of targets based on planned effects. During the execute phase, certain practices would be employed. The model can thus be further expanded based on other factors which play an influential role. This is carried out in the next section.

4. **Expansion of CLC Model**

Figure 2 shows an expansion of the CLC model, with the four main phases shown in the innermost circle. The Deter phase appears on an outer edge as the encompassing countermeasures are applicable across all four main phases. The expanded CLC Model is based on a mapping of cyberterrorism to the OODA loop, shown in Figure 3 [33].

The original OODA loop phases (see Figure 3) are adapted to the PACED phases, Prepare, Acquaint, Choose and Execute (see Figure 2). The Deter phase is also added and consists of countermeasures specific to cyberterrorism. Within each of the four main phases factors are displayed that applies to that specific phase. These factors are labeled A-H in Figure 2, 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 phases (indicated by the overarching outer circle of Figure 2). However a social factor like upbringing is influential in the initial phases of prepare and acquaint (indicated by the A in the innermost circle). Thus, social factors are represented as a ring covering all phases, as well as a specific factor overlapping during the Prepare and Acquaint phases (in Figure 2).

Some of the factors captured in the model were slightly adapted from the original OODA loop mapping. For example, Malicious Goals and Support Functions (in Figure 3) have been encapsulated into a single factor entitled Objectives (E) in the CLC model (in Figure 2). Similarly Attack levels and Modes of Operation (in Figure 3) have been removed and Effects (G) has been added (in Figure 2). These changes are based on the analysis from an ontological study by Veerasamy Grobler and Von Solms [34], [36] 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 [36] and were thus included in the CLC model.

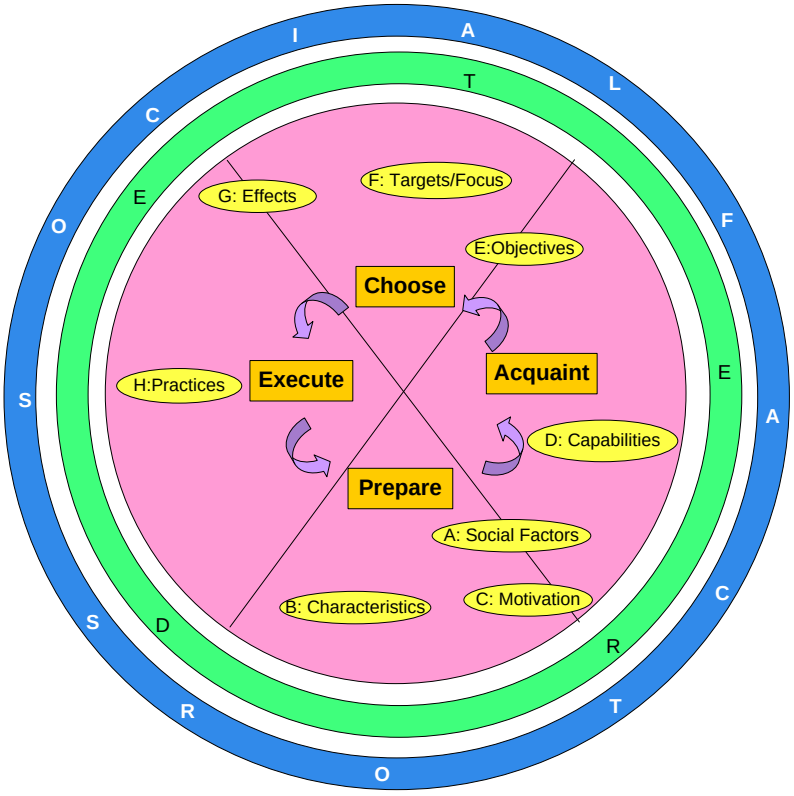

Figure 2: Expansion of CLC Model

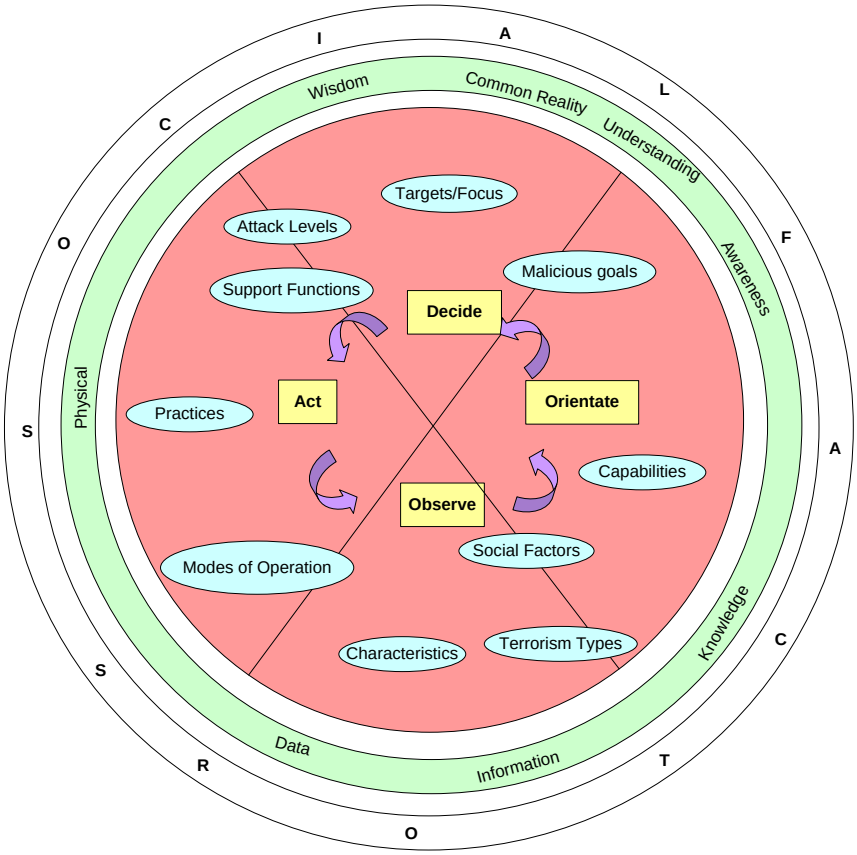

Figure 3: Mapping of Cyberterrrorism to OODA loop [33]

5. Development of CLC Model

The CLC model was derived based on the identification of critical points from literature and various existing models. The critical points were identified from findings taken from a framework summarizing the core aspects of cyberterrorism [32], a study of terrorists' use of terrorism [34], an ontological compilation to identify the core aspects relevant to the field of cyberterrorism [36] as well as an investigation of countermeasures [35]. These critical points are matched against identified factors in the CLC model to which the main contribution is made (labelled A-H in Figure 2). This section describes these various points.

5.1 Social Factors

- Various social factors can influence the development of a cyberterrorist. These include: culture, beliefs, political views, upbringing and personality traits [32], [18]. These social factors are a significant influential force in the CLC model during the Prepare and Acquaint phases.
- Social factors are an influential factor throughout the life-cycle of a cyberterrorism [33]. This critical concept will be reflected in the CLC model.

5.2 Characteristics

- 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 [32], [7], [39], [29].
- During the initial OODA loop's Observation phase, the important influential factors are the characteristics of ICT that make it a viable target or weapon, together with initial motivations forces that stems from the classification of terrorism types [33]. This idea will be represented in the CLC model during the Prepare Phase.

5.3 Motivation

- The differentiation between cybercrime and cyber-terrorism is an important aspect that is often confused. For a cybercrime or attack to be considered as cyberterrorism, there needs to be elements of terror through threats, disturbances or the infliction of violence [32]. The CLC model will take into consideration an ordinary cybercrime and those that take the form of cyberterrorism.
- Cyberterrorism is mainly motivated by political, social or religions reasons. The CLC model will incorporate the different motivating reasons [15], [8], [25].
- In a framework summarising cyberterrorism, [32] an explanation is given on the different types of terrorism based on motivations. These include: Religious, New-Age, Ethno-National Separist, Revolutionary Thinking and Far-Right Extremism. The different motivations will be captured in the CLC model [39].
- Motivation is a key aspect in separating traditional cybercrimes from cyberterrorism. The ontology shows motivations that correspond to cybercrime in general (criminal, ethical, financial, military and recreational) [30] and those that relate to cyberterrorism (political, social and religious) [15]. The CLC model will specifically capture the motivations relating to cyberterrorism.

5.4 Capabilities

- 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: education, training, skills, expertise, financial support, resources, intelligence and insider knowledge. These capabilities will be reflected in the CLC model [32].
- 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 [33]. This will be shown during the CLC model's Acquaint Phase.
- An actor is needed to initiate and execute an action [36]. The following types of actors were identified: commercial competitor, hacker, insiders, criminal and protestor [30]. 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.

5.5 Objectives

- 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 and will be covered in the CLC model [32].
- Some of the support functions that can be carried out include training, recruitment, networking and funding. The support functions will be covered in greater detail in the CLC model [32], [6].
- The driving forces behind cyberterror stems from different objectives. Cybercrime can be related to causing annoyance, economic loss, fraud and espionage whereas cyberterrorism is linked to causing fear [32]. The CLC model will cover the different objectives behind cyberterrorism that will demonstrate its distinction from cybercrime in general.
- Cyberterrorism differs from cybercrime due to its distinct malicious goals. These include goals like: protest, disrupt, kill or maim, terrify, intimidate, demands, access sensitive information, affect crucial services, publicity and soliciting money [32], [39], [13]. The CLC model will describe the specific malicious goals that differentiate cyberterrorism from other forms of cybercrime.
- ICT can also play a support role to cyberterrorism. The supporting functions that ICT can play include: recruitment, training, intelligence, reconnaissance, planning, logistics, finance, propaganda and social services [32], [18], [29]. The CLC model will show how ICT can also be used as a support function.
- Due to the unique nature of the Internet, many traditional and innovative Internet activities can be carried out in either a uni-directional or bi-directional fashion, depending on the nature of the communication required [34]. The traditional and innovative uses of the Internet will be represented as malicious objectives and support functions in the CLC model respectively.
- These support functions include all the processes from recruitment and training of new members, communicating with existing members, planning and executing operations, distributing propaganda, fund raising and carrying out psychological warfare [34]. These support functions will be captured in the CLC model.
- During the OODA loop's Decision phase, the malicious goals or support function features with the target [33]. This will contribute to the development of the CLC model to show the formulation of objectives and targets which will be represented in the Choose Phase.

5.6 Targets

- Targets of cyberterrorist attacks include governmental and critical systems [37], [32]. The CLC model will include the identification of prime targets of attack and facilitation.
- Cyberterrorism attacks will most likely be carried out against high-profile targets in order to maximize the damage and coverage of the attack. Typical targets include the following industries and areas: transportation, utilities, finance, communication, emergency, public health and agriculture [8], [32], [4], [12]. The CLC model will cover the different types of targets.
- The types of cyberterrorist targets were classified in the ontology in order to distinguish between low-profile individual attacks and wider-spread government or organization targets. The various targets identified in a framework by Veerasamy and Grobler [32] were placed into the governmental and critical targets category. Examples in the organizational targets group are email, production sales and marketing systems [36]. The range of targets would be specified in the CLC model.

5.7 Effects

- A cyber event can have different targeted effects which are null, minor, major or catastrophic damage [36], [30], [22]. The CLC model will show the effects that cyberterrorist are trying to achieve depending on a malicious objective or support function.

5.8 Practices

- Crashing critical systems demonstrate the types of practices that are used to carry out cyberterrorist attacks [37], [32]. The CLC model will describe the different practices.
- Cyberterrorism has been compared to cybercrime and cyberattacks. Cyberattacks can be performed by ordinary recreational hackers testing out their skills or trying to commit some fraudulent activity, and hacking skills and security violations can also be used as part of cyberterror attacks [32]. 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.
- 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 [32].
- The use of the Internet for cyberterrorism can also be grouped under the following classifications: web literature, social-networking tools, anti-forensics and fundraising [34]. These classifications and detailed uses will form part of the practices in the CLC model.
- Propaganda and knowledge creation is carried out using web literature. Examples of web literature include periodicals, essays, manuals, encyclopedias, poetry, videos, statements and biographies [19], [3], [16], [38]. These concepts will form part of the explanation of practices in the CLC model.
- Social-networking tools include forums, blogs, websites, gaming, virtual personas, music and applications [40]. 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 offer opportunities for significant further research in studying the recruitment, training and communication practices in order to develop ways of interception and prevention.
- Terrorists are constantly trying to utilize 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 anonymizers [21], [23], [2]. 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 cyber activity and highlight that new and innovative methods will most likely be developed.
- Fund-raising is carried out using various scams including auctioneering, casinos, fake drugs, donations, credit card theft and phishing [40], [24], [14]. The CLC model will incorporate these fund-raising schemes.
- When carrying out a cyberterrorism act, certain practices will be employed [33]. The CLC model will show the various practices that can be utilized as part of a cyberterror attack or support function.
- Further practices that were identified and classified are web defacement and data manipulation [36]. A broader range of cyberterrorism practices will be covered in the CLC model.

6. Additional Input to CLC Model

Further input to the model was based on general observations of the cyberterrorism field as well as a study of possible countermeasures. These findings are discussed in this section.

6.1 Countermeasures

Countermeasures form part of the Deter phase of the CLC model. The development of the countermeasures is discussed next.

- Countermeasures need be devised from a strategic and technical point of view. . Examples of countermeasures cannot strictly be classified as belonging to a single category. For example, the establishment of cultural centers which promotes the understanding of religion and culture while exposing visitors to outside opinions can be considered as both a social and religious countermeasure [35]. The CLC model will show the overlapping classification of countermeasures.

- Strategic countermeasures can be grouped as legal, political, economic, social and religious categories [35]. Other examples of strategic countermeasures include: media, charities, cultural centers, analysis, education, humanitarian aid, military response, peace-keeping, policies, treaties, protocols, laws, fusion centers and perception management [35], [5], [41]. The range of countermeasures will be captured in the CLC model.
- Technical countermeasures include: CSIRTs, intrusion prevention, network monitoring, interception and blockage, disaster recovery and forensics [35]. These technical countermeasures will form part of the CLC model.

6.2 General Points

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. The definition given in Section I states that overall cyberterrorism can be seen as the threat or act of causing harm in order to create fear and shock, targeting critical ICT infrastructures based on political, religious or social reasoning [15], [8].

Cyberterrorism is often mistaken as any cybercrime event. Ontologies helped identify the defining concepts of cyberterrorism as it allows for a structuring of a field by showing relationships, interactions and definitions. In the ontological study of cyberterrorism, the following concepts are introduced based on the motivation, objective, effect, target and practice: a cyberterror attack, support function and an unknown cyber event [36]. The CLC model caters for the different types of objectives and practices.
In order for a cyber event to be classified as cyberterrorist 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 organization, government or critical target [36]. The requirements for a cyberterror attack will be shown in the CLC model. 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 [36].

Overall, the CLC model was compiled based on the identification of the various factors, as well as the adaptation of the OODA loop. The model encapsulates the critical aspects pertinent to the field of cyberterrorism.

7. Conclusion

Since various factors can either directly or indirectly influence the development of a cyberterrorist, there is a lot of uncertainty in terms of classifying cyber events as either a terrorist attack or a cybercrime. This paper set out to propose the development of the CLC model to address this classification.

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 regular cybercrime or cyberterrorism.

References

[1] J. Boyd, "A discourse on winning and losing," Maxwell Air Force Base, 1987.

[2] J. Carr, "Anti-Forensic Methods Used by Jihadist Web Sites," ESecurity Planet, 1608. 2007.

[3] S. Coll and S.B. Glasser, "Terrorists turn to the Web as base of operations", The Washington Post, vol. 7, pp. 77–87, 2005.

[4] B.C. Collin, "The Future of Cyberterrorism: The Physical and Virtual Worlds Converge", Crime and Justice International, vol. 13, pp. 14-18, 1997.

[5] A.K. Cronin, "The diplomacy of counterterrorism lessons learned, ignored and disputed," International Research Group on Political Violence (IRGPV), pp. 1-8, 2002.

[6] A. de Borchgrave, T. Sanderson and J. Harned, "Force multiplier for intelligence," Centre for Strategic and International Studies, 2007.

[7] D. Denning, "Cyberterrorism," Global Dialogue, vol. 18, 23 May. 2000.

[8] K.C. Desouza and T. Hensgen, "Semiotic Emergent Framework to Address the Reality of Cyberterrorism", Technological Forecasting and Social Change, vol. 70, pp. 385-396, 5 2003.

[9] M. M. Elmusharaf , "Cyber Terrorism:The new kind of terrorism", Computer Crime Research Center, Accessed 20086 October, Available online at http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism.

[10] J.M. Epstein, "Why Model?", Journal of Artificial Societies and Social Simulation, vol. 11, pp. 12, 2008.

[11] H.E. Eriksson and M. Penker, Business modeling with UML, New York: John Wiley & Sons, 2000.

[12] C. Foltz Bryan., "Cyberterrorism, Computer Crime, and Reality", Information Management & Computer Security, vol. 12, pp. 154-166, 2004.

[13] G. Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism", Studies in Conflict and Terrorism, vol. 27, pp. 387-408, 2004.

[14] S.E. Goodman, J.C. Kirk and M.H. Kirk, "Cyberspace as a medium for terrorists", Technological Forecasting and Social Change, vol. 74, pp. 193-210, 2007.

[15] S. Gordon and R. Ford, "Cyberterrorism?", Computers & Security, vol. 21, pp. 636-647, 2002.

[16] Jamestown Foundation, "Next Stage in Counter-Terrorism: Jihadi Radicalization on the Web," 2310. 2006.

[17] L. Janczewski and A.M. Colarik, Cyber warfare and cyber terrorism, Information Science Reference, 2007.

[18] B.M. Jenkins, "The New Age of Terrorism," New York: McGraw-Hill, 2006, .

[19] D. Kimmage and K. Ridolfo, "Iraqi Insurgent Media. The War of Images and Ideas. How Sunni Insurgents in Iraq and Their Supporters Worldwide are Using the Media", Washington, Radio Free Europe/Radio Liberty, 2007.

[20] I. Lachow, "Cyber security: A few observations," 2008.

[21] S. Lau, " An analysis of terrorist groups' potential use of electronic steganography ", Bethesda, Md.: SANS Institute, February, pp. 1-13, 2003/02/18 2003.

[22] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms", ACM SIGCOMM Computer Communication Review, vol. 34, pp. 39-53, 2004.

[23] Y. Noguchi and S. Goo, "Terrorists' Web Chatter Shows Concern About Internet Privacy," The Washington Post, 0413. 2006.

[24] P. Piper, "Nets of terror: Terrorist activity on the internet," Searcher, vol. 16, November/December 2008. 2008.

[25] M.M. Pollitt, "Cyberterrorism - fact or fancy?", Computer Fraud & Security, vol. 1998, pp. 8-10, 1998.

[26] R.C. Puran, "Beyond Conventional Terrorism… The Cyber Assault," SANS, Tech. Rep. GIAC Security Essentials Certification (GSEC) v1.4b, 2003.

[27] Supercourse lectures, "Cyber Terrorism (When the Hackers Grow Up)," 2008.

[28] I. Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," Guardian, vol. World News, 2007.

[29] US Army Training and Doctrine Command, Critical infrastructure threats and terrorism, Fort Leavenworth, Kansas: US Army Training and Doctrine Command, 2006.

[30] R.P. Van Heerden, B. Irwin and I.D. Burke, "Classifying network attack scenarios using an Ontology", in Proceedings of the 7th International Conference on Information Warfare and Security, 2012.

[31] M.A. Vatis, "Cyber Attacks During the War on Terrorism: A Predictive Analysis", 2001.

[32] N. Veerasamy, "A high-level conceptual framework of cyberterrorism", Journal of Information Warfare, vol. 8, pp. 42-54, 2009.

[33] N. Veerasamy, "High-level Mapping of Cyberterrorism to the OODA Loop", in Proceedings of the 5th International Conference on Information Warfare and Security, pp. 352-360, 2010.

[34] N. Veerasamy and M. Grobler, "Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure", in Proceedings of the 6th International Conference on Information Warfare and Security, pp. 260, 2010.

[35] N. Veerasamy and M. Grobler, "Countermeasures to consider in the combat against cyberterrorism", in Proceedings of the Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2010, pp. 58, 2010.

[36] N. Veerasamy, M. Grobler and B. Von Solms, "Building an Ontology for Cyberterrorism", in Proceedings of the 11th European Conference on Information Ware and Security, 2012.

[37] B. Von Solms, "Critical Information Infrastructure Protection- Essential During War Times, or Peace Times or both?", in IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace, pp. 36-40, 2008.

[38] G. Weimann, "How modern terrorism uses the internet", The Journal of International Security Affairs, vol. Spring 2005, Spring 2005 2005.

[39] G. Weimann, "Cyberterrorism: How real is the threat?" United States Institute of Peace, Tech. Rep. 119, pp. 1-12, 2004.

[40] J. Whelpton, "Psychology of Cyber Terrorism," in Cyberterrorism 2009 Seminar, South Africa: Ekwinox, 2009, .

[41] C.J. Williers, C.J. Voster, A. van 't Wout, J.P. Venter, S.J. Naude and R. van Buuren, "IW Basic Course," Council for Scientific and Industrial Research, Tech. Rep. DEFT-IW-00200, 2005/06.

A review of IPv6 security concerns

R.P. van Heerden[1,3], I.M. Bester[2], I.D. Burke[1,4]
[1]DPSS,CSIR, Pretoria, South Africa
[2]Computer Engineering, University of Pretoria, Pretoria, South Africa
[3]Computer Science, Rhodes University, Grahamstown, South Africa
4Computer Science, University of Pretoria, Pretoria, South Africa
rvheerden@csir.co.za
naasbester@gmail.com
iburke@csir.co.za

Abstract: This study focus on the security concerns of IPv6. We make a broad introduction to IPv6 then briefly look at the differences between the IPv6 and IPv4 protocols, their known vulnerabilities and identifies some security concerns when implementing IPv6. Even after 13 years, IPv6is still considered a new network protocol. With this in mind not much is known about IPv6. Since the IPv4 address space will be used up within the next few months, IPv6 should finally become more mainstream.

Keywords: IPv6

1. Introduction:
Darrin Miller, Security Researcher, CIAG, Cisco System stated: “IPv6 makes some things better, other things worse, and most things are just different, but no more or less secure” [1].The Internet Engineering Task Force (IETF)proposed a new internet protocol in 1990s [2]. Internet Protocol Next Generation (IPng) was created, which then became Internet Protocol version 6 (IPv6) [1] and is the successor to IPv4. Its development is ongoing for more than 13 years and this protocol is still described as the new generation protocol since most of its implementation is still in engineering laboratories and by academia. Less than approximately 1% of all internet traffic is IPv6 based. The migration to IPv6 is happening at a very slow pace.

2. The Internet Protocol
What is Open Systems Interconnection Model (OSI)?
The OSI model is a way of sub-dividing a communications system into smaller parts called layers. Similar communication functions are grouped into logical layers. A layer provides services to its upper layer while receiving services from the layer below. On each layer, an instance provides service to the instances at the layer above and requests service from the layer below [3].

Figure 1 shows the 7 OSI layers and accompanying protocols. Internet Protocol (IP) forms part of the third layer, the Network Layer.

2.1 What is Internet Protocol?
A protocol (in the context of a computer network) is a set of rules governing the exchange or transmission of data electronically between devices. IP is the principal communications protocol used for relaying data packets across a network. It is responsible for routing packets across network boundaries. It is the primary protocol that establishes the Internet.

IPv4 is currently the dominant protocol of the Internet, but is envisioned to be succeeded by IPv6.

2.2 Why was IPv6 Developed?
IPv6 was developed because IPv4 does not have enough addresses available to sustain the ever growing internet and all the devices that need a unique IP address to connect to it. IPv4 has a theoretical upper limit of about 4 billion (4,000,000,000) unique addresses but in practice IPv4 is unlikely to support a sustainable population of no more than about 250 million uniquely addressed nodes [4].

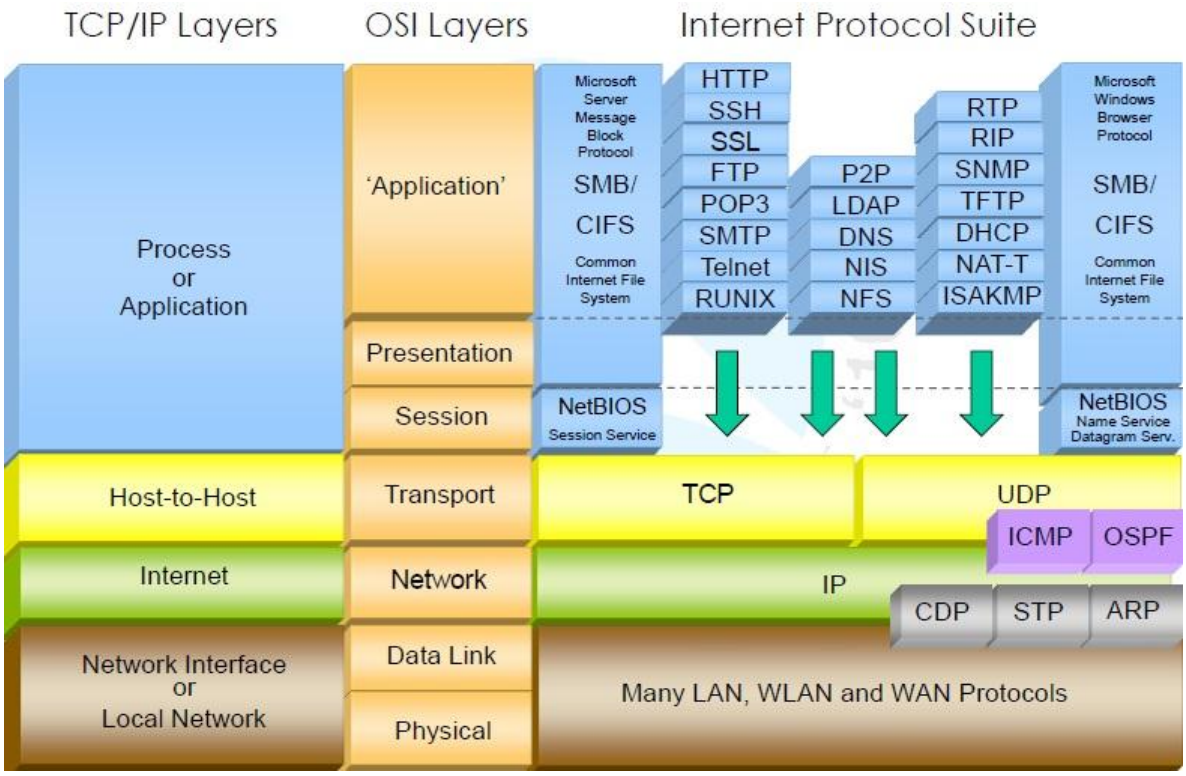

Figure 1: Open Systems Interconnection model (OSI model) [5]

2.3 What about Network Address Translation?

Network Address Translation was developed to alleviate the effects of IPv4 address depletion.Network Address Translation (NAT) basically translates one or more addresses into another, typically a private address into a public address and vice-versa. Many users and sites do this today on a small scale. An end-user laptop may have a private address which is translated by the home router into a public address provided by theInternet Service Provider (ISP). The public address is unique and this is the address depended on for global Internet connectivity. So what happens when the ISP runs out of addresses? Before address exhaustion, it would simply apply for and receive new addresses [6].

The Internet Assigned Numbers Authority (IANA) will assign the last of the available IPv4 addresses during 2012 after which there are no more new IPv4 addresses available [7].

2.3.1 Large Scale NAT

This is basically address translation upon address translation, also called Carrier Grade NAT. Intermediate endpoints like home routers will also get a private address instead of a public one and then translate its traffic at a new heavy-duty Large Scale Network Address Translation (LSN) device that lives elsewhere on the Internet. Thousands of users will share a single IP address through this massive translator. What is unclear is whether this will provide the same performance, reliability, and security currently on the Internet [6].

2.3.2 LSN compared to IPv6 as a solution

IPv6 has been years in development and is considered a longer-term and more reliable solution than LSN. Adopting IPv6 means that people with IPv6 addresses can talk to IPv6-enabled or dual-stack sites without LSN translators. Figure 2 describes some other aspects of LSN compared to end-to-end IPv6 connectivity [6].

LSN	IPv6
Adds a device between user and websites	Provides direct, native HTTP connection, like today
Off-path detour and load on translator adds latency	Shortest path, no added latency
1000s of users share one IP address	One address per user (or household)
Single attacker can poison an address shared by 1000s of users; attackers can hide easily	Same security model as today
Unknown location and uptime of LSN devices	Same SLA model as today

Figure 2: Large scale NAT vs. End-to-End IPv6

IPv6 represents the last and best hope for continued, unencumbered Internet growth. Not going this route will lead to islands of IPv4 "NAT'ed" or similar networks with various toll gates and bridges that offer a small aperture to the rest of the world [8].

2.4 Why is the migration happening so slowly?

The major stumbling block to the deployment of IPv6 is that it is not backwards compatible. That means network and website operators have to upgrade their network equipment and software to support IPv6 traffic, and so far most have been unwilling to do so [9].

There exists a Catch-22of supply and demand for IPv6 content/traffic. Network equipment vendors don't put their weight behind producing affordable large range IPv6 compatible equipment, because enterprises won't buy it. Web based enterprises don't upgrade their equipment to IPv6 compatible devices because no or little endpoint users will be able to use it. Most equipment in homes today won't support IPv6. Then it goes back, most endpoint users won't buy expensive equipment that support IPv6 if their ISP does not and if most of the internet websites are still hosted through IPv4 technology etc.

Security is a concern but it is not the driving force behind the slow migration. There is no definite start or end date for the migration and it is predicted that it will still go on for years.

2.5 Header Structures

The common way to represent theses header is to draw them as a succession of 32-bit words. The top word is transmitted first and the left most byte of each word is transmitted first [10].

2.5.1 IPv4 Header

IPv4 provides 32-bit address space and has a theoretical upper limit of about 4 billion (4,000,000,000) unique addresses but in practice IPv4 is unlikely to support a sustainable population of no more than about 250 million uniquely addressed nodes. The IPv4 header structure is described below and shown in Figure 3.

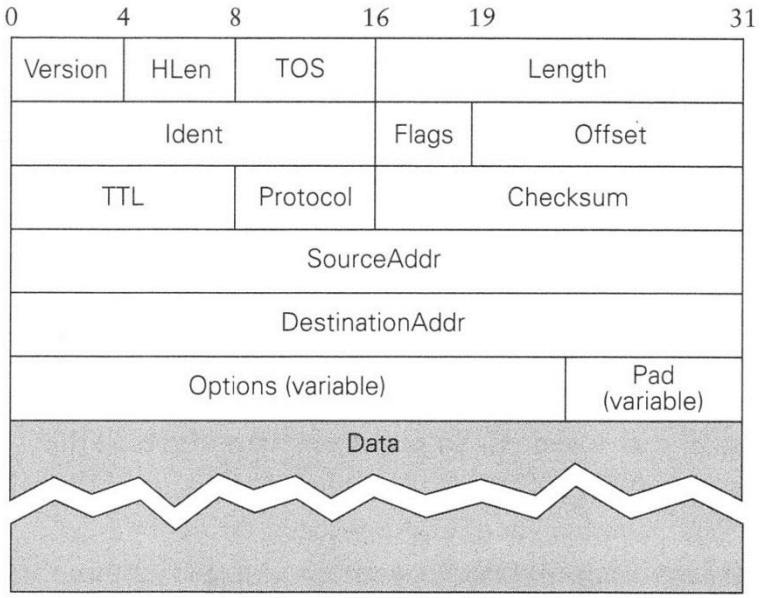

Figure 3: IPv4 Header Structure

- **Version**: The Version field specifies the current version which is 4 in this case. The header processing software checks this first and then knows how to process the rest.
- **HLen**: The HLeng specifies the number of 32-bit words in the header. Minimum is 5 where 5×32=160 bits or 20bytes. The maximum is 15 where 15×32=480 bits or 60 bytes.
- **TOS**: Differentiated Services Code Point formerly known as TOS (Type of service) is used to indicate if a packet should receive some sort of special or priority processing.
- **Length**: This is a 16-bit field defining the total length of the datagram (header and data). The minimum is 20bytes and the maximum is 65,535 bytes.
- **Ident**: The Ident is used for identifying fragments of the original datagram.
- **Flags**: The Flags is a 3-bit field used to control and count fragments of the datagram.
- **Offset**: The Offset is a 13-bit field that specifies the offset of a particular fragment relative to the beginning of the original unfragmented datagram. The first fragment has an offset of zero.
- **TTL**: The TTL (Time to Live) reflects historical intention where the time the packet was allowed to exist on the network was considered but it has become more of a hop count than a timer.
- **Protocol**: The Protocol field is a key that identifies to which of the OSI higher-level protocol the IP packet should be passed to. Examples are TCP and UDP.
- **Checksum**: The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header. It is used for error checking the header. If an error is detected the packet is discarded and must be resend.
- **SourceAddr**: The SourceAddr (Source Address) is the IPv4 address of the sender. It is included so that the recipient can decide if it wants to receive data from this sender and also to know where to reply to if it wants to reply. Note that during transit a NAT device could change this address.
- **DestinationAddr**: The DestinationAddr (Destination Address) is the IPv4 address indicating the receiver of this packet. Note that during transit a NAT device could change this address.
- **Options** and **Pad** (variable): There may be a number of options at the end of the header but these are not used often.

2.5.2 IPv6 Header

Migration to IPv6 support is a gradual process, and mechanisms to gracefully support IPv6 in IPv4 networks have been an important part of the IPv6 development project from the start. IPv6 provides a 128-bit address space and can address 3.4×1038 nodes.

The IPv6 header structure is described below and shown in Figure 4.

Figure 4: IPv6 Header Structure

- **Version**: The Version field is set to 6 for IPv6.
- **TrafficClass**: The TrafficClass field identifies the priority and class of service of this packet.
- **FlowLabel**: The FlowLabel field is for future use in identifying packets that are part of a unique flow, stream, or connection
- **PayloadLen**: The PayLoadLen field defines the length in octets of the packet that follows the IPv6 header.
- **NextHeader**: The NextHeader field identifies the type of header that follows the IPv6 header. This replaces the Options and Protocol field of IPv4.
- **HopLimit**: The HopLimit field is a counter for the number of remaining hops the packet can traverse. This is simply the TTL of IPv4 renamed.
- **SourceAddress**: The IPv6 address of the node that originated this packet.
- **DestinationAddress**: The IPv6 address that this packet is destined for.

2.6 IP Security

2.6.1 Comparing IPv6 with IPv4

The following was identified as prominent problems with IPv4 for which IPv6 are the solution [11].

- The imminent exhaustion of the IPv4 addressing space.
- The imminent collapse of the Internet routing structure due to explosive growth of the non-default routing table.
- The problem of end-to-end interoperability across routing domains in which IP addresses may not be globally unique.

The way in which IPv6 is capable of solving these problems becomes clearer when keeping in mind their different header compositions as described in the previous sections [10].

2.6.2 Migrating from IPv4 to IPv6 vulnerabilities

The migration from IPv4 to IPv6 has no determined end date. The process is slow.

Table 1 lists some important documents for migrating to IPv6.

Table 1: IPv6 Documents

RFC#	Title
2071	Network Renumbering Overview- Why would I want it and what is it anyway?
2072	Router Renumbering Guide
2185	Routing Aspects of IPv6 Transition
2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
2767	Dual Stack Hosts Using the Bump-in-the-Stack Technique (BIS)
2893	Transition Mechanisms for IPv6 Hosts and Routers
3056	Connection of IPv6 Domains via IPv4 Clouds
3142	An IPv6-to-IPv4 Transport Relay Translator

Three transition techniques were developed by the IETF:

- Dual-stack: The nodes have two protocol stacks (IPv4 and IPv6) enabled and use IPv6 to contact IPv6 nodes and use IPv4 to contact IPv4 nodes.
- Tunnels: Hosts or routers send and receive IPv6 packets using an overlay network of tunnels established over an IPv4 network or over label switched path (LSP) (in a Multiprotocol Label Switching [MPLS] network).
- Protocol translation: A protocol translator acts as an intermediary between the IPv4 and IPv6 worlds.

A list of vulnerabilities of running dual-stack:

- Protected against IPv4 attacks but not IPv6 attacks. A lot of users are not aware that their operating system is running both version of the protocol automatically.
- Denial of Service attacks

A list of vulnerabilities of running tunneling:

- Address spoofing
- Reflection attack

2.6.3 Similarities between IPv6 and IPv4 vulnerabilities

IPv6 and IPv4 both fall within the Network Layer of the OSI stack. If for example a network layer application is vulnerable in IPv4, it will also be vulnerable in IPv6.

A list of similar vulnerabilities:

- Attacks against the physical, data link or application layers
- Man-in-the-middle attacks
- Sniffing/eavesdropping
- Denial of Service (DoS) attacks [12]
- Spoofed packets: forged addresses and other fields
- Attacks against routers and other networking devices

2.6.4 Differences between IPv6 and IPv4 vulnerabilities

The way in which IPv6, as part of the network layer of the OSI stack, interacts with the layers above and below it can also introduce new vulnerabilities.

A list of vulnerabilities where the difference is only slightly:

- LAN-based attacks through the Address Resolution Protocol (ARP) or Neighbor Discovery Protocol (NDP)
- Attacks against Dynamic Host Configuration Protocol(DHCP)or DHCPv6
- Denial of Service (DoS) against routers (hop-by-hop extension headers rather than router alerts)
- Fragmentation (IPv4 routers performing fragmentation versus IPv6 hosts using a fragment extension header)

- Packet amplification attacks (IPv4 uses broadcast versus IPv6 uses multicast)

A list of vulnerabilities where the difference is unique to IPv6:

- Reconnaissance(since brute force with the larger address space is more time consuming) and scanning worms
- Attacks against the required component Internet Control Message Protocol for IPv6 (ICMPv6)
- Extension Header (EH) attacks
- NDP attacks (Auto configuration) are simple to perform
- Attacks on dual stack implementation migrating from IPv4 to IPv6.
- Mobile IPv6 attacks. Devices that roam are susceptible to much vulnerability.
- IPv6 protocol stack attacks because bugs and shortcomings might exist in the code.

3. IPv6 Security Concerns

The following section categorizes security concerns regarding IPv6 implementation [13]-[20].It is discussed like a ripple effect starting at the protocol itself and rippling outwards through the network along the path of communication. Implementation of Current Best Practice (CBP) is strongly advised when planning or working on these different parts of the IPv6 network. It is also encouraged to research the specific area of implementation in the context of the intended network. Hence the description current best practice, because it is still changing.

3.1 Protocol Security

This concern involves the protocol itself, its structure and how it works. The implementation of ICMPv6 and Extension Headers are especially important. IPsec is mandatory in IPv6 and its implementation is very important. Its presence is carried over to some of the other sections as well.

3.2 Operating System Security

This concern is with the IPv6 security capabilities and setup of operating systems running on the different client and server machines composing the intranet. These machines hold the most valued information and the operating system is the connection between the information and the rest of the network.

3.3 Network Security

This concern is with the organizations intranet or network inside the perimeter mostly regarding the Data Link Layer of the OSI [12]. The CSI/FBI 2007 Computer Crime and Security Survey reported that 64 per cent of the surveyed organization's losses were partially or fully a result of insiders. The implementation of Neighbor Discovery Protocol (NDP) and DHCPv6 are especially important.

3.4 Perimeter Security

This concern is based on the old military strategy where the city border is fiercely protected leaving the inside save. It involves the perimeter around an organizations network where it connects with the internet or other organization networks. The implementation of IPv6 firewalls is especially important. New proposed security models might incorporate firewalls into an Intruder Detection System (IDS).

3.5 Internet Security

This concern is with the cloud. It involves the internet, traffic and equipment like routers. These threads could come from anywhere across the web, even form distributed threats working together. Configuration of routers is especially important.

3.6 Virtual Private Network Security

This concern is with Virtual Private Network (VPN) setup over IPv6 also known as “tunneling”. This is a secure private connection through a public network or an otherwise unsecure environment. The implementation of IPsec is especially important.

3.7 Mobile Security

This concern is with mobile devices like laptops and smart phones where the need to roam around while staying connected is growing fast. Here again the implementation of IPsec is especially important. Take note of the new Mobile Internet Protocol (MIP) implementation.

3.8 Conscientious Security

This concern is with the users and more importantly the administrators of the system. Their skills, discipline and awareness might be the last defence in a possible security disaster. Cultivation of such skills and users are encouraged.

4. World IPv6 Day

On 8 June, 2011, under the sponsorship of the Internet Society, top websites and ISP's around the world, including Google, Facebook, Yahoo!, Akamai and Limelight Networks joined together with more than a 1000 other participating websites in World IPv6 Day. This entailed a 24-hour global-scale "test flight"of the new Internet Protocol, IPv6 [21].

During this trail all the participating web sites served up their content using IPv6 as well as the current standard IPv4. The event was hailed a massive success, raised visibility of IPv6 and allowed network engineers to determine how well IPv6 works and to pinpoint technical difficulties such as misconfigured systems and delays for some end users trying to access participating Web sites [22].

4.1 Data traffic statistics

For a bright 24 hour period, shown in Figure 5, the IPv6 network looked a little bit more like its IPv4 big brother. Web traffic grew during the day up until the midnight cut-off point where some of the major content providers withdrew their namespace support. At midnight UTC the web traffic falls off the cliff and the traffic mix returns to its pre-v6-day chatter [23].

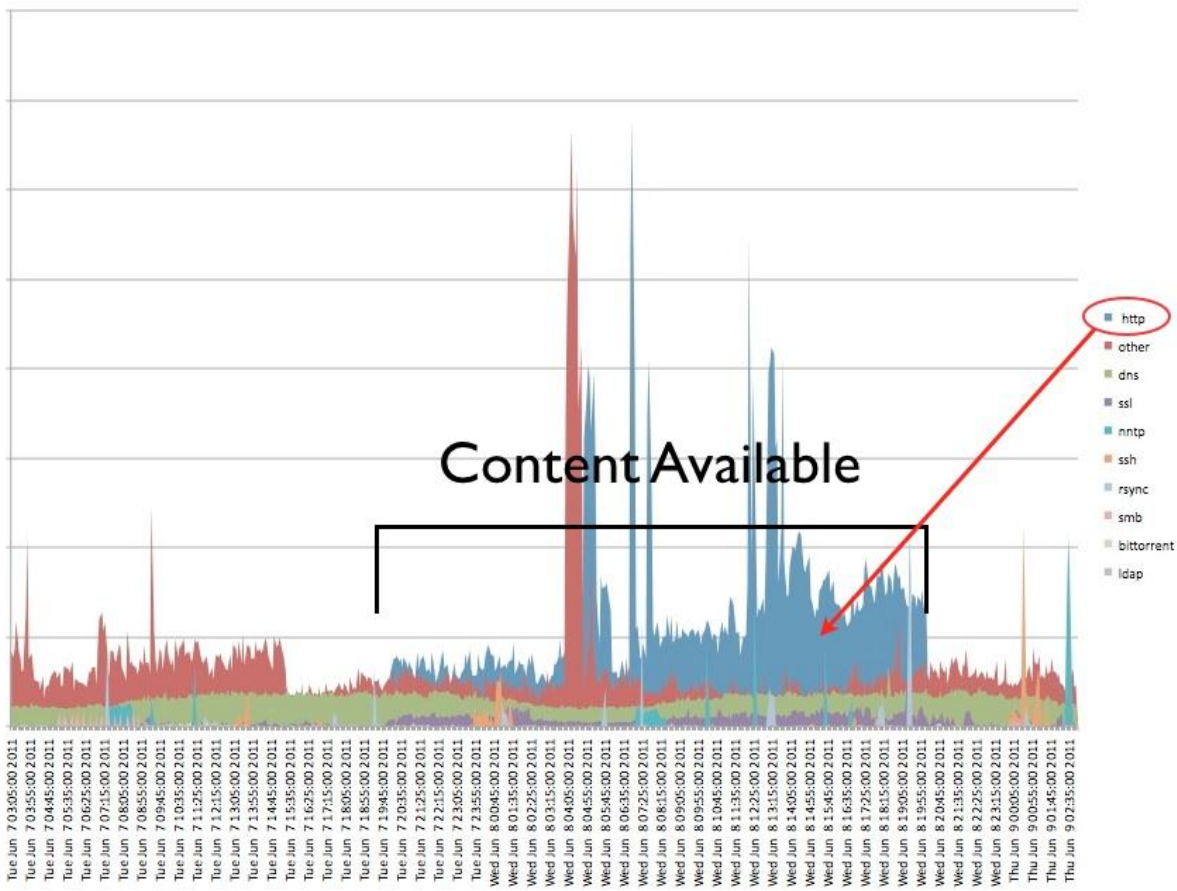

Figure 5: Application breakdown for native IPv6 traffic from six carriers [23]

In Figure 6 the percentage of IPv6 traffic of all Internet traffic in six carriers roughly doubled during the v6-day period. However, doubling a fraction of a per cent is still a fraction of a per cent. Most end users probably have at least a mediating Domain Name System (DNS) caching device (home router

or wireless base station) that may not elegantly switch back and forth from v4 to v6. The inertia and complexity of changing this element of the Internet is massive [23].

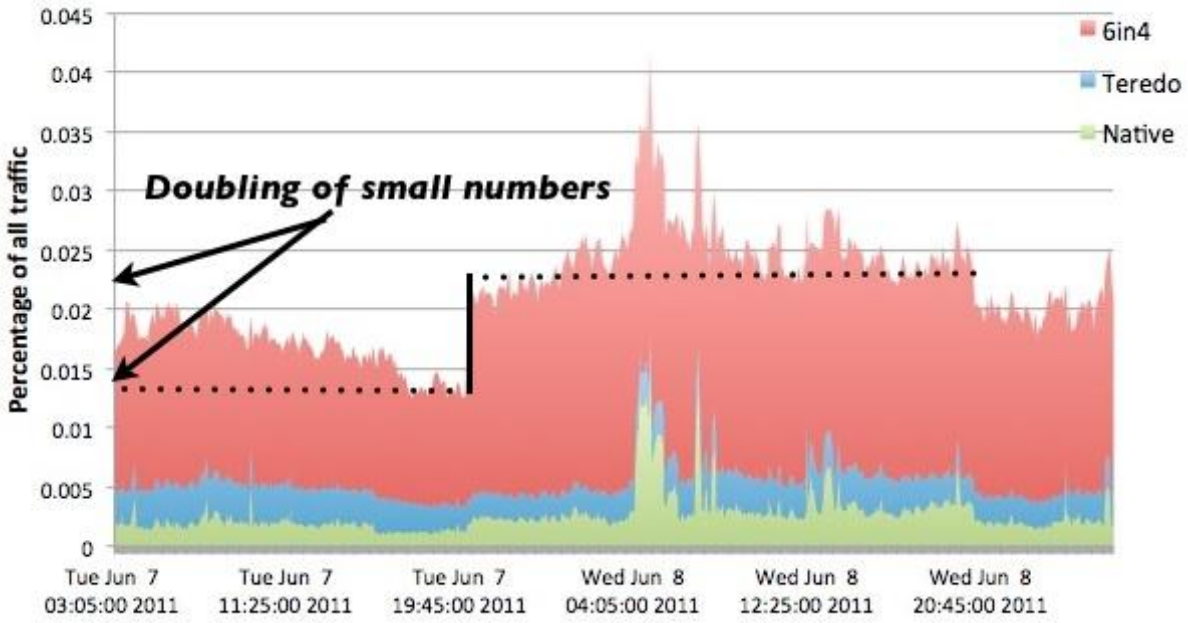

Figure 6: Percentage of IPv6 traffic of all Internet traffic in six carriers [23]

4.2 Test your IPv6 Connectivity

The Internet Society made a test site (http://test-ipv6.com/) available for end users to test their IPv6 compatibility [24]. Figure 7 shows the results of my local machine connected via a Wi-Fi router to an ADSL line.

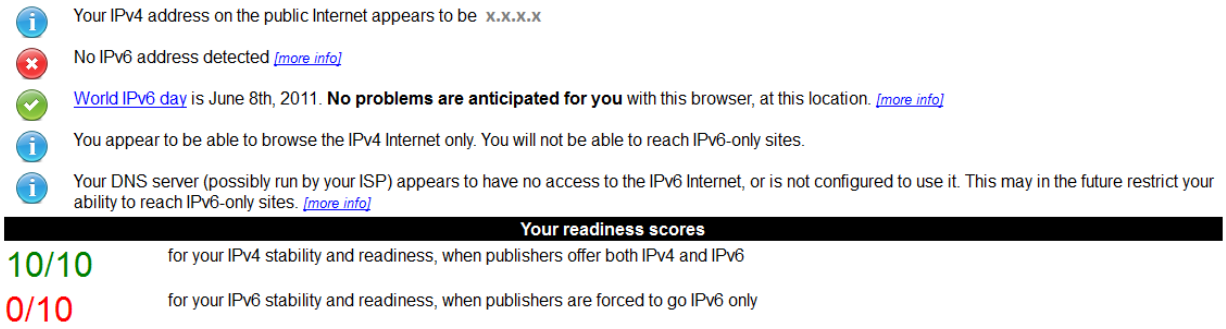

Figure 7: Local Machine Test Results

4.3 Google after IPv6 Day

Google said it has decided to leave its main YouTube website enabled for IPv6 for the time being. Since 2008, Google has supported IPv6 on separate websites -- such as www.ipv6.google.com -- rather than on its main websites. Lorenzo Colitti, IPv6 Software Engineer at Google stated that “We saw 65% growth in our IPv6 traffic on World IPv6 Day" [25].

Google over IPv6 uses the IPv4 address of your DNS resolver to determine whether a network is IPv6-capable. If you enable Google over IPv6 for your resolver, IPv6 users of that resolver will receive AAAA records for IPv6-enabled Google services. Normally, if a DNS resolver requests an IPv6 address for a Google web site, it will not receive one but a DNS resolver with Google over IPv6 will receive an IPv6 address, and its users will be able to connect to Google web sites using IPv6 as shown in Figure 8 [26].

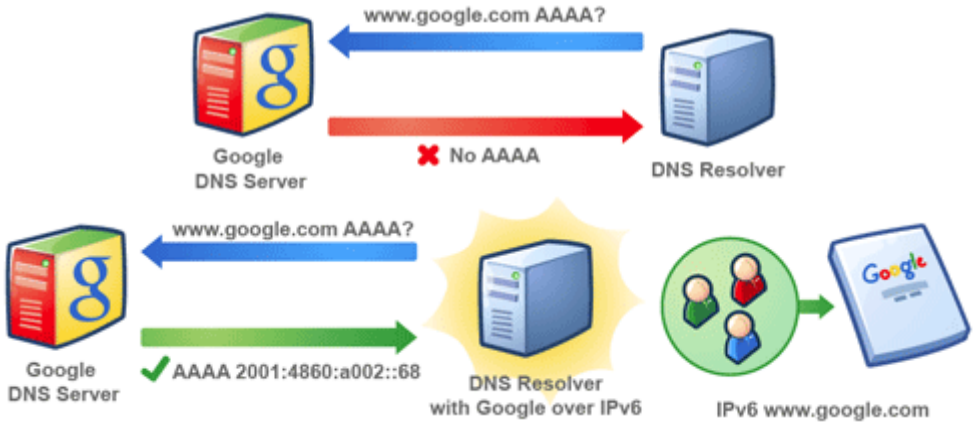

Figure 8: Google over IPv6

4.4 Facebook after IPv6 Day

Don Lee, senior network engineer at Facebook stated: "At Facebook, we saw over 1 million of our users reach us over IPv6 ... There were no technical glitches in this 24-hour period. We were encouraged by the many positive comments on our blog. ... It is really interesting to see how passionate people were about IPv6 around the world" [25].

Because of the positive results from World IPv6 Day, Facebook has decided to support IPv6 on its Website for developers, which is developers.facebook.com.

4.5 Security on IPv6 Day

The general conclusion of the 24-hour trail is that security stayed in tacked. It is also generally known that this is too short a time to form any conclusive opinions regarding the mater. Some security feedback after IPv6 day follows.

“Latest reports state that the 24-hour global test run did not hit any major glitches, according to a spokesman for Arbor Networks, an Internet security company monitoring the IPv6 activity” [27].
"The Internet is under constant attack, and a lot of it is insignificant," Champagne says. "We did see some DoS attacks that were going on over IPv4, and when folks switched to IPv6, the attacks switched to IPv6. But it still wasn't material. We haven't seen any massive attacks." As this large-scale experiment draws to a close, no major outages or security breaches were reported at the 400-plus corporate, government and university websites participating in the IPv6 trial. Champagne says Akamai has not seen more broken IPv6 connections than expected, nor has it noticed any major attacks aimed at IPv6 [28].

Some people had predicted that hackers were going to take advantage of World IPv6 Day. The thought was that if these large sites, which had historically been IPv4, were to become IPv6 accessible they would be vulnerable. Many organizations may have significantly sophisticated IPv4 defences but their IPv6 defensive capabilities may not be sufficient. The attackers could perform reconnaissance on the public IPv6 addresses of these sites and see if they are more vulnerable with IPv6 than with IPv4. The SANS Internet Storm Center (ISC) and the Cisco Security Intelligence Operations (SIO) didn't report any security issues related to IPv6. However, that doesn't mean that attackers were not performing some reconnaissance and data gathering [13].

5. Conclusion

Since so little IPv6 implementation is currently out there it is difficult to see the results of this new and complex protocol. Advising people to be aware of the security holes and implement current best practice is the only way to progress with the migration.

References

[1] S. Deering and R. Hinden. IETF, RFC 1883 ,"Internet Protocol Version 6 (IPv6) Specification," Accessed 20110923, Available online at http://www.ietf.org/rfc/rfc1883.txt

[2] S. Deering and R. Hinden. "IETF, RFC 2460, Internet Protocol Version 6 (IPv6) Specification," Accessed 20110925, Available online at http://www.ietf.org/rfc/rfc2460.txt

[3] Wikipedia, "OSI model," Accessed 20110925, Available online at http://en.wikipedia.org/wiki/OSI_model

[4] P. Loshin, "IPv6 Theory", 2nd ed. Arlington: Internet-Standard, 2004.

[5] R. Leutert, "Discovering IPv6 with Wireshark," SHARKFEST'10, 2010.

[6] D. Lee. "Facebook, World IPv6 Day: Solving the IP Address Chicken-and-Egg Challenge," Accessed 20110915, Available online at http://www.facebook.com/notes/facebook-engineering/world-ipv6-day-solving-the-ip-address-chicken-and-egg-challenge/484445583919

[7] C. D. Marsan. "Network World, No more IPv4 addresses,", Accessed 20110925, Available online at http://www.networkworld.com/news/2011/020111-ipv4-apnic.html

[8] C. D. Marsan. "Network World, What if IPv6 simply fails to catch on?" Accessed 20110622, Available online at http://www.networkworld.com/news/2011/052311-ipv6-fail.html?page=1

[9] C. D. Marsan. "What if IPv6 simply fails to catch on?" Network World. Accessed 20110811, Available online at http://www.networkworld.com/news/2011/052311-ipv6-fail.html?page=1

[10] L. Peterson and B. Davie, "Computer Networks A Systems Approach", 2nd ed. London: Academic Press, 2000.

[11] P. Loshin, "IPv6 Theory, Protocol and Practice", 2nd ed. Arlington: Internet-Standard, 2004.

[12] Stephen Shankland. cnet.com , Accessed 20110910, Available online at http://news.cnet.com/8301-30685_3-57378307-264/ddos-attacks-spread-to-vulnerable-ipv6-internet/

[13] S. Hogg, "IPv6 Security". Indianapolis: Cisco Press, 2008.

[14] Yong-Woon KIM and Hyoung-Jun KIM, "IPv6: No more Next Generation," in the 7th International Conference on Advanced Communication Technology (ICACT), pp 8-11, 2005.

[15] D. Zagar and K. Grgic, "IPv6 Security Threats and Possible Solutions," in Automation Congress (WA06), p 1-7, 2006.

[16] D. Zagar and S. Vidakovi, "IPv6 Security: Improvements and Implementation Aspects," in Proceedings of the 8th International Conference on Telecommunications, 2005.

[17] M. Ford, "New Internet Security and Privacy Models Enabled by IPv6," in the 2005 Symposium on Applications and the Internet Workshops, p 2-5, 2005.

[18] A.R. Choudhary and A. Sekelsky, "Securing IPv6 Network Infrastructure: A New Security Model," in IEEE International Conference on Technologies for Homeland Security (HST), p 500-506, 2010.

[19] S. Szigeti and P. Risztics, "Will IPv6 Bring Better Security?:, in the Proceedings of Euromicro Conference, p 532-537, 2004.

[20] H. Zimmermann, "OSI Reference Model," IEEE Transactions on Communications, vol. COMM-28(4), 1980.

[21] Internet Sociaty, "About World IPv6 Day.", Accessed 20111025, Available online at http://www.worldipv6day.org/

[22] C. D. Marsan. "Network World, Large-scale IPv6 trial set for June 8." , Accessed 20110925, Available online at http://www.networkworld.com/news/2011/060311-ipv6-day.html

[23] R. Malan. "Arbor Networks, World IPv6 Day: Final Look and "Wagon's Ho!"." , Accessed 20111011, Available online at http://asert.arbornetworks.com/2011/06/world-ipv6-day-final-look-and-wagons-ho/,

[24] Internet Sociaty, "Test your IPv6 connectivity." , Accessed 20110925, Available online at http://test-ipv6.com/,

[25] C. D. Marsan. "Network World, Google, Facebook promise new IPv6 services after successful trial." , Accessed 20110925, Available online at Google, Facebook promise new IPv6 services after successful trial,

[26] Google, "Google over IPv6.", Accessed 20110801, Available online at http://www.google.com/intl/en/ipv6/,

[27] A. Moyo. "ITWebs Portal, Trouble-free World IPv6 Day." , Accessed 20110911, Available online at http://www.itweb.co.za/index.php?option=com_content&view=article&id=44423%3Atroublefree-world-ipv6-day&catid=100&Itemid=219

[28] C. D. Marsan. "Network World, No news is good news on World IPv6 Day.", Accessed 20110925, Available online at http://www.networkworld.com/news/2011/060811-ipv6-day-wrapup.html?nwwpkg=ipv6&ap1=rcb,

An Exploratory Framework for Non-Aggressive Response to Hostile Network Traffic

Samuel Oswald Hunter, Etienne Stalmans, Barry Irwin, John Richter
SNRG, Computer Science Department, Rhodes University, South Africa
sam@rootentropy.co.za
g07s0924@campus.ru.ac.za
b.irwin@ru.ac.za
j.richter@ru.ac.za

Abstract: Hosts connected to the Internet experience a constant and ever increasing onslaught of hostile network traffic. At the same time organisational Internet footprints are growing, extending their presence and increasing the number of possible vectors for attack. Existing methods of defence are failing against these advanced and evolving threats. In this framework various non-aggressive responses to hostile traffic are proposed. These responses include reconnaissance regarding the sources of malicious traffic, as well as passive threat mitigation through false information. Through the exploration of this framework it is hoped to document methods of response to hostile network traffic that would provide valuable information on the threats that networks face in addition to possible mitigation techniques.

Keywords: OODA, Framework, Network Security

1. Introduction

With expanding Internet connectivity organisations, academic institutions, governmental agencies and other entities are becoming more accessible through their "online footprint". This has resulted in an increase in targeted attacks. Attackers are determined and technically opportunistic, looking to exploit any perceived weakness such as out-of-date, unpatched or misconfigured software. Furthermore, determined and trained attackers will look to penetrate a target network using 0-day attacks that exploit previously unknown software vulnerabilities. This allows attackers that have access to sufficient resources to gain remote access to even the most well defended network. Mikko Hypponen, the chief of research at F-Secure, noted that all of the Fortune 500 companies had been breached by attackers [9], dispelling the myth that even corporate networks are secure. In a 2012 article, Richard Bejtlich was quoted as saying that the average cyber espionage attack goes on for 458 days [14]. Current detection and mitigation techniques are clearly failing. The estimated cost of network crime exceeded $388 billion in 2011 [5].

The interconnected nature of the Internet dictates that it forms a shared and integrated domain, where distinguishing between legitimate and malicious network traffic activity can be difficult. The ability to attribute an attack that has been detected is central to solving many of the challenges with classifying network activity. The act of attribution may never be perfect but improved categorisation of specific attacks helps support remediation of damage done by malicious agents. Information sharing between affected parties may assist in attribution and categorisation and will lead to the formulation of appropriate responses to incidents. Furthermore, attribution may assist in determining whether a specific attack is a targeted offensive from a trained threat or an opportunistic attack that may be considered a lesser threat. Attackers involved in targeted attacks have specific goals of what they are aiming to accomplish and will display a more determined approach than opportunistic attackers. The more sophisticated an attack, the more likely that the attacker is focusing on specific assets [10]. Determining the end goal of the attacker may assist in formulated the defensive structure of the network and how incident response should proceed.

In this work a framework for responding to the hostile network traffic that constitute attacks on a monitored network is proposed. At the core of this exploratory framework are active and passive responses that are considered non-aggressive. These responses include active reconnaissance towards the hosts responsible for hostile traffic through the use of fingerprinting techniques and Open Source Intelligence (OSINT) gathering. This information may serve as evidence in legal proceedings or as the first step towards mapping an attack vector for an offensive strike-back. In addition to active responses, the framework will also include passive responses which consider the possibility of false

information. This false information is a form of misdirection aimed towards mitigating and misleading a threat. False information consists of spoofed responses to DNS zone transfers, ICMP ping requests, traceroutes and network scanning attempts. The framework is outlined using the OODA loop (Observe, Orient, Decide, Act), which will be used to categorise the four phases of processing and decision making.

2. Related Work

There exist numerous techniques that may be applied towards detection, prevention and mitigation of malicious traffic on a network. Traditional techniques employ a passive approach towards hostile traffic detection and mitigation. It is, however, important to note that there is a subtle distinction between active responses and breaking the law. While the law concerning network based reconnaissance is unclear, we consider any traffic that may cause harm to another host as hostile. As such, any form of hostile response is excluded from our active response techniques. Before we discuss our framework for non-aggressive responses to hostile network traffic it is important to consider the technologies that have historically played a pivotal role in network and host based defences.

Traditional Anti-Virus (AV) software relies on known signatures of malicious binaries and over-the-wire exploits. AV software often operates at the kernel level giving it the capability to intercept and stop malicious events. While AV software is commonly found at endpoints on a network, Intrusion Detection Systems (IDS) are deployed at traffic bottlenecks such as upstream routers and proxy servers. They share characteristics of AV software in that both rely on known signatures for detecting malicious traffic. In contrast, however, they are placed in less volatile, often dedicated, environments and thus extend their capabilities over an entire network's ingress and egress traffic.

An extension of IDSs are Intrusion Prevention Systems (IPSs). These operate in a more defensive manner by both detecting malicious traffic and blocking it. The most commonly deployed application for defending a network is the firewall. A firewall filters traffic by a set of rules that packets must adhere to when entering or leaving a network. A simplified example of a firewall would be a set of IP tables configured to allow only inbound TCP traffic to port 80. This may be the case for a typical firewall used by a web server. In this example it is only capable of handling HTTP traffic (port 80). Firewalls provide blanket cover against any attacks that do not operate over the ports or protocols defined by the rule set.

There are, however, methods for circumventing almost all defensive techniques. For example, firewalls can be circumvented by tunneling or by reverse connections. The defensive techniques listed above are used to defend against various types of malicious activity that may be represented as hostile traffic and while they work against the majority of attacks, they are less effective against determined attackers.

We consider incoming hostile traffic to include Denial of Service attacks (DoS), exploitation attempts and reconnaissance techniques. Denial of Service attacks are normally represented as resource consumption or exhaustion attacks with a goal of disrupting normal operation and availability of a service. This may be achieved through the use of a botnet in a Distributed Denial of Service attack (DDoS). Exploitation attempts represent specially crafted packets or input data to a service aimed at exploiting a vulnerability or logical fault. Reconnaissance techniques such as port scanning and Operating System (OS) identification are often the first signs of an attack. These reconnaissance techniques are used to map an attack vector which includes possible services and applications that may be attacked. In addition there are threats to a network that are much harder to detect and defend against: these threats often form part of the post-exploitation process and include information leakage, data manipulation and data exfiltration.

Over time the threat landscape has evolved, forcing researchers to find more inventive and efficient means of defending against hostile network traffic. An example of this is a pre-emptive network defence scanner introduced by Fulp [6]. The scanner would pro-actively seek out vulnerable hosts on a local network and quarantine them in order to prevent a possible compromise. The remainder of this section will discuss some of the more recent software applications and services that have been developed as a result of the problems with traditional AV, IDS/IPS and firewalls.

2. 1 Artillery

David Kennedy's Artillery [2] is a combination of a honeypot, file monitor, integrity alerting system and brute-force prevention tool. It is lightweight and employs multiple methods of attack detection, alerting users of insecure *nix configurations. Artillery differs from most traditional honeypots by actively blocking remote clients from accessing monitored hosts if they exhibit potentially malicious behaviour.

2.2 LaBrea

LaBrea a “sticky” honeypot that makes use of persistent capture and throttling to slow down and (in some cases) completely stop the spread of certain self-propagating TCP-based worms. This is achieved by intercepting probes from worms and then forcing them into unexpected states. Throttling is achieved by completing the 3-way TCP handshake and then advertising a very small receiver window. During persistent capture a TCP receiver window of 0 is advertised. This results in the worm sending periodic window probe packets to determine if the window has opened. During the peak of the Code Red worm outbreak approximately 300 000 hosts were infected [1]. For LaBrea to hold 3 scanning threads from Code Red, it would require approximately 8bps. If each infected host was running 100 scanning threads, LaBrea would require 80Mbps to capture and hold all threads. A1000 hosts connected to T1 lines would only have to use 5.2% of their total bandwidth to contain all of Code Red’s scanning during the peak of its outbreak [1].

2.3 Tartarus

Tartarus is a framework for malware tracking and mitigation that makes use of honeypots to detect and quarantine malicious traffic on a local network. A dynamic quarantine is implemented through the use of ARP poisoning. This quarantine mitigates the spread of self-propagating worms in realtime as they are detected by honeypots deployed on a monitored network [8].

3. Active & Passive

Understanding network threats requires security administrators to have awareness of all network activity. This awareness is known as pervasive network awareness and provides administrators with the ability to collect network based information from any point on the network. Pervasive network awareness allows for network threats to be accurately modelled and assessed, allowing the effectiveness of current mitigation strategies to be evaluated. Furthermore, effective network monitoring allows for comprehensive post-incidence forensics. Achieving pervasive network awareness requires the use of multiple network analysis techniques. These may be either active techniques or passive techniques. These techniques are defined by the extent to which the framework interacts with hostile traffic or the entity responsible for generating that traffic.

3.1 Passive Analysis

Passive analysis allows for the monitoring of network traffic without interaction with, or introduction of, any new traffic on the network [4]. Passive traffic analysis does not alert attackers that traffic is being analysed, making it possible to silently monitor the attackers behaviour: an attacker that is aware that their activity is being monitored might alter their behaviour in order to remain undetected. This Intrusion Detection System (IDS) uses passive network monitoring to detect possible threats. Further sources of passive traffic data include network traffic logs from services such as DNS [3], firewalls and domain controllers. A recent SANS survey concluded that administrators were spending too little time analysing logs for security information [10].

3.1.1 Passive Operating System identification

The operating system (OS) being used by an attacker can be determined using passive network traffic monitoring. Passive OS identification relies on the differences in implementation of Request For Comment (RFC) in every OS. The most accurate OS identification can be performed using the TCP SYN packet as it has the greatest number of uniquely identifiable elements. The most commonly used identifiers in passive OS identification are the time-to-live (TTL), fragmentation flags, type of service (TOS), window size, maximum segmentation size, and the flags “Sack OK” and “NOP”. Further OS identification can be performed through the analysis of packet payloads.

Custom scanning tools can be detected through packet analysis by the identification of raw sockets. This can be accomplished as raw socket packet creation requiring all header fields be completed by

the program. The programmatic setting of header fields has a high probability of creating inconsistencies compared to packets generated using the standard sockets API.

Further passive analysis can be performed on attacker traffic by using the source address of the attack. The source address may be used to identify the geographic location of the attacker, along with the organisation to whom the source address belongs. Passive traffic analysis may be used to determine which assets the attackers are targeting. This can be accomplished using destination address analysis, where the intended destination for an attack is recorded and matched to assets belonging to the organisation. Furthermore, passive protocol analysis may assist in target identification. Knowing which protocols are used by applications on the internal network is essential for effective passive protocol analysis. A spike in traffic for a certain protocol may indicate a new attack aimed at a previously unknown vulnerability for that protocol. This type of monitoring allows for a higher degree of protection from zero-day attacks.

3.2 Active Analysis

Active traffic analysis requires interaction with the attacker. There are multiple ways to accomplish this interaction. The primary way to interact with an attacker is through the use of tools similar to those that attackers use against their targets. Active techniques include network scanning, host fingerprinting and vulnerability scanning. Unlike passive analysis, attackers are able to detect active analysis in the same way as defenders can detect attack traffic.

Multiple tools for active analysis exist. Many of these tools have overlapping functionality. Certain tools aim to perform specialised tasks such as network scanning, host fingerprinting and vulnerability identification. Three of the best known tools for these tasks are;

- nmap - a network scanning tool that allows attackers to map out network infrastructure, including the IP addresses of accessible hosts and the ports that are open on those hosts [12].
- p0f - a host fingerprinting tool. p0f is mostly used in conjunction with nmap to identify the Operating System and the applications running on scanned remote hosts. This is done through OS identification techniques along with Open Source intelligence [7].
- Nessus - a vulnerability scanner that is able to use the result of an nmap scan to perform vulnerability scans on remote hosts. A variety of information sources, including open ports and network application headers, are used to identify whether remote hosts are vulnerable to known attacks [13].

These tools have been used by attackers to identify weaknesses in target networks. Defenders have access to the same tools and are able to use them in response to attackers. This allows defenders to gain the same type of network intelligence that hostile attackers would be gathering about their networks.

4. Observe Orient Decide Act (OODA)

The different processes within the framework are divided into phases represented by the OODA loop. These phases model the operations performed on observed hostile network traffic, and also the decisions and actions that should be taken in response [15].

The OODA loop is conceptually applied to combat situations to better model, understand and reach a decision in response to some event. The OODA loop is used to illustrate the process of response to hostile network traffic. In the physical world, self-defence is seen as appropriate and proportional response to mitigate a threat targeting oneself or others. While the framework outlined in this section responds to events generated from hostile traffic, it does so in a non-aggressive manner. As a result, it would never attempt to exploit (or “strike-back”) at the source of hostile traffic in any capacity that could be considered malicious.

The *active* section of the framework is concerned with the collection of information regarding the hostile traffic and the source of the traffic. The information retrieved includes fingerprinting data such as Operating System, open ports/services, geolocation, ASN, traceroute data and DNS records. The hostile traffic would also be analysed through the use of traditional IDSs to determine the intent and type of attack. The collection and aggregation of this data represents the first steps towards mitigating a threat. This data could be submitted to a national CERT (Computer Emergency Response Team) or local law enforcement. In addition to out-of-band defence, a blacklist may be generated by the framework for passive defence.

The passive section of the framework is concerned with misdirection through the use of false information. During this process false information, such as DNS records and incorrect network topologies, are fed to an attacker.

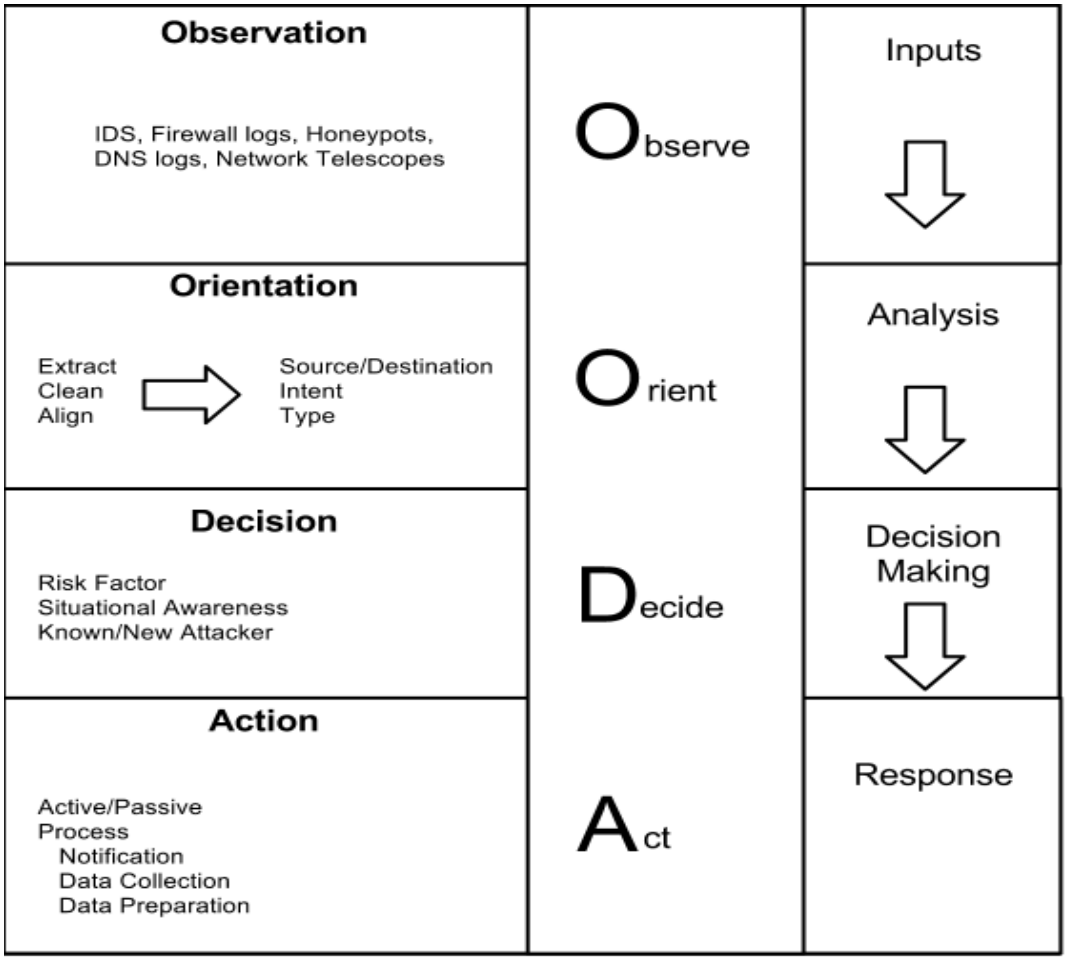

Figure 1: Proposed Processing for Non-Aggressive Response Framework

Bait-and-switch honeypots may also be deployed as a form of passive defence once an exploit has been detected. The remainder of this section will outline a framework for non-aggressive responses to hostile network traffic by aligning it to the phases adapted from the OODA loop. The proposed OODA framework is described in Figure 1 and explained in detail below.

4.1 Observe

The *observation* phase is concerned with determining the threat landscape. To achieve this aim the system makes use of multiple sensors to provide input. Data sources need to be configured in a manner that assists in accomplishing the pervasive network awareness detailed in Section 3. To this end existing sensory data infrastructure may be used to gain a greater awareness of activity on the network.

These data sources consist of, but are not limited to:

- Intrusion Detection Systems (IDS) alerts and logs
- Firewall logs
- Honeypot logs
- DNS logs
- Network Telescope data

The information obtained by these sensors needs to be aggregated to a central server for processing. This may be accomplished through the use of a messaging service such as AMPQ. This aggregation of data must be near-realtime to allow for relevant fingerprinting of the attacking host. The vast majority of hosts connected to the Internet make use of dynamic IP addresses that are leased from an Internet Service Provider (ISP). If the source IP address of an attack is not analysed nearly immediately after an event has occurred, the results of analysis may no longer be relevant.

4.2 Orient

Orientation should result in an understanding of the threat landscape being established. This may be reached through effective analysis of all input data obtained during the *Observe* phase. As discussed in Section 3, analysis can be either active or passive. The different analysis techniques each have strengths and weaknesses and are not exclusive in use, so should be combined to allow for holistic understanding to be reached.

Input data may be obtained from multiple sources and each source may represent sensor data in a different format. This heterogeneous representation of data means that data "cleaning" must take place in order to extract relevant information. The cleaning process should consist of data migration into common, well-organised and well-defined structure which will assist in the rapid extraction of related information. Relevant data that may be obtained from sensors include:

- Source and destination IP addresses
- Source and destination ports (service targeted)
- Traffic type (protocol)
- Inferred intent or attack type (through analysis or IDS signatures)
- Timestamps

Analysis of observed data will result in accurate information flow for the next step in the OODA framework, *Decide*.

4.3 Decide

The results from the *Analysis* phase are used as inputs for the decision-making process. Decision-making relies on the accuracy of observed data, so it can be seen that every phase of OODA relies upon the preceding phases.

During this phase a risk factor is calculated by assigning weights to the extracted categories. For example, a non-production web server may be assigned a relatively low value of 5 while more critical infrastructure such as a mail server would be assigned a high value of 8. These weights would be unique to each network being monitored as they take into account the value of operation objectives and critical infrastructure as determined by the entity that is monitored. The inferred intent or attack type could range from a 2 for network scanning to a 7 for a DoS attack. These weights would be added together to achieve a risk factor that it used in conjunction with pervasive network awareness to determine the action that should be taken in response.

The decision making phase is used to determine the severity of a threat, the threat's target and way in which a response should be formulated and executed.

A number of important data points will influence decision making, including data pertaining to the perceived threat, the state of the system's internal infrastructure and the currently available response mechanisms. After the risk factor has been calculated, the current availability of infrastructure is assessed. This includes ascertaining which services are currently running, such as backup services or redundancy mechanisms. At this point the threat is also categorized as either a new, never-before-seen threat or a previously-observed threat. For this to be achieved *priori* must be matched with the current event and the following information must be determined:

Has this IP, with its characteristics determined by fingerprinting, been seen in the past?

Has this pattern of attack been observed before?

Based on the answers to these questions, the risk factor is calculated. This, coupled with the current availability of responses and the state of the system infrastructure allows for a decision regarding the appropriate response action to be made.

Possible outputs from the *decision* phase include:

- Null routing traffic from the threat (this should be temporary: the traffic will only be null-routed for a predetermined period of time).
- Deploying a bait-and-switch honeypot and routing traffic from the attacker to it in order to further observe the attack and protect critical infrastructure.
- If the source IP address of hostile traffic is within an appropriate geographic jurisdiction and the attack is severe enough, data collected through the *Observation* and *Analysis* phases should be prepared as a report for the national CERT or local law enforcement.
- Raising an alert for human verification and interpretation of results. This allows for reliance on HUMINT for assistance in classification and decision making in ambiguous or unclear cases.
- Adding the attacker's source IP to a blacklist for immediate deployment (this is similar to the null routing response, but permanent).

4.4 Act

The final phase of the OODA framework results in an action being taken in response to all the information received from the preceding three phases. The type of action taken will depend on the outcome of the *decision* phase. Severity levels, based on the principles of risk management and mitigation, will be used to measure the required level of action to be taken.

The traditional response to network-based threats is to block all offending traffic. This proposed framework introduces passive and active responses. These responses, as determined by the *decision* phase of the framework, should be performed in a timely manner in order to reduce or completely mitigate any damage caused by attackers. The actions recommended by the decision phase are implemented during the action phase. These actions may include null routing, bait-and-switch honeypots and opening a case with local law enforcement.

A key area of the action phase is reporting. Reports should include detailed summaries of all information obtained during the preceding phases, along with all conclusions reached and the resulting suggested courses of action. Detailed reporting will assist in preparation for future attacks, as well as determining the effectiveness of the whole framework.

5. Conclusion

Modern networks are exposed to ever-increasing, persistent attacks. Traditional methods of defence against these attacks are failing, evidenced by the prevalence of Advanced Persistent Threats (APT) and an increase in monetary damage attributed to cybercrime. A framework for non-aggressive response to network threats is proposed in this paper. This framework is based on the OODA (Observe, Orient, Decide, Act) framework. Possible actions to be taken at each step of the OODA process are examined, with a feed-forward network being established where the output of each step is used as input to the subsequent step.

The proposed framework aims to provide both passive and active measures for identifying malicious network activity and to determine the appropriate responses based on the perceived threat. Through the implementation of this framework we hope to provide a means of better understanding the threats and sources of hostile traffic, while also providing a means of self-defence through measured non-aggressive responses.

References

[1] J. Boyd, "A discourse on winning and losing", Maxwell Air Force Base, Air University Library Document No. M-U 43947, 1987.

[2] D. Kennedy, Accessed 20120505, "Artillery 0.3 Alpha Released!" Available online at https://www.secmaniac.com/blog/2012/02/06/artillery-0-3-alpha-released/

[3] E. Talmans and B. Irwin. A framework for DNS based detection and mitigation of malware infections on a network. In ISSA. ISSA, Pretoria, South Africa, 2011.

[4] Forensic Focus, Accessed 20120505, “Passive network security analysis with networkminer.” Available online at http://www.forensicfocus.com/passive-network-security-analysis-networkminer

[5] Insecure.org, Accessed 20120505, Nmap. Available online at http://nmap.org

[6] J. V. Antrosio and E. W. Fulp, “Malware defense using network security authentication,”

in Proceedings of the Third IEEE International Workshop on Information Assurance, ser. IWIA ’05. Washington, DC, USA: IEEE Computer Society, pp. 43–54, 2005.

[7] M. Zalewski, Accessed 20120505, P0f. Available online at http://lcamtuf.coredump.cx/p0f3/

[8] Microsoft Corporation, Accessed 20120505, “Microsoft security intelligence report”, White paper, Available online at http://download.microsoft.com/download/C/9/A/C9A544AD-4150-43D3-80F7-4F1641EF910A/Microsoft_Security_Intelligence_Report_Volume_12_English.pdf

[9] Milken Institute, Accessed 20120505, “Currency of ideas insights from the institute.” Available online at http://www.milkeninstitute.org/newsroom/newsroom.taf?function=currencyofideas&blogID=462

[10] Network World, Accessed 20120505, “Sans survey: It spending too little time analyzing logs for security clues.” Available online at http://www.networkworld.com/news/2012/050312-sans-survey-258838.html?page=1

[11] S O. Hunter and B. Irwin. Tartarus: A honeypot based malware tracking and mitigation framework. In ISSA. ISSA, Pretoria, South Africa, 2011.

[12] Symantec Internet Security, Accessed 20120505, “Internet security threat report”, White paper, Available online at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

[13] Tenable Network Security, Accessed 20120505, Nessus. Available online at http://www.tenable.com/products/nessus

[14] Threat Level, Accessed 20120505, “Everyone has been hacked. now what?” [Online].

Available: http://www.wired.com/threatlevel/2012/05/everyone-hacked/all/1

[15] T. Liston , Accessed 20120505, “The tactical and strategic use of LaBrea.” Available online at http://www.mail-archive.com/leafuser@lists.sourceforge.net/msg01054.html.

A Prologue to Estimating the Intent of a Potential Rhino Poacher

Hildegarde Mouton, JP de Villiers
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
Electrical, Electronic, and Computer Engineering, University of Pretoria, Pretoria, South Africa
hmouton@csir.co.za
jdvilliers1@csir.co.za

Abstract: A dramatic increase in rhino poaching, if allowed to continue at current rates, is threatening South Africa's rhino population with extinction. The available detection and prevention systems are not sufficient in solving this crisis. Targets are detected, but their intent is unknown, thus a system is proposed that fuses the available data and infers a potential poacher's intent. A mixture of behaviour modelling and intent estimation, coupled with a suitable computational intelligence technique will address the problem of how to infer whether a person is a rhino poacher. This article sheds some light on the current systems that are in place and we offer a formulation of the rhino poacher problem in the Kruger National Park (KNP).

The proposed research is to model the terrain of the KNP, as well as the behaviour of rhinos and humans. A simple generic and high-level model will initially be used and the complexity adjusted as the project progresses. The model will be based on experience and observations of game rangers, park officials, South African Police Service (SAPS), South African National Defence Force (SANDF), and other groups that see to the safety of the animals of the KNP. Data will be generated with the model and used to train a chosen computational intelligence algorithm.

The contribution will be to show whether computational intelligence techniques can be effective in estimating the intent of potential rhino poachers in a statistical model of rhino poacher behaviour in the KNP. With the proper infrastructure this work could be used to provide decision support to park officials. This is extremely important for the rapidly waning rhino population in South Africa, as well as the rest of the world.

Keywords: intent estimation, computational intelligence, rhino poaching

1. Introduction

From January 2012 until 20 June 2012, a total of 251 rhinos have been poached in South Africa. Out of this 251, 149 rhinos were poached in the KNP [19]. Table 1 is courtesy of the South African Parks (SANParks) and shows a breakdown of the rhino poaching statistics for South Africa between 2010 and 20 June 2012.

A total of 147 poachers were arrested so far this year. This is encouraging, but the unfortunate fact is that the arrests were made after the rhinos were poached. It would be ideal to catch the poachers before they attack the rhinos.

The main reasons why rhinos are poached are trophy hunting and the believed medicinal purposes of their horns. In China (and recently also Vietnam) it is believed that ground rhino horn can cure many ailments, even cancer [5]. This has scientifically been proven to be untrue. In Yemen the horns are used for handles of daggers called “jambiya”, but China and Vietnam have overtaken Yemen as the driving forces behind rhino poaching.

According to [7], a “foot” poacher receives about R81,000 per rhino horn, whereas the sophisticated poacher who is part of a syndicate can receive an estimated R12,000 per kilogram. The only real risks involved for a poacher is that he can be shot by a law enforcement official or that he can be charged and receive a five year sentence, of which he will only serve a single year. When the risks are compared to the rewards, it is clear why there are so many poached rhinos in South Africa.

Table 1: Rhino poaching statistics for South Africa

South Africa	2010	2011	2012
Kruger National Park	146	252	149
MNP (SANParks)	0	6	3
Gauteng	15	9	0
Limpopo	52	74	36
Mpumalanga	17	31	9
North West	57	21	24
Eastern Cape	4	11	3
Free State	3	4	0
KwaZulu-Natal	38	34	26
Western Cape	0	6	1
Northern Cape	1	0	0
	333	448	251

Currently, almost three rhinos are poached every two days. At this rate, 2012's figures will be even higher than that of the 448 rhinos poached in 2011. This is a serious problem and if a solution is not found quickly, there might not be any rhinos left in the near future.

1.1 Literature

1.1.1 Rhino poaching

In his article *Rhino poaching in South Africa - Is it a losing battle?* [7], Eloff examines the spread of rhino poaching incidents in South Africa through the use of Geographic Information System (GIS) and remote sensing. Various spatial analytical techniques are combined with research to conceptualise the problem in twelve steps. The research for the project was done in the KNP from January 2010 until May 2010 when 71 rhinos were killed. From the 55 arrested perpetrators, 40% was found to be Mozambican citizens and 60% South African citizens. By sampling the ages of 22 of the perpetrators, it was found that they were mostly between 21 and 39 years old.

Statistical analysis revealed that there was no direct correlation between if it was raining or not during an attack. Temperature also did not seem to play a considerable role, so it was deduced that poachers do not have any preference when it comes to weather conditions. An interesting statistic that came to light, however, is the correlation between poaching and the phases of the moon. It seems that poachers prefer to attack during a lighter moon than a crescent (darker) moon. It was also found that most attacks occur in the southern part of the KNP and that the most popular days for attacks are Thursdays (22%) and Fridays (18.8%).

Eloff further states that "...addressing the rhino poaching problem in South Africa is a very complex task with an organised mesh of activities that involves the uneducated poor poacher from a rural village, professional individuals (vets, pilots, park officials) as well as corrupt public officials."

According to [13], the average rhino poacher is male, has paramilitary training, is an excellent marksman and tracker, operates both day and night and is poor (usually comes from rural areas). These characteristics could be used to infer the intent of potential poachers.

1.1.2 Border safeguarding

Border safeguarding has similarities to the problem of rhino poaching, as most rhino poachers either seem to come from bordering countries, or are South African citizens who smuggle rhino horns over

the border. Certain border safeguarding units have also been deployed in the KNP to apprehend poachers.

Operation Corona is the border safeguarding operation developed in partnership with the SANDF. “Border safeguarding is a Joint Command and Control (JC2) operation between the SANDF and SAPS. It deals with situations such as rhino poaching, smuggling of narcotics into South Africa, and transporting stolen goods and vehicles out and across the border.” [21].

From the available statistics it seems that nearly half of the poachers come from neighbouring countries [7] and use the KNP's border to enter South Africa [16]. According to Ken Maggs from SANPArks, 70% of rhino poaching in South Africa occurs in the KNP, with 70% of those poaching incidents occurring along the KNP's 4,000 km border with Mozambique [13]. The main reasons for the high percentage of poaching figures in the KNP is the fact that there is a large concentration rhinos roaming free, probably more than in any other part of the country, and the fact that the KNP shares a national border with Zimbabwe and Mozambique.

Border safeguarding falls under the heading of Operations Other Than War (OOTW) where the threats are civilians, unarmed, and not hostile. The aim is to apprehend threats, not kill them, and then to hand them over to the SAPS to be placed under arrest [21]. According to [20], OOTW can be defined as military missions that include a range of military skills for uses other than what the military skill set would normally be used for. “Such military missions could include border protection, peace support operations, counter crime, civil operations and disaster relief.” [20]

In 2003 the government announced that the SANDF would have to withdraw their border patrol operations from the border by March 2009 in favour of the SAPS [11]. This process was stopped in October 2009 and by mid-November 2009, the Cabinet said that the SANDF would once again be responsible for border control and protection [4]. Their first deployment took place in 2010. The deployment was to be incorporated by the Justice, Crime Prevention and Security (JCPS) cluster, which include the departments of Defence and Veterans, Correctional Services, Home Affairs, Justice, Police and State Security.

The SANDF cannot patrol the border in isolation [4], [17]. Border patrol in South Africa needs to be a cross-discipline effort. There is no SAPS exit and SANDF entry strategy and that leads to certain parts of the border not being patrolled, thereby creating blind spots, which in turn makes it easier for poachers to cross the border.

The border safeguarding operation consists of a five-year rollout plan, of which phases one to three have already concluded. In the first phase, four companies were deployed along the borders with two engineering troops in support to repair broken-down border fences. The second phase saw a further three companies deployed. The Mozambique borderline enjoys priority as they hold a specific threat to South Africa's rhinos. Phase three is currently in process and is deploying twelve sub-units. Phase four will see units being deployed along the rest of the border in April 2013. Phase five will see the deployment of additional units, bringing the total to 22 companies safeguarding the borders of South Africa [17].

1.1.3 Intent estimation

The potential application areas for intent estimation are numerous. Estimating the intent of an aircraft aids in the classification of airborne targets [3], [14], [18], as well as in the threat assessment of such aircraft [1]. The authors of [3] extend tracking and identification modelling to reduce the positional error by formulating a hybrid state space approach to deal with continuous-valued kinematics and discrete-valued target type, pose, and intent behaviour.

The authors of [14] use a hybrid model for intent estimation. According to the authors, data acquired in real-time suffer from two types of imperfection, namely vagueness and ambiguity. The design of a hybrid system is explored that processes both these types of imperfections by integrating fuzzy (vague) and probabilistic (ambiguous) data types. Fuzzy logic is used for the vague data, and Bayesian networks are used for the ambiguous data. The model explores the representative transformation methods between probability and possibility.

In [18], the author proposes that the intent of possible threat aircraft be estimated by modelling a Command and Control (C2) simulation system using Agent Based Modelling to capture human interactions. It is further proposed that this can be implemented as a sense-making tool, whereby the enemy C2 process is modelled and simulated to be used in estimating a set of planned actions.

Intent estimation is also of utmost importance in the maritime environment where pirating and poaching are of great concern. The author of [10] presents an algorithm that provides Unmanned Undersea Vehicles (UUVs) with the ability to estimate the intent of the targets it is observing. A probabilistic model of the target's possible intents is developed and used to estimate the target's real intent. The results from the algorithm are used to analyse the target's observed path to detect objects. The values are logged in an obstacle inference map, which incorporates the results from the analysis of any number of observed paths from multiple targets. Bayesian updating and the forward-backward approach are used in developing the algorithms.

1.2 A roadmap of the article

In Section 2 we take a look at the current systems that are in place in the KNP and Section 3 gives an overview of the proposed system. Section 3.1 discusses the modelling of the problem while Section 3.2 presents the conceptual model. Section 3.3 deals with the feature selection issue and Section 3.4 discusses the training and testing of the algorithm. Section 3.5 ends the discussion of the high-level system with a few words on model complexity and the paper concludes with Section 4.

2. Current systems in place

The current systems that are in place for the detection of poachers and the safeguarding of the animals are mostly human observations in the form of rhino sightings. For instance, a game ranger would say that he saw a certain rhino at a certain position in the park at a certain time. Different sightings can be fused to form a track of where the rhino was and where it is headed. Potential poachers can also be sighted and identified as such.

These systems are, however, not sufficient in solving the rhino poaching crisis. The biggest problem with rhino poaching is in the KNP, which is where we will concentrate our efforts.

Currently there does not seem to be a way to fuse these human observations to form a situation picture. What we propose is a system that fuses different sources of data to infer the potential poacher's intent. This is the topic of the next section.

3. Proposed high-level system

We propose an integrated system based on a statistical graphical model that fuses the available data and infers a potential poacher's intent. A mixture of behaviour modelling and intent estimation, combined with a suitable computational intelligence technique will address the problem of how to infer whether a person is a rhino poacher.

A simple generic and high-level model will initially be used and the complexity will be adjusted as the project progresses. The model will be based on experience and observations of game rangers, the police, SAPS, SANDF, *etcetera*. Data will be generated from the model and will be used to train a computational intelligence algorithm.

3.1 Modelling the problem

The terrain of the KNP will be modelled with care taken to include points of interest such as mountains, dense patches of trees, rivers, watering holes, foot paths, and roads. The importance of these points of interest is that poachers will most probably use them to their advantage. For instance, it would be more difficult to detect a potential poacher if he is hiding in mountainous areas or areas where the trees are very dense. Rivers and watering holes will also be popular locations for rhinos, thus increasing the chance for them to be poached. Footpaths and roads are also important in the sense that that is the only places where persons travelling on foot or in a vehicle are allowed to be. If we suddenly detect someone moving in a certain area and we know that there are no footpaths or roads, it is likely that we have detected a poacher.

The behaviour and movement of rhinos and humans will also be modelled. Humans and animals behave differently as they have different motivations and goals. According to [8], there are three products that make up a person's behaviour: motivation, ability and triggers. For a person to exhibit a certain type of behaviour, he/she must be motivated, have the ability to perform the behaviour and experience a trigger to perform this behaviour. Furthermore these three products have to happen at the same time. Humans also behave differently in different situations. There will have to be distinguished between “normal” human behaviour and “poacher” behaviour.

Animals do not behave in the same way as humans, thus there will have to be a separate model for the behaviour of the rhinos. For instance, Folse *et al* [9] uses “object-oriented programming, dynamic linkages, rule-based decision procedures, and several concepts from the field of Artificial Intelligence (AI) for modelling animal movements in a heterogeneous habitat.”

To model the movements of a rhino, one of the first tasks will be to create a probability density surface that describes the spatial distribution of the rhino's location [6]. This is called a *home range*. Our aim with this is to reveal ways in which the rhinos use complex and changing environments [12]. Rhinos will move in a specific manner and visit the same locations. Variations in this behaviour could indicate the proximity of a poacher. We will have to distinguish between “normal” rhino behaviour and “threatened” rhino behaviour. Just as humans behave differently when in danger, rhinos will have different movement patterns when they feel they are being threatened.

We will also have to decide whether to model rhinos in a group or as individuals. This will depend on the movement and behaviour of the rhinos: do they move in herds, do they move two-by-two or do they move alone? If rhinos are modelled collectively, a group of rhinos' behaviour can be seen as a result of individuals following the same set of behaviour rules and can thus be modelled by mathematical equations. A proposed method to model the distribution of the rhinos' positions is to use a Gaussian mixture model. A Gaussian mixture model is a linear superposition of a number of Gaussians formulated as a probabilistic model [2]. The means and covariance of the different Gaussians as well as the weights of the superposition (mixing coefficients) are parameters that can all be determined as part of the learning process.

3.2 A conceptual model

Figure 1 illustrates the conceptual model for the rhino poacher problem. The model is shown in plate notation, which is a more compact way of representing graphical models [2]. The plate (the big box labelled *N*) represents the *N* targets of which only a single example is shown explicitly. The smaller plate labelled *K* denotes the *K* time steps.

The *Class* random variable determines all the features and motion properties of the target of which there are *N* copies. Examples of *Class* include “poacher”, “game ranger”, “tourist”, “rhino”, and “other animals”. The variables indicated by $a_1 – a_L$ represent attributes of the targets. These variables will be dependent on the class and may include the shape of the target, the weight of the target, the size of the target, *etcetera*. They are observed through attribute observations $y^{a1} – y^{aL}$. These may include infrared signatures of the target, visual images, radar imagery and radio-collar signals. The variables $p_1 – p_M$ represent motion parameters and are dependent on the target class. For example, the movement of a rhino will be different than the movement of another animal or human being. Examples include maximum speed, movement patterns and other kinematic properties. These influence the actual motion model of the target, which is a hidden Markov model, detailed in Figure 2. This model simply implies that the state vector of the target is dependent on the target state vector of the previous discrete time step (a discrete time model is assumed here). The target motion is observed through the variable y_k, which are the positions, and possibly velocities, of the target for all time steps until the current time step.

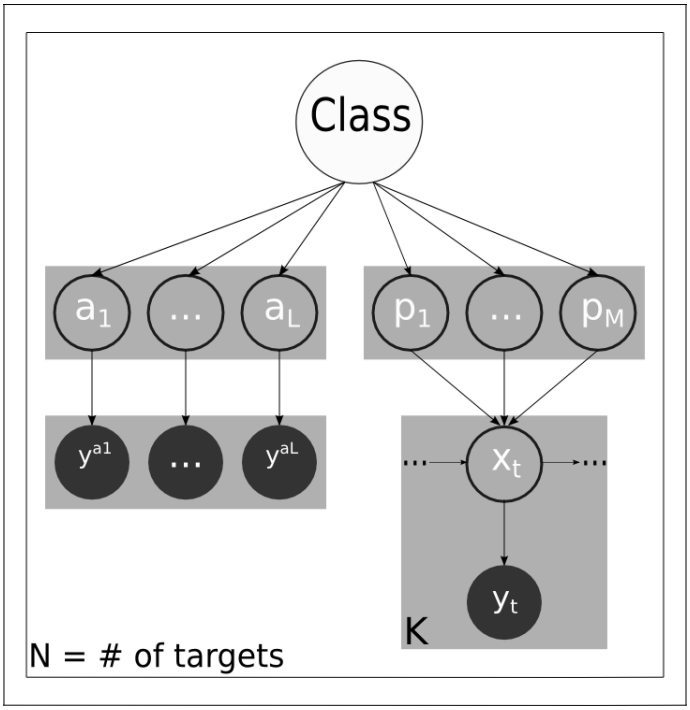

Figure 1: Conceptual model of the rhino poacher problem

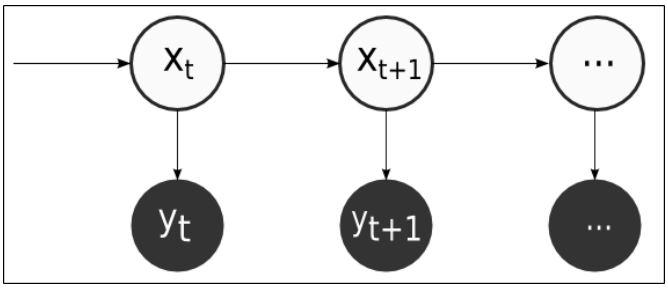

Figure 2: Target state vector as a hidden Markov model

3.3 Feature selection

A significant part of the problem is to decide which features are relevant to make decisions regarding the intent of a potential poacher. Some of these features have already been stated, such as the positions of the humans. Are they on a footpath, are they on a road or are they in the middle of a dense patch of trees far away from any roads? Are the human tracks in a restricted area? Human tracks in a restricted area could mean that we are detecting a game ranger or a park official, it can mean that some tourists got lost, or it could be a poacher.

We can also examine previous poaching locations in order to calculate a poaching pattern and try to understand which features are relevant to poachers in selecting a poaching location.

Other features that can be considered are time of the day, day of the week, weather conditions (although we know that according to [7] poachers do not favour certain weather conditions above others), and moon phases (according to [7] poachers favour a lighter moon).

3.4 Training and testing the algorithm

At this stage we will have models for the KNP's terrain, rhino behaviour and human behaviour. These models will then be used to generate data to train our chosen generative model machine learning algorithm. A *generative model* is an approach where the underlying distributions of the classes are modelled. By sampling them, synthetic data points can be generated in the input space [2]. The other

approach in machine learning is to use *discriminative techniques* that only focus on learning the class boundaries [15].

We will generate positions and tracks of rhinos, as well as positions and tracks of humans. We will generate tracks for game rangers and park officials as well as tourists and poachers since these groups will all have different movement patterns.

After training the algorithm we will test the system on real world data. The real world data will mostly be the positions of rhinos and humans (position and time of observation). The goal is to fuse the data and obtain a situation picture before inferring the intent of the potential rhino poacher.

3.5 Model complexity

A simplified statistical model of the rhino poaching problem and of rhino poacher behaviour will be used. We will base our model on experience and observations of game rangers, park officials, SAPS and SANDF, and any other data that might be available at the time. The model might not work as expected at the start, as it is a simplified statistical version of the problem, but it will capture the core of the problem.

4. Conclusion

In this article we highlight the importance of protecting the rhino population of South Africa and we show that the biggest number of rhino poaching occurs in the KNP. The current methods of detection and protection are not adequate and we propose a new integrated system for fusing available data to make inferences concerning potential poachers. The conceptual model is also introduced.

The aim of this project is twofold. We aim to show that computational intelligence techniques can be used to effectively estimate the intent of potential rhino poachers in a statistical model of rhino poacher behaviour in the KNP. We also aim to provide decision support for park officials and hopefully put a stop to the increasing number of savage attacks on rhinos.

References

[1] A. Benavoli, B. Ristic, A. Farina, M. Oxenham, and L. Chisci, “An Approach to Threat Assessment Based on Evidential Networks,” in *10th International Conference on Information Fusion*, 2007.

[2] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer, 2006, pp. 1-738.

[3] E. Blasch, “Modeling Intent for a Target Tracking and Identification Scenario,” in *SPIE*, 2004, vol. 5428, no. April 2004.

[4] H. Boshoff, “SA Police Roles and Responsibilities: Border Environment,” in *Border Control*, 2011.

[5] R. Cota-Larson, “Revealed: China’s ‘Rhino Horn Cancer Treatment’ Scheme,” *www.rhinoconservation.org*, 2012, Accessed 20120703. Available online at http://www.rhinoconservation.org/2012/01/26/revealed-chinas-rhino-horn-cancer-treatment-scheme/.

[6] J. Downs and M. W. Horner, “Analysing infrequently sampled animal tracking data by incorporating generalized movement trajectories with kernel density estimation,” *Computers, Environment and Urban Systems*, pp. 1-9, Jan. 2012.

[7] C. Eloff, “Rhino poaching in South Africa -– Is it a losing battle?,” *PositionIT*, pp. 57-61, 2012.

[8] B. Fogg, “A behavior model for persuasive design,” in *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive ’09*, 2009, pp. 40:1-40:7.

[9] L. J. Folse, J. M. Packard, and W. E. Grant, “AI Modelling of Animal Movements in a Heterogeneous Habitat,” *Ecological Modelling*, vol. 46, pp. 57-72, 1989.

[10] E. H. L. Fong, “Maritime Intent Estimation and the Detection of Unknown Obstacles,” 2004.

[11] K. Geldenhuys, “South African Borders - The Army is Back,” *Servamus - Safety and Security Magazine*, no. December 2011, pp. 2011-2013, 2011.

[12] E. Gurarie, R. D. Andrews, and K. L. Laidre, “A novel method for identifying behavioural changes in animal movement data,” *Ecology Letters*, vol. 12, no. 5, pp. 395-408, 2009.

[13] G. Hoskin, “Major boost in resources to fight poachers,” *IOL*, 2011.

[14] K. Lee and J. Llinas, “Hybrid model for intent estimation,” in *Proc. 6th Int. Conf. Information Fusion*, 2003, pp. 1215-1222.

[15] J. Lester, T. Choudhury, N. Kern, G. Borriello, and B. Hannaford, “A Hybrid Discriminative/Generative Approach for Modeling Human Activities,” in *Proceedings of the 19th international joint conference on Artificial intelligence*, 2005, pp. 766-772.

[16] R. Maota, “More soldiers patrol borders,” *MediaClubSouthAfrica.com*, 2012.

[17] G. Martin, “Border security is now a national priority, SANDF says,” *defenceWeb*, 2011.

[18] R. Oosthuizen, “MSDS EDERI Threat Intent Estimation in JAD Operations (SAJADS 2011),” pp. 1-17, 2011.

[19] SANParks, “Media Release: Latest statistics on rhino poaching,” *Media Release*, 2012, Accessed 20120703. Available online at http://www.sanparks.org/about/news/default.php?id=55203.

[20] C. J. Smith, “From Close Air Support to Joint Operations Other Than War,” in *South African Joint Air Defence Symposium*, 2011.

[21] S. Van Rooyen and L. Leenen, “Developing a Simulation for Border Safeguarding,” in *South African Joint Air Defence Symposium*, 2011.

Authors' Biographies

The following biographies are in alphabetical order of the surname.

Naas Bester was born in 1981, and grew up in small town called Fochville. He completed his engineering degree in 2005 and completed basic training under reserve forces, Pretoria Tank Regiment while he was a student. He has always been interested in security and information fusion. He is currently enrolled for an Honours degree and intends to register for a Master's degree.

Ivan Burke is a MSc student in the department of Computer Science at the University of Pretoria, South Africa. He currently works full time at the Council of Scientific and Industrial Research South Africa in the Defence, Peace, Safety, and Security unit, where he works within the Command, Control and Information Warfare competency area.

Dr JP de Villiers obtained his PhD from the University of Cambridge and holds a post as Extraordinary Senior Lecturer at the University of Pretoria's Electronic Engineering department. He is currently working at the Radar Applications Group of the CSIR and specializes in data fusion.

Dr Warren du Plessis received the B.Eng. (Electronic), M.Eng. (Electronic) and Ph.D. (Engineering) degrees from the University of Pretoria in 1998, 2003 and 2010 respectively, winning numerous academic awards including the prestigious Vice-Chancellor and Principal's Medal. He spent two years as a lecturer at the University of Pretoria, and then joined Grintek Antennas (since split between Poynting Antennas and Saab EDS) as a design engineer for almost four years. Since 2006, he has been working in electronic warfare (EW) at Defence, Peace, Safety and Security (DPSS), a division of the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa. His primary research interests are cross-eye jamming, and thinned and sparse antenna arrays.

Prof Marthie Grobler has been working as a Cyber Security Researcher at the Council for Scientific and Industrial Research (CSIR) since January 2008. She has a PhD Computer Science (Live Digital Forensics), and an MSc in Computer Science (Information Security Governance), both from the University of Johannesburg. Her research focus is on cyber security awareness, digital evidence and standardisation, strategic data management and information security research in general. Marthie represents CSIR DPSS on ISO/IEC JTC 1 SC 27 71F and is the national convenor of SABS SC 71F Workgroup 4 (Security Controls and Services). She is co-editor of ISO/IEC 27037. Marthie is an ISACA Certified Information Security Manager and is appointed as a visiting Professor at the University of Johannesburg, Academy for Computer Science and Software Engineering. She is Managing Editor of the Journal of Contemporary Management.

Mr Samuel Hunter received his Bachelors of Science Honours degree in 2011 from Rhodes University. He is presently in his second year of study towards his Master of Science degree. Samuel is part of the Security and Networks Research Group at Rhodes University and is supervised by DR Barry Irwin. His research interests include device fingerprinting, host tracking and offensive network security. His current research focuses on remote fingerprinting, tracking and visualization of potentially malicious hosts in dynamic IP address space.

Dr Barry Irwin holds a PhD in computer science. He currently heads the Security and Networks Research Group (SNRG) within the department of Computer Science at Rhodes University. His research interests include low level traffic analysis, data visualization and anti-phishing.

Mr Francois Maasdorp received his B.Eng (electronics), 2001 and his M.Eng (cum laude), 2008 from the University of Pretoria, South Africa. He was employed at the University of Pretoria from 2003 to 2005 where he lectured undergraduate courses in Digital Communications and Linear System Analysis. Since 2006, he has been working in electronic warfare (EW) within the Council for Scientific and Industrial Research (CSIR). His research interest is Communications EW, Passive Coherent Location, Modeling and Simulation and Signal processing.

Prof Manoj Maharaj (PhD) is currently Associate Professor at the University of KwaZulu-Natal, where he teaches information systems, specializing in information systems strategy and information security. He has supervised numerous post-graduate students from throughout Africa, at the Masters, MBA, DBA, and PhD levels. He has consulted widely in the IT industry and presented workshops on topics ranging from IT Auditing, IT strategy, Information Security, Risk Management and others.

Ms Mercia Malan is a software developer at Dariel Solutions where she works on business systems. Mercia completed her BSc - Information Technology and Music degree at University of Pretoria at the end of 2011. She is currently busy with her honours degree in the department of Computer Science at the University of Pretoria, South Africa.

Mr Francois Mouton is a PhD student in the department of Computer Science at the University of Pretoria, South Africa. He also works full time at the Council of Scientific and Industrial Research South Africa in the department of Defence Peace Safety and Security, where he works within the Command, Control and Information Warfare research group.

Miss Hildegarde Mouton is working on her PhD at the CSIR's Command, Control, and Information Warfare competency area. After completing her Masters degree in Applied Mathematics at the University of Stellenbosch, she joined the CSIR and the University of Pretoria's Electronic Engineering department where she is part of the Intelligent Systems Group (ISG).

Mr John Richter is a lecturer in the computer science department of Rhodes University, with an interest in Information Security, network simulation, Internet worms and the development of autonomous software. His research spans the fields of artificial intelligence, behavioral emergence and Worm simulation.

Mr Jaco Robertson has been working as a Cyber Security Researcher at the Council for Scientific and Industrial Research (CSIR) since April 2007. He has a BSc (Computer Science, Applied Mathematics) from the University of the Free State and a BSc Hons (Computer Science) from the Randse Afrikaanse Universiteit. He worked for nine years as a Software Engineer in the Telecommunications Industry.

Mr Adam Schoeman holds both CISSP and CISA certification. He is a member of the Security and Networks Research Group (SNRG) within the department of Computer Science at Rhodes University, where he is working toward his Master's Degree. His research interests include low interaction detection systems and procedural information security.

Mr Etienne Stalmans is currently in his 2nd year of an MSc Computer Science degree at Rhodes University in South Africa. His work falls under the banner of the Security and Networks Research Group (SNRG) supervised by Dr Barry Irwin. Focusing on network security and primarily on botnet detection, mitigation and remediation, his research aims to apply new and novel techniques to the problems faced in network security. Work done in epidemiology, animal and plant dispersion and lexical analysis are all incorporated into his research. He presented his work in Fast-Flux domain detection at ISSA 2011, where he received the best paper award. He also presented at SATNAC 2011 and BSides Cape Town 2011, where his work was awarded the prize for local information security research.

Jacques Théron is a Lieutenant Colonel in the South African National Defence Force (SANDF). For 17 years he was employed as an Intelligence officer in the operational environment at various units within the SANDF. He then was involved in the electronic collection environment at Defence Intelligence with focus on electronic intelligence analysis and Electronic Warfare for seven years. For the past four years he is staffed at Directorate Information Warfare (DIW) within Command Management Information System Division (CMIS Div). He is currently responsible for Information Based-processing Warfare (IBW) as well as Command and Control warfare (C^2W).

Mr Renier van Heerden is a senior researcher at Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa in the field of Information Warfare and Cyber Defence. Prior to joining the CSIR he worked as a software engineer in advanced optics applications for South African based

Denel Optronics and as a Lecturer at the University of Pretoria. Renier obtained a degree in Electronic Engineering and a Masters in Computer Engineering at the University of Pretoria and is currently registered for a PhD at the University of Rhodes.

Dr Brett van Niekerk completed his B.Sc. in Electronic Engineering, and graduated with a M.Sc. Electronic Engineering at the University of KwaZulu-Natal in 2006. He worked at ThoroughTec Simulation on mining and military projects, and managed the Electronic Design Department. He joined the School of Information Systems and Technology at the University of KwaZulu-Natal in 2009. He completed his PhD in 2012, analysing vulnerabilities in modern communication technologies and infrastructures from information warfare and electronic warfare perspectives. He is currently a Postdoctoral research scholar at UKZN.

Ms Namosha Veerasamy has obtained a BSc: IT Computer Science Degree and both a BSc: Computer Science (Honours Degree) and MSc: Computer Science with distinction from the University of Pretoria. In 2005 she joined the Council for Scientific and Industrial Research (CSIR) in Pretoria and now works as a senior researcher. Her research focus is directed at cyber security; including network perimeter defence, threat modelling and security awareness. Namosha is also qualified as a Certified Information System Security Professional (CISSP) as well as an ISACA Certified Information Security Manager.

Prof. SH (Basie) von Solms is a Research Professor in the Academy for Information Technology of the University of Johannesburg. He obtained his PhD in Computer Science at the University of Johannesburg (previously the Rand Afrikaans University) and has been lecturing Computer Science and IT at this University since 1 October 1970. Basie specialises in research and consultancy in the area of Information Security, Cyber Security and Critical Information Infrastructures, and is on the Editorial Board of the International Journal of Critical Infrastructure Protection. Prof von Solms has also served as the President of IFIP, the International Federation for Information Processing (www.ifip.org).

Organising Committee Biographies

The following biographies are in alphabetical order of the surname.

Ms Zama I. Dlamini completed both her Undergraduate and Honours Degrees in Computer Science, at the University of Zululand, South Africa. She is currently pursuing her MSc in Network Forensics with the University of Pretoria. Zama works as Cyber Security Specialist and Researcher at CSIR-DPSS (Cyber Defence Research Group), since 2008 to date.

Prof Marthie Grobler has been working as a Cyber Security Researcher at the Council for Scientific and Industrial Research (CSIR) since January 2008. She has a PhD Computer Science (Live Digital Forensics), and a MSc Computer Science (Information Security Governance), both from the University of Johannesburg. Her research focus is on cyber security awareness, digital evidence and standardisation, strategic data management and information security research in general. Marthie represents CSIR DPSS on ISO/IEC JTC 1 SC 27 71F and is the national convenor of SABS SC 71F Workgroup 4 (Security Controls and Services). She is co-editor of ISO/IEC 27037. Marthie is an ISACA Certified Information Security Manager and is appointed as a visiting Professor at the University of Johannesburg, Academy for Computer Science and Software Engineering. She is Managing Editor of the Journal of Contemporary Management.

Dr Louise Leenen has been working as a Senior Researcher at the Council for Scientific and Industrial Research (CSIR) since October 2007. She holds a PhD Computer Science (Constraint Programming) from the University of Wollongong in Australia, and a MSc Computer Science (Operations Research) from the University of Johannesburg. Louise has 18 years of teaching experience lecturing to students in Computer Science and Informatics at universities in South Africa and Australia. Her research focus is on artificial intelligence applications in the defence environment and ontology development.

Prof. Manoj Maharaj (PhD) is currently Associate Professor at the University of KwaZulu-Natal, where he teaches information systems, specializing in information systems strategy and information security. He has supervised numerous post-graduate students from throughout Africa, at the Masters, MBA, DBA, and PhD levels. He has consulted widely in the IT industry and presented workshops on topics ranging from IT Auditing, IT strategy, Information Security, Risk Management and others.

Dr Jackie Phahlamohlaka completed an MSc in Computational and Applied Mathematics at Dalhousie University in Canada and a PhD in Informatics from the University of Pretoria. He currently is Competency Area Manager at the Council for Scientific and Industrial Research (CSIR), South Africa. He has more than 50 publications in national and international conferences, book chapters and journals. He supervised well over 20 honours and 10 Masters students. His first PhD student successfully defended his PhD thesis and graduated in September 2010 at the University of Pretoria. Apart from his research and managerial activities, he has been a central figure in a very successful rural community educational project, the Siyabuswa Educational Improvement and Development Trust (SEIDET), since 1990. He is a member of the South African National Committee for the International Federation for Information Processing (IFIP). In September 2010, he was elected as the International Chairperson of TC9 of IFIP. He is the CSIR designated representative on the Council of the University of Venda, where he also serves in the Senate and the Academic Planning Committee of the University. His research interests are in ICT and Socio-Economic Development, Web-based Group Support Systems, and most recently, Broadband access and National Security.

Ms Trishana Ramluckan completed her B.A. majoring in Politics, Legal Studies and Classics at the University of Natal, where she went on to complete her Honours degree. She then graduated with her M.A. from the University of KwaZulu-Natal in 2006. She is a Researcher and Lecturer at the Management College of South Africa, where she co-ordinates the information systems courses. She is currently doing her PhD research, focussing on the roles of social media in crisis management and communications.

Dr Brett van Niekerk completed his B.Sc. in Electronic Engineering, and graduated with a M.Sc. Electronic Engineering at the University of KwaZulu-Natal in 2006. He worked at ThoroughTec Simulation on mining and military projects, and managed the Electronic Design Department. He joined the School of Information Systems and Technology at the University of KwaZulu-Natal in 2009. He completed his PhD in 2012, analysing vulnerabilities in modern communication technologies and infrastructures from information warfare and electronic warfare perspectives. He is currently a Postdoctoral research scholar at UKZN.

Mrs Joey Jansen van Vuuren is the Research Group Leader for Cyber Defence at the CSIR, South Africa. This research group is mainly involved in research for the SANDF and Government sectors. Her research is focused around national security and the analysis of Cyber threads using non quantitative modelling techniques. She is also actively involved in facilitating Cyber awareness programs in South Africa. She is currently studying towards a PhD in Cyber security policy implementation.

Review Panel

Johann Amsenga	International Council of System Engineering
Elmarie Biermann	Infobahn
Ivan Burke	Council for Scientific and Industrial Research
Alta de Waal	Council for Scientific and Industrial Research
Mariki Eloff	University of South Africa
Stephen Flowerday	University of Fort Hare
Aurona Gerber	Council for Scientific and Industrial Research
Marthie Grobler	Council for Scientific and Industrial Research
Hennie Harris	Council for Scientific and Industrial Research
Rut Laubscher	Military Academy
Herman le Roux	Council for Scientific and Industrial Research
Louise Leenen	Council for Scientific and Industrial Research
Manoj Maharaj	University of KwaZulu-Natal
Mathias Mujinga	University of South Africa
Martin Olivier	University of Pretoria
Jackie Phahlamohlaka	Council for Scientific and Industrial Research
Trishana Ramluckan	University of KwaZulu-Natal and MANCOSA
Jan Roodt	StoneToStars Limited
Mogie Subban	University of KwaZulu-Natal
Ignus Swart	Council for Scientific and Industrial Research
Renier van Heerden	Council for Scientific and Industrial Research
Brett van Niekerk	University of KwaZulu-Natal
Joey Jansen van Vuuren	Council for Scientific and Industrial Research
Cobus Venter	Council for Scientific and Industrial Research

UNIVERSITY OF
KWAZULU-NATAL
INYUVESI
YAKWAZULU-NATALI

The Premier University
of African Scholarship

CSIR
our future through science