Motivation and Requirements for Determining a Network Warfare Capability

N Veerasamy and JHP Eloff
University of Pretoria, Pretoria, South Africa
nveerasamy@csir.co.za

Abstract:. (300-500 words)

Keywords:

Computers and networks have provided for increased connectivity, ease of use and convenience. Other advantages include the ability to communicate across borders, have access to information at your fingertips and the huge capacity for storage and transport. However, there also arises the need to properly protect these vital resources. At a computer security level, there exists the underworld community of hackers and crackers who seek to cause damage. From a military point of view, offensive actions are part of the warfare mode of operation. Thus, the attack, together with the protection of information, can take place for various reasons ranging from recreational pastimes, to skilful challenges, as well as military requirements.

Networks and cyberspace have become the battleground as attacks are launched to disrupt, destroy or deny access to valuable resources. Network Warfare can thus be seen as the branch of Information Warfare that deals with the utlisation of Information and Communication Technology (ICT) to carry out various exploits of information, as well as the various defensive mechanisms that are deployed in order protect information against attack.

Individual users and organisations need to be warned about the latest face of warfare that is not only being played out in the military networks, but also on the Internet and cyberspace. Consequently, Network Warfare has various facets which are often difficult to distinguish between. This paper builds on the field of Network Warfare and contains the motivation for determining a Network Warfare Capability.

The motivation and requirements for determining a Network Warfare Capability are explored in this paper. This helps to recognise important considerations for determining a Network Warfare Capability. Some of the requirements are intricate and required further discussion. The extended discussion served to describe some of the requirements in greater detail. A noteworthy requirement of portraying offensive and defensive techniques is elaborated on through the use of UML diagrams.

This paper, thus describes the importance of determining a Network Warfare Capability and serves as an introduction to future work in which a model to determine a Network Warfare Capability is proposed.

Keywords: Network Warfare Capability, offensive, defensive

1. Introduction

Technological advancement has led to the development of fast and reliable information processing and storage capabilities. According to the United States Defense Science Board, the 20th century has seen technological advances that have radically changed how people interact, what machines can perform and have shown that the dependency on information has revolutionised day-to-day activities (2007). Today, computers and networks are critical tools for many daily operations involving information, as they are used for a myriad of tasks that range from word processing to entertainment. Critical infrastructure, like the public telephone networks, banking, finance industry and other vital services, are dependant on information technology for their day-to-day operation (Panda, Giordano 1999).

A report by the Defense Science Board in the United States of America (USA) explains that challenges in the present age include information assurance, and that this requires new security frameworks and thinking (2007). One emerging area, in which information security lies at the heart of it, is Information Warfare. Information Warfare is a modern type of conflict in which organisations try to secure their own resources and thus prevent adversaries from

denying and exploiting information that would otherwise minimise capabilities. Information Warfare at its simplest level is the use of computers to attack the information infrastructure of an adversary while protecting one's own information infrastructure (Elbirt 2003-2004). In this way, Information Warfare focuses on how best to undermine the information and facilities of the enemy while maintaining the protection of one's own resources.

Networks have now become the battleground for various forms of attacks as vicious users attempt to deny and exploit networked resources. Network Warfare is thus a form of Information Warfare in which the connectivity provided by networks is used to carry out exploits on information. The examples of Munro of modern day Network Warfare includes computerised mishaps, air traffic control breakdowns, electronic bank-robberies, haywire flight control systems, phone outages, AOL crashes and KGB-sponsored computer spying (1996).

This paper builds on the field of Network Warfare and contains the motivation for determining a Network Warfare Capability. Previous investigations were carried out in preparation for clarifying the field of Network Warfare.

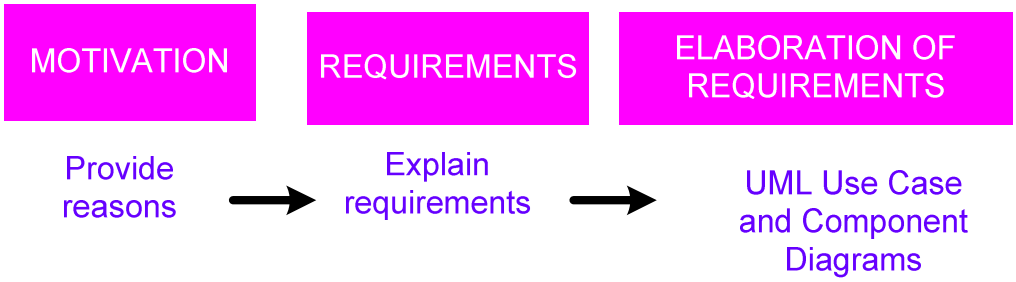

Figure 1: Outline of Paper

Figure 1 shows a outline of the paper. Firstly, the motivation and requirements for determining a Network Warfare Capability are explained in this paper. This helps to recognise important considerations for determining a Network Warfare Capability. Some of the requirements are intricate and required further discussion. The discussion served to describe some of the requirements in greater detail. A noteworthy requirement of portraying offensive and defensive techniques is elaborated on through the use of UML diagrams.

This paper thus describes the importance of determining a Network Warfare Capability and serves as an introduction to future work which a model to determine a Network Warfare Capability is proposed.

2. Motivation

This section looks at providing various reasons for determining a Network Warfare Capability and addresses the underlying motivating factors that drive the determination of a Network Warfare Capability.

It is the belief of the authors that Network Warfare is an abstract idea that consists of various information security techniques. Many aspects in the Network Warfare domain are conceptual and, while the definition and attributes can be encompassed in simple statements, the interactions of the various techniques are complex. To ensure that Network Warfare is represented in a comprehensive and holistic way, it is important to determine a Network Warfare Capability that takes into consideration these various interrelated techniques.

Determining a Network Warfare Capability provides the opportunity to gauge whether a group can respond to or recover from vulnerabilities, threats or other imminent dangers. A Network Warfare Capability indicates the readiness and strength of an organisation to prevent, detect, react to and even execute Network Warfare attacks. An underlying problem is, therefore, how does one determine a Network Warfare Capability? Determining a Network Warfare

Capability is a complex, and, as yet, unresolved problem. This has led the author to search for techniques that have the potential to model this complex field.

Furthermore, network security could be mistaken for Network Warfare. However, the distinction between network security and Network Warfare lies in the development of both offensive and defensive techniques. One motive serves to damage or interfere with operations, while the other aspect looks at protecting the resources and maintaining integrity and availability. Computer and network security spans information security and, while information security has traditionally focused on defensive strategies, a Network Warfare Capability encompasses both aspects.

According to Park and Ruighaver, information security strategy has been seen as the co-coordinated deployment of appropriate defensive information security technologies and measures to protect the information infrastructure of an organisation against threats- both internally and externally (Park, Ruighaver 2008). However, from a South African National Defence Force perspective, defensive Network Warfare looks at all activities relating to the protection of information systems, and offensive Network Warfare addresses all activities resulting in the destruction of foreign information or network systems (Williers et al. 2005/06).Thus, determining a Network Warfare Capability would cover more aspects than looking at network security alone, in that both offensive and defensive aspects would be addressed.

3. Requirements

The previous section provided a motivation for determining a Network Warfare Capability. The findings also raised some important considerations when determining a Network Warfare Capability. Provided next is, therefore, a list and an explanation of the requirements that necessitate determining a Network Warfare Capability that stem from investigating Network Warfare:

- Network Warfare needs to be represented holistically and as many aspects as possible should be covered. However, due to the complexity of Network Warfare there is a need to operate at a certain high-level of abstraction and not focus on very intricate details.
- While both offensive and defensive techniques will need to be evaluated, offensive techniques are mainly applicable to the domain of the military and, therefore, this determination of a Network Warfare Capability is more suitable in this field. However, if an organisation, for example a research institution, has the mandate to carry out offensive Network Warfare techniques, the determination of a Network Warfare Capability will be equally applicable.

Furthermore, additional requirements also arise. These requirements depict additional considerations that will influence the way in which the Network Warfare Capability will be interpreted. These requirements are important to prevent misconceptions, as well as to ensure that the necessary input data is incorporated. They include the following:

- The involved parties must grasp the difference between auditing and determining a Network Warfare Capability. It is encouraged to incorporate the use of auditing in the technique set underlying Network Warfare.
- To determine a Network Warfare Capability, assessments of the various techniques that contribute to Network Warfare are necessary. This will incorporate expert opinion and can use quantitative and qualitative assessments. The qualitative assessments will require expert opinion for the formulation of natural language descriptions that provide an adequate evaluation of the techniques. Expert opinion is necessary in other aspects too. An example would be the compilation of the input data. This ensures that the core techniques are considered, as well as that more important aspects are also reflected
- Various contributing techniques influence the high-level indication of a Network Warfare Capability. Therefore, the assessment is dependent on the compilation of representative input data, with the output denoting an overall capability that can be interpreted again.

In summary, the requirements for a Network Warfare Capability Determination are shown in Table 1:

Table 1: Network Warfare Capability Determination Requirements

Network Warfare Capability Determination Requirements
Holistic but abstracted representation of Network Warfare
Offensive and defensive techniques evaluation
Difference between Auditing and Network Warfare Capability
Compile and assess techniques using expert opinion
Representative input data and output that can be interpreted again

4. Further Discussion of Requirements

Some of the requirements listed in the previous section can be further elaborated to provide more clarity on their contribution to determining a Network Warfare Capability. These include the distinction between auditing, Network Warfare, quantitative and qualitative assessments as well as a further refinement of the offensive and defensive perspectives of Network Warfare. A more detailed discussion of these requirements follows next.

4.1 Understanding Auditing and a Network Warfare Capability

While a Network Warfare Capability Determination resembles a network security audit, some distinguishing factors do exist. A Network Warfare Capability indicates the readiness and strength of an organisation to prevent, detect and react to Network Warfare attacks. It also shows the aptitude and level of Network Warfare skills of the organisation, which are both offensive and defensive.

According to Landwehr, auditing provides the ability to review security-critical actions so that the initiation of an action can be reliably traced back to the responsible individual (Landwehr 2001). This aspect of auditing focuses on the data that is collected electronically from logs, as well as on the examination of the digital footprint that is generated from activities on systems.

Another perspective of auditing relates to the checking of conformance to policies that govern the applicable information and systems. Vroom and Von Solomons discuss information security auditing as checking the use of security policies to ensure that employees adhere to the rules and regulations specified in these guidelines, and thus protecting the confidentiality, integrity and availability of information and other valuable assets (Vroom, Von Solms 2004). Furthermore, Kizza states that an audit will consist of reviewing all aspects of the stated criteria of systems and reviewing threats and practices to ensure compliance with written guidelines (Kizza 2006).

These descriptions of auditing depict a testing and checking approach to ensure conformance to established guidelines. The difference between network security auditing and determining a Network Warfare Capability is that network security auditing evaluates compliance with controls in a very detailed manner, whereas in the latter, an assessment is given of the current state of Network Warfare skills. This assessment can involve expert opinion, controls and guidelines. According to Bragg et al, an assessment is not an audit, which is used to test compliance with existing policies and represents a very detailed focus on a particular system or network (Bragg, Rhodes-Ousley & Strassberg 2004). An assessment provides an evaluation, and in this case, a judgment of how well-developed an organisation is, in a range of Network Warfare techniques, both offensive and defensive.

An audit is very detailed, specific and focuses on select controls in a system. A Network Warfare Capability Determination tries to achieve a high-level evaluation of various techniques. It is important to understand the difference between auditing and Network Warfare in order to prevent misconceptions, as well as to realise that auditing can play a role in determining a Network Warfare Capability.

4.2 Quantitative and Qualitative Assessments

Information security plays a pertinent role in Network Warfare and covers various techniques. These include techniques like Risk Analysis, Physical Security, Incident Response, Penetration Testing, Security Evaluations, Network Intelligence, Forensics, Disaster Recovery, Threat Estimate, Legal, Regulations, Compliance, Covert Communications, Research, Innovation, Analysis, Development and Maintenance (Williers et al. 2005/06) (Harris 2007) (Tittel, Cahpple & Stewart 2003). In addition, information security and Network Warfare also have more offensive aspects like Hacking, Vulnerability Injection, Network Attacks, Denial of Capability, Interception and Blockage Blockage (Williers et al. 2005/06) (Qingbao et al. 2008) (Anwar, Zafar & Ahmed 2007). The contribution of these various techniques should be considered in the determination of a Network Warfare Capability. Consequently, to determine a Network Warfare Capability, an assessment of each of the techniques is also necessary. In some instances, metric measures play a role and in other cases reflective judgement can be used.

Metrics are incorporated in quantitative assessments and judgement is reflected in qualitative assessments. The distinction between quantitative and qualitative assessments can be elaborated on and is provided next.

An area in which a quantitative assessment can indicate the level of a skill is penetration testing. Should an internal system repeatedly be entered by bypassing security controls, this indicates an accomplishment of the penetration testing technique, as well as the weakness of the system. Similarly, a successful vulnerability injection technique can be determined by the number of times a payload can be executed on a machine before it is blocked by a new patch.

However, since a metric value cannot always be assigned to the skills involved in having strong personnel security, an assessment of a weak personnel security would qualitatively describe the technique level.

An example that incorporates the importance of both quantitative and qualitative assessments follows. If an organisation is involved in research and innovation, a metric value of ten journal papers may indicate good progress. However, other factors could have an impact on the qualitative rating. An assessment of the usefulness, value and application of the work may also be relevant, and not merely the metric count of publications. An expert panel could evaluate the usefulness, value and application of the research based on knowledge and experience in the field. Thus, the qualitative assessment of excellent research and innovation can be influenced by factors that do not strictly map to quantitative techniques.

Thus, when determining a Network Warfare Capability, there will also be the ability to analyse input that does not necessarily have metric values. Quantitative assessments can play a role in evaluations, but intuition and judgment can greatly influence the qualitative assessments as well. In some cases, a quantitative value can reflect the capability, while in other cases the data can only be judged qualitatively. This implies that a mix of skills, which do not operate independently, is required to determine a Network Warfare Capability.

4.3 Further Elaboration of Offensive and Defensive Network Warfare

While various techniques are involved in Network Warfare, both offensively and defensively, many organisations engage in various defensive strategies to protect their systems and information. Offence, is often considered the best defence, which is especially applicable in the abstract asymmetric realm of cyberspace but due to the legal implications of launching offensive attacks, many companies resort to intensive defensive strategies without much attention to offensive tactics. However, in the military arena, offensive measures are a necessary part of operations. While many projects may be classified, offensive tactics are developed to launch attacks, should the need arise.

To elaborate on the offensive and defensive aspects of Network Warfare UML diagrams will be provided. Firstly, use case diagrams are given of offensive and defensive Network Warfare. Thereafter, component diagrams are provided. This serves to further clarify the offensive and defensive perspectives of a Network Warfare Capability and provide more detail of the interaction of techniques (mentioned in Section 4.2) involved in a Network Warfare

Capability. The examples provided, typically deal with military scenarios and have been used to show the application of UML in clarifying Network Warfare. The aim of the next few sections is to indicate how UML can be used to capture pertinent relationships by using specific military scenarios. The technique can thus also be applied to include targets like Critical Information Infrastructure in the public domain and Supervisory Control and Data Acquisition (SCADA) systems (electrical, water, transport). We commence with the use case diagrams followed by component diagrams to demonstrate the need to determine a Network Warfare Capability.

4.3.1 Use Cases

The use case diagrams depict the high-level classification of determining a Network Warfare Capability into assessing own system's capability and assessing foreign system's capability (see Figure 2).

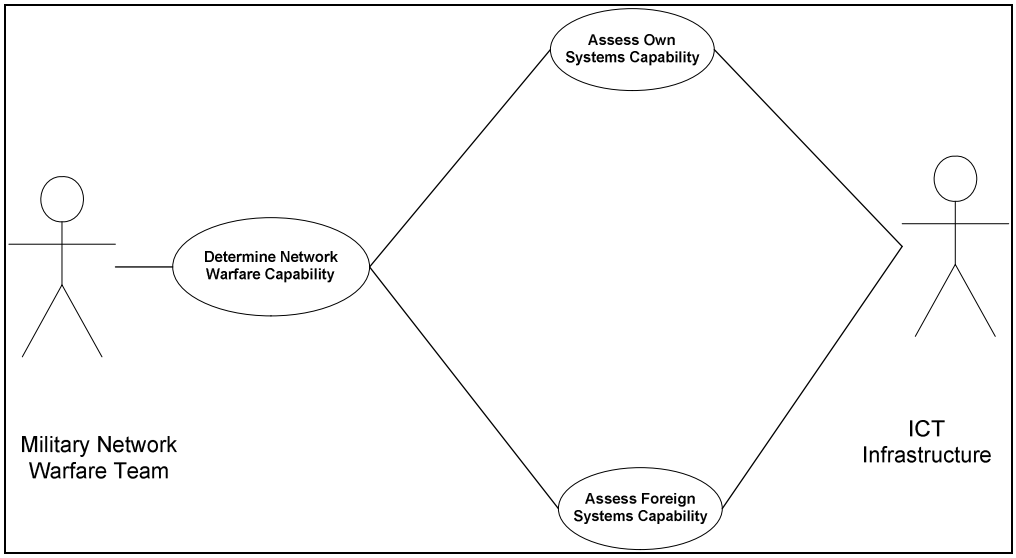

Figure 2: Use Case of High-level Network Warfare Capability Determination

Assessing capabilities of own and foreign systems can then be broken down into assessing offensive and defensive capabilities. This is shown in Figure 3 and Figure 4 .

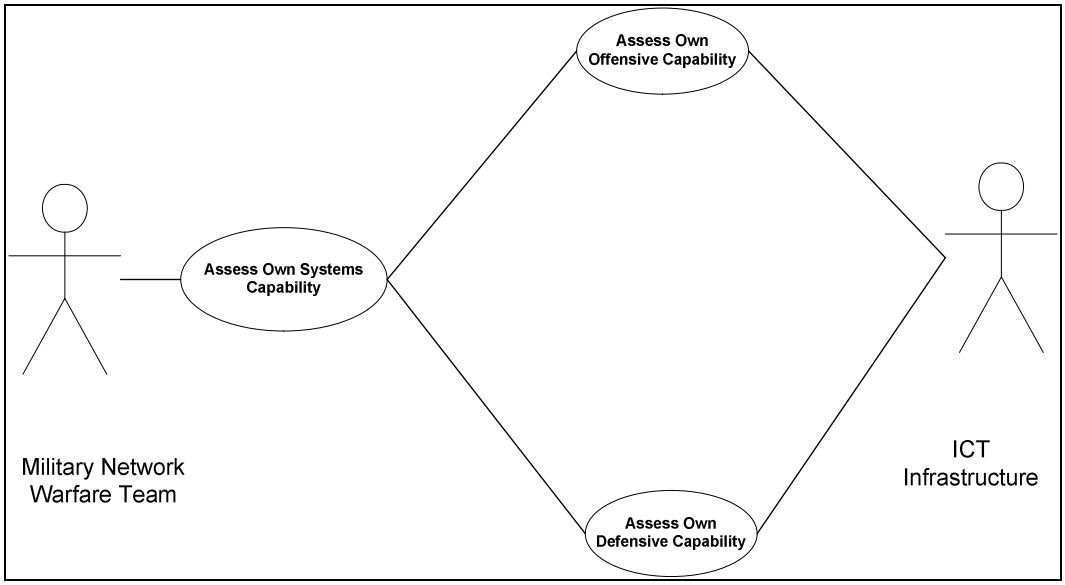

Figure 3: Use Case of Assessing Own Systems Capability

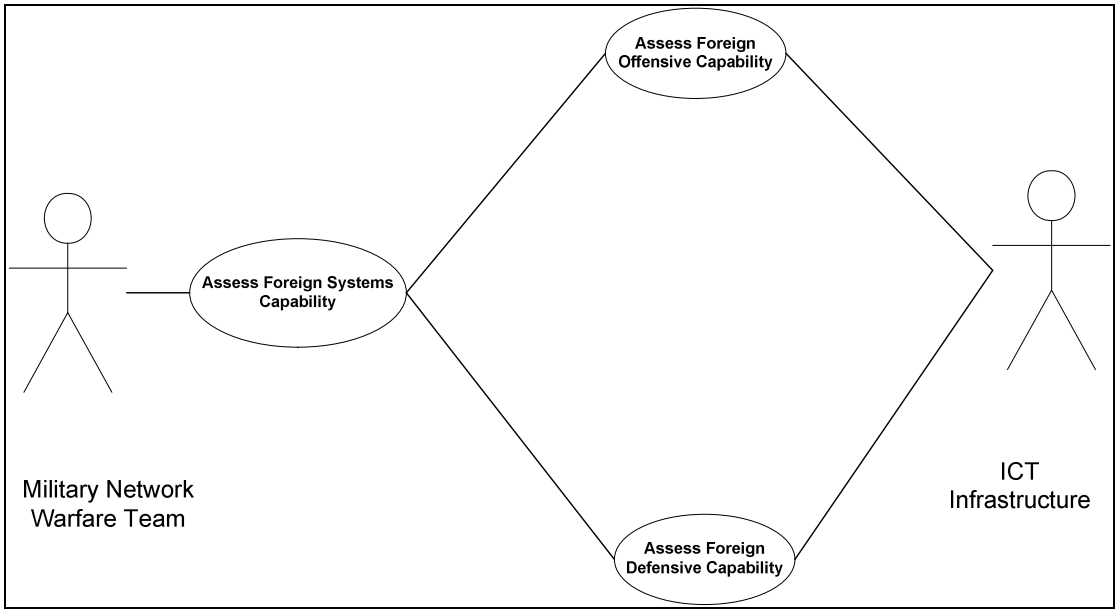

Figure 4: Use Case of Assessing Foreign Systems Capability

4.3.2 Component Diagrams

The determination of a Network Warfare Capability can consider own systems and foreign systems, as well as offensive and defensive perspectives. To show the interaction between offensive and defensive techniques on both own and foreign systems, component diagrams will be shown next.

In order to interpret component diagrams, a short explanation follows. Components are shown in the blocks and are used to group elements in logical structures. In this example, the components are the Network Warfare techniques. The relationships are represented by the connectors between component blocks: it is summarised in Figure 5. For example, the technique Risk Analysis in Figure 5, provides a list of identified threats and vulnerabilities and requires guidance to be carried out. Thus, to summarise a dependence arrow comes out of the consuming socket and the arrow head connects with the lollipop of the provider. Furthermore, the arrow emerges from the required technique and is later used by a provider interface.

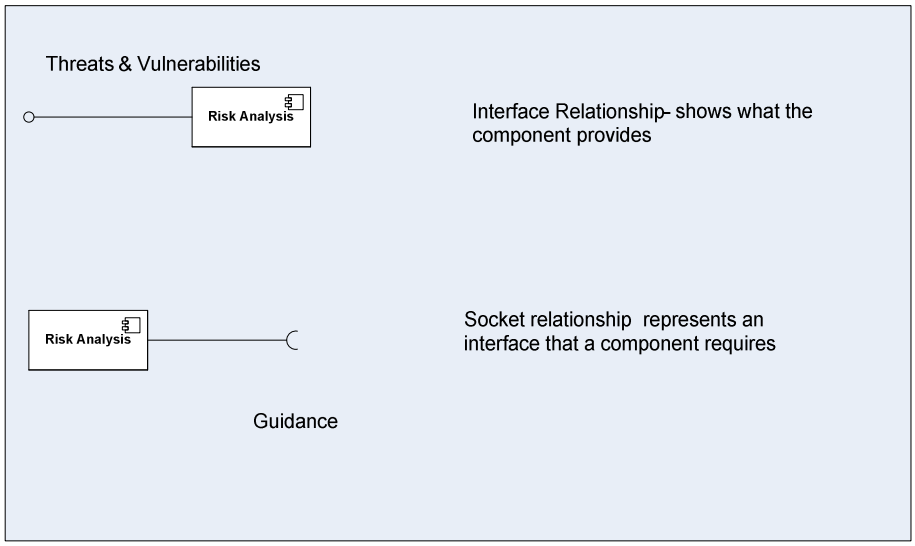

Figure 5: Key to reading Component Diagrams

Component diagrams are a means of showing the structural relationships in a system. In this case, the Network Warfare Capability represents the systems and the various techniques are the underlying structures that contribute to Network Warfare. In order to show relationships, it is important to show the interaction between techniques. Therefore, it would not be suitable to isolate offensive and defensive techniques, but rather to show how the techniques relate and feed off each other.

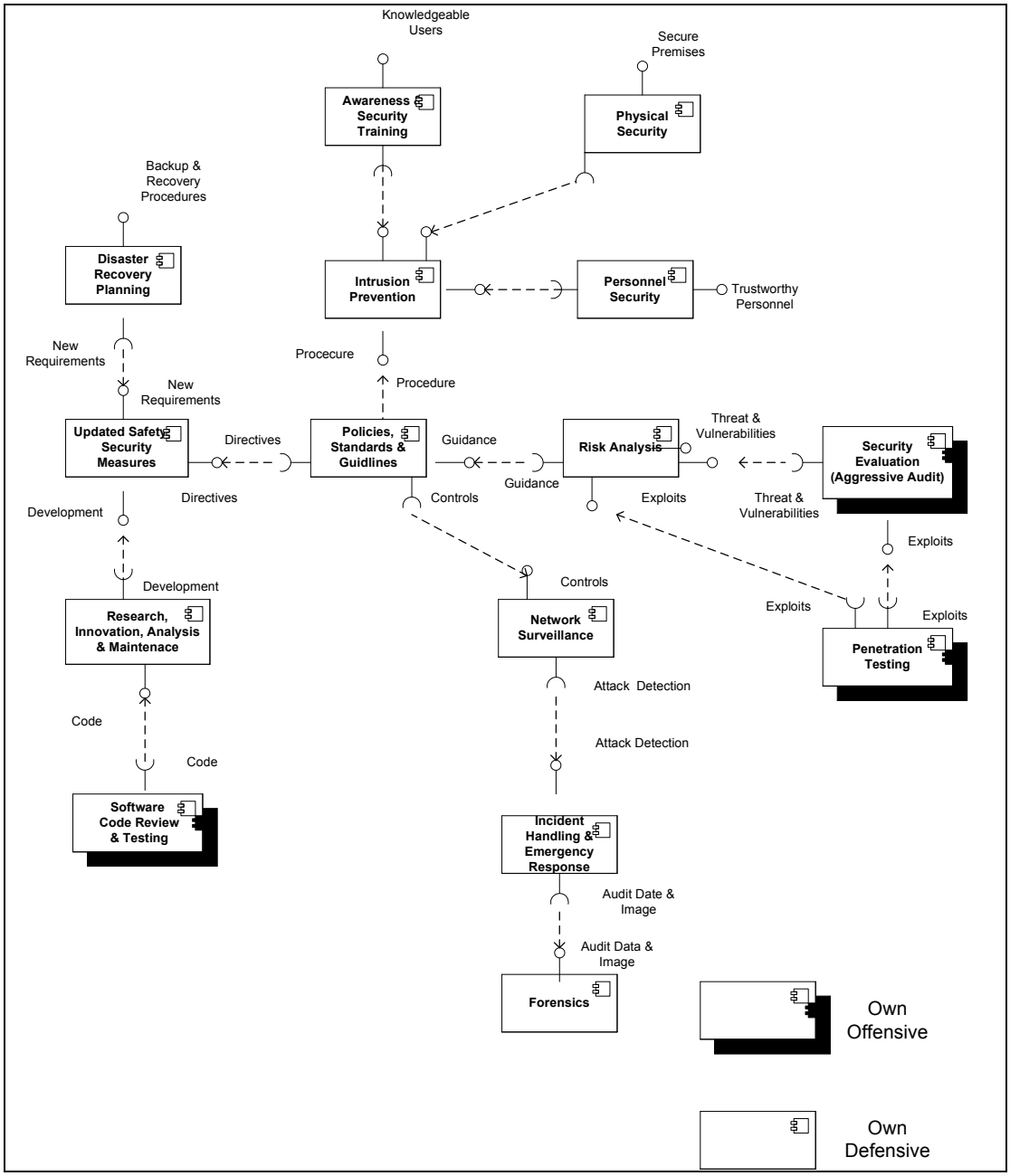

Figure 6: Component Diagram for Own Systems

The component diagram for Own systems is shown in Figure 6. In this component diagram, unlike use cases of sequence diagrams, there is no defined starting point, but rather the diagram reflects the interaction between the various techniques. However, to explain the diagram, the discussion will commence at the technique Risk Analysis.

Network Warfare in an organisation requires Risk Analysis to determine threats, vulnerabilities, probabilities of occurrence and the impact. Thereafter, the findings from the

Risk Analysis can be used to compile Policies, Standards and Guidelines that will govern the systems and networks. Security measures that form part of Policies, Standards & Guidelines, do not remain constant and, therefore, require periodic updates. Disaster Recovery Planning also requires period updates as the systems change.

In addition, Software Code Review & Testing deals with code inspection, evaluation or modification. From an offensive perspective, code can be adapted such that it is not detected by antivirus software. The modification, whether it is malware development or optimisation, all contributes to Research, Innovation, Analysis & Maintenance, which in turn can impact the updating of security measures.

Furthermore, Policies, Standards & Guidelines are used to set up the systems and networks in order to prevent intrusions. Other techniques used to provide Intrusion Prevention include, Awareness & Security Training, Physical Security and Personnel Security. These aspects look at educating the user with regards to best practices and ensuring that trustworthy personnel enter and use the premises and facilities.
Moreover, Policies, Standards & Guidelines guide the way in Network Surveillance takes place. During Network Surveillance, an attack can be detected which then requires the services of Incident Handling & Emergency Response. As part of the incident investigation, Forensics may be needed.

At an offensive level, own systems can be aggressively audited to detect weaknesses and non-compliance. During Penetration Testing, attempts are made to break into systems. The findings of the Aggressive Audit and Penetration Testing can then be fed into Risk Analysis.

In this sense, the various techniques interact and impact each other. The component diagram and explanation represent one example of looking at Network Warfare and, while many other interactions exist, this merely illustrates another example of abstraction and the representation of key relationships.
A component diagram for foreign systems is discussed next. Figure 7 shows the core relationships between offensive and defensive techniques on foreign systems.
Similar to the component diagram for own systems, the component diagram for foreign systems does not have a specific starting point, but for the purposes of explanation, the discussion will commence at the Information Gathering technique.

Information Gathering looks at the collection of information from foreign systems. Once information is gathered, attack and manipulation techniques can be developed, or the information can be used to attempt to break into systems though Hacking.

Furthermore, Attack & Manipulation Development includes the injection of vulnerabilities, interference to cause a denial of capability or the creation of a covert channel for communication. Another, more active spin-off from Hacking is Data Interception, Decryption & Modification, which seeks to alter the data and thus compromise the integrity of foreign system data.

With respect to foreign systems, information gathering can also be linked to Reconnaissance & Intelligence, with looks at actively monitoring foreign systems to identify enemy plans and activities. As part of Reconnaissance & Intelligence, threats and vulnerabilities can be assessed to determine potential exploits that can be taken advantage of on foreign systems, should the need arise. A more passive form of Reconnaissance & Intelligence is merely intercepting and blocking data without altering the contents of data packets.

Many other examples of interaction between the techniques do exist, such as a covert channel feeding into Reconnaissance & Intelligence or the injection of a vulnerability to block data. Thus, the component diagram for foreign systems, like the component diagram for own systems, tries to capture a few examples of interaction between techniques to demonstrate the connectivity and dependence of techniques in a Network Warfare Capability.

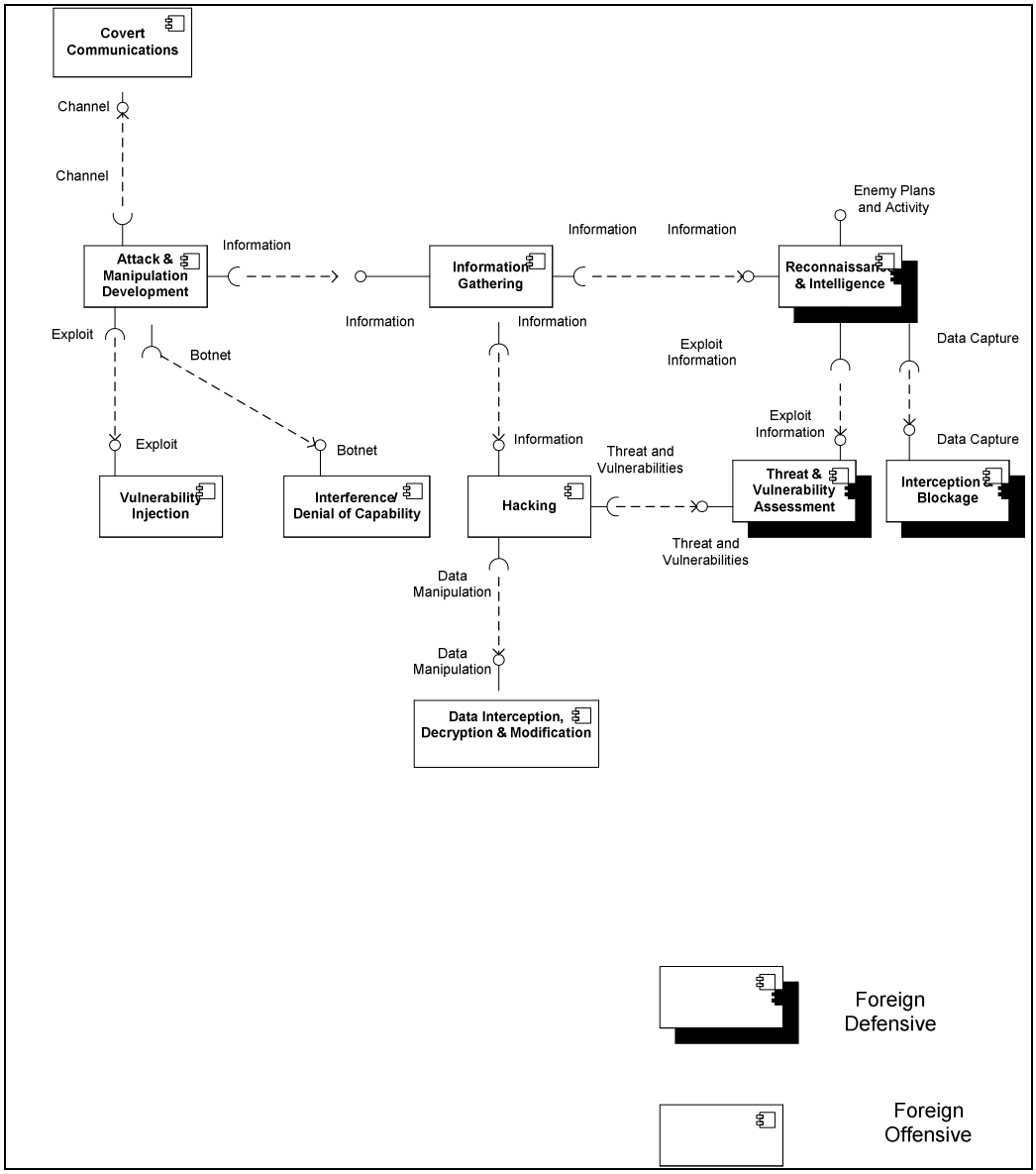

Figure 7: Component Diagram for Foreign Systems

5. Conclusion and Future Work

In this paper, a motivation and description of requirements of the Network Warfare Capability Determination Model were given. This was provided through listing various reasons that justify the usefulness of a Network Warfare Capability Determination model, as well as through UML diagrams to illustrate the interaction of Network Warfare techniques. This preparatory work will form the basis of a future model to determine a Network Warfare Capability.

This paper thus focuses on a preliminary introduction that deals with the research question of determining a Network Warfare Capability. Future work will entail the development of the model for determining a Network Warfare Capability that takes into consideration the identified requirements.

Acknowledgements

This work was carried out and supported by funds at the Council for Scientific and Industrial Research (CSIR). The support of the Defence, Peace, Safety and Security (DPSS) at the

CSIR, SAP Research CEC Pretoria and SAP Meraka UTD (CSIR) towards this research is hereby acknowledged.

References

Information management for Net-centric Operations 2007, Defense Science Board, Washington DC.

Anwar, M.M., Zafar, M.F. & Ahmed, Z. 2007, "A proposed preventive information security system", *International Conference on Electrical Engineering (ICEE)*IEEE, , pp. 1.

Bragg, R., Rhodes-Ousley, M. & Strassberg, K. 2004, *Network security: The complete reference,* McGraw-Hill Osborne Media.

Elbirt, A.J. 2003-2004, "Information Warfare: Are you at risk?", *Technology and Society Magazine, IEEE,* vol. 22, no. 4, pp. 13-19.

Harris, S. 2007, *CISSP certification all-in-one exam guide,* McGraw-Hill Osborne Media.

Kizza, J.M. 2006, *Computer network security and cyber ethics,* McFarland & Co Inc Pub.

Landwehr, C.E. 2001, "Computer security", *International Journal of Information Security,* vol. 1, no. 1, pp. 3-13.

Munro, N. 1996, "Sketching a national Information Warfare defense plan", *Communications of the ACM,* vol. 39, no. 11, pp. 15-17.

Panda, B. & Giordano, J. 1999, "Defensive Information Warfare", *Communications of the ACM,* vol. 42, no. 7, pp. 30-32.

Park, S. & Ruighaver, T. 2008, "Strategic approach to information security in organizations", *Proceedings of the 2008 International Conference on Information Science and Security*IEEE Computer Society Washington, DC, USA, , pp. 26.

Qingbao, L., Hongbo, G., Bing, X. & Zhiyong, J. 2008, "Hardware threat: The challenge of information security", *International Symposium on Computer Science and Computational Technology (ISCSCT)*IEEE, , pp. 517.

Tittel, E., Cahpple, M. & Stewart, J.M. 2003, *CISSP: Certified Information Systems Security Professional study guide,* Sybex, California, United States of America.

Vroom, C. & Von Solms, R. 2004, "Towards information security behavioural compliance", *Computers & Security,* vol. 23, no. 3, pp. 191-198.

Williers, C.J., Voster, C.J., van 't Wout, A., Venter, J.P., Naude, S.J. & van Buuren, R. 2005/06, *IW Basic Course*, Council for Scientific and Industrial Research, Pretoria, South Africa.