UNDERSTANDING THE ELEMENTARY CONSIDERATIONS IN A NETWORK WARFARE ENVIRONMENT: AN INTRODUCTORY FRAMEWORK

N Veerasamy and JPH Eloff

Council for Scientific and Industrial Research

University of Pretoria

nveerasamy@csir.co.za

PO Box 395

Pretoria

0002

Abstract Information warfare has surfaced as an emerging concept that affects not only military institutions but ordinary organisations as well. Information warfare in itself consists of various components ranging from its electronic and psychological aspects to its network enabled capabilities and functionality (network warfare). Various computer and information security practices form part of network warfare techniques. Whilst various information and security practices are well-known and applied by many, there is a need for a more structured approach to understanding the various techniques required for a network warfare capability.

A conceptual framework describing the most important network warfare techniques and considerations is proposed. It seeks to offer a better introductory understanding to the field of network warfare. This paper addresses the requirements for a network warfare capability and will look at the high-level approach, constraints, focus areas, levels, techniques and objectives. The framework therefore intends to present a more conceptual and structural examination of network warfare requirements and techniques. It should therefore provide a good baseline when establishing the capability or determining the practical consequences in any sector.

Keywords: Information warfare, network warfare, framework, capability

1. Introduction

As the world has moved into the Information Age, there is an increased need for the protection of the precious commodity information. The new emphasis is on Information warfare which is a modern type of conflict in which groups try to secure their own resources and thus prevent adversaries from denying and exploiting their information which would otherwise minimise capabilities. Information warfare refers to actions taken by the opposition to abuse information processing functionality to their benefit. Information warfare at its simplest level is the use of computers to attack an adversary's information infrastructure while protecting one's own information infrastructure [1].

Due to the increased use of computers and the connectivity afforded by networks, information can easily be stored and transported. The need also rises to properly protect these resources. Many users make use of global network connections to communicate and

exchange information. However, there also exists the underworld community of hackers and abusers who seek to damage, destroy and deny access to information.

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 afforded by networks is utilised to carry out exploits on information. “The term netwar refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organisation and related doctrines, strategies and technologies attuned to the information age.”

Network warfare is thus not only a military strategy but also application to the ordinary user domain as personal attacks and corporation exploitations are commonplace. Hacking attempts and the release of malware affect the average consumer and now ordinary users have become targets for netwar personal and social modes of attack. Protective software, like anti-virus and firewalls all try to protect the corruption of information across networks. Both the offensive and defensive sides of network warfare can be seen to applicable to all types of global users. Thus, it can be seen that netwar is relevant to all users of computers and the Internet due to the large number of exploits and defense mechanisms in place.

Network warfare can be seen to encompass various computer and information security principles and techniques. Thus, the basis of technical capabilities of network warfare lie within the area of information and computer security practices. Most computer and information security plans focus on the various security technologies that should be implemented. Whilst these techniques would fit into a network warfare capability plan, other aspects covering the objectives and other strategic factors of netwar have not been fully explored. Further investigation into the requirements and objectives of network warfare is necessary to understand the form of conflict that is being played out across the global community.

A key objective of a netwar capability will be protection and preservation of integrity of information. Previous research into a scheme of transferring data has been carried out to demonstrate the objective of protecting data and thus creating a stealthy means of transportation. The proof-of concept is explored in [2] and [3]. However, it has been identified that a framework of the high-level area of network warfare would be useful in identifying further requirements, objectives and influential considerations. Such a framework has been proposed in this paper.

This paper addresses the requirements for a network warfare capability and will look at the high-level approach, functional activities, constraints, capability requirements and objectives. The framework therefore intends to present a more conceptual and structural examination of network warfare requirements and techniques. It aims to provide a better introductory basis into the field of network warfare. It should therefore provide a good baseline when establishing the capability and determining the practical consequences in any sector.

The remainder of this paper is structured as follows; the background section provides an introduction topic of network warfare as a component of information warfare. Section 3 describes the need for understanding network warfare. Thereafter, the framework is introduced in section 4. The framework is further explored in Section5, before the conclusion is given in Section 6.

2. Background

This section contains a brief introduction to network warfare as a facet of information warfare. We merely wish to provide the context of the concepts of network warfare and thus elaborate on the initial purpose of this paper. More detailed overviews can be found in other literature [[4],[5] and[6]].

Information warfare consist of the activities carried out in various domains (social, personal political and the military) that seeks to destroy, damage or deny information resources as well as the various defensive measures that are employed to prevent such attacks. Simply put, information warfare implies a range of measures or "actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary" (Alger, 1996, p. 12).[7].

The exploitation of information can have various consequences ranging from the psychological ramifications to the impact on control and management processes and the economic effects. The findings of the United States Air Force Armstrong Laboratory show that information warfare has the following unfolding types: command and control warfare, intelligence warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare and cyberwarfare [6]. Dai further argues that information warfare is composed of six 'forms': operational security, military deception, physcological war, electronic war (EW), computer network war and physical destruction [[8] in [9]]. Thus it can be seen that computers, networks, hacking and cyberspace have an active role to play in information warfare. Network warfare can be seen to encompass the various previously categorised computer and security related warfare concepts into a single branch that deals with information security at a computer and network level. Furthermore network warfare is not simply about the technological solutions that can be used to wage or defend against attacks. Network warfare also entails the high-level approach, strategy and plans to best protect, recover or attack if necessary. The term netwar connotes that the information revolution is as much about organisational design as about technological prowess and that this revolution favours whoever masters the network form [10].

Network warfare relates to the various types of network crime that takes place on computers and through networks and cyberspace to the many defense mechanisms that are deployed to prevent attacks and thus protect information. Arquilla and Rondfeldt explain that "many writers enamored of the flashy, high-tech aspects of information revolution have often depicted netwar as a term for computerised aggression waged via stand-off attacks in cyberspace- that is, as a trendy synomyn of infowar, information operations, "strategic information warfare" Internet war, "hackitivism, 'cyberterrorism, cybotage,etc' [4]". In many cases ordinary users are totally unaware that they are being hacked through cyberspace. Leeson and Coyne propose that hackers are of 3 types: "good": these hackers break into computer systems illegally but voluntarily share security weaknesses with those in charge, "fame-driver": members seek infamy and the accolades of their cohort by breaking into the electronically stored information of vulnerable parties and wreaking havoc, and lastly "greedy": driven by profits [11]. The motive of perpetrators is unknown to the beguiling user: fun, profit or challenge are possible answers. A worrying aspect identified by Annual Review of Institute for Information Studies is that "hacking for fun" is being supplanted by hacking for profit as freelancers, businesses, governments and intelligence agencies turn to computer networks to facilitate both legitimate and criminal activities [11]. Therefore, in

order to create an awareness of offensive and defensive approaches to network warfare, an understanding of high-level tasks and objectives is necessary. Users, companies and institutions need to be alerted of the new face of warfare that is not only being played out between military forces but also affects their personal and corporate activities.

Network warfare can be seen from different approaches which are often difficult to distinguish between. This blurring of offense and defense reflects a broader feature of netwar: It tends to defy and cut across standard spatial boundaries, jurisdictions, and distinctions between state and society, public and private, war and crime, civilian and military, police and military, and legal and illegal [10]. Offensive and defensive methods, legal and civilian boundaries, geography and physical limitations are all issues that are to be considered against the context of netwar. Network warfare is a multi-faceted issue that is facing the global community due to the increased ease and convenience of use of various computing and networking technologies. Awareness of the various technological and strategic requirements will help better prepare users and organisations.

The rest of the paper will examine the exact considerations that affect building a network warfare capability. The focus will turn to elaborating on all the key issues that could impact on a network warfare capability. However, first a brief motivation to understanding network warfare will be provided.

3. Motivation

Users of computers and the Internet may be unaware of the various exploits that are taking place across cyberspace. Awareness needs to be created on the ease and type of netwar techniques in the ordinary user domain. Examples of attacking network warfare techniques range from web site defacement to malware that is unleashed on the Internet. Defensive network warfare techniques include the use of scanners and intrusion detection software to detect unwarranted actions on networks.

However, the use of various computer and security techniques does not fully describe the high-level objectives and considerations required to establish a netwar capability. “Although information warfare would be waged largely, but not entirely through the communication nets of a society or its military, it is fundamentally not about satellites, wires and computers. It is about influencing human beings and the decisions they make [12]. This highlights the need to realise that network warfare is not simply an issue of which technologies to deploy but has deeply embedded in its roots the requirement to formulate a strategy to influence the thought processes and thus the control and organisational structure to ensure that suitable management is applied and maintained. The network warfare capability would be quite limited if the focus was merely placed on the technologies. A greater understanding of the topic from a strategic point of view is required. This will aim to ensure that all influential factors have been considered.

Network warfare will become increasingly important due to the growing dependency on computers and networks. Certain security precautions and measures need to be instilled to try and prevent severe damage (financial and reputation for example). By describing the overall considerations in a network warfare environment, a better understanding of this relevant field can be gained. To provide a more thorough understanding of network warfare, a framework, considering key issues, has bee proposed. It is hoped that the framework will offer a more structured and formal overview of the topic so as to highlight the impacting factors and needs.

4. Framework

In this Section, the framework is introduced, which allows for exploration of the topic thereof. Each component of the framework will be further discussed.

The framework is given in Figure 1. It mainly consists of three sections, the planning considerations, the techniques and the objectives which will each be discussed in Sections 5, 6 and 7 consecutively.

We consider four contributing considerations: constraints/implications, target/focus, levels, and approach. Each contributing consideration in turn consists of applicable sub-items. The contributing considerations provide the context for which the network warfare techniques and objectives are trying to achieve. The contributing considerations describe aspects that define or result from network warfare. Various computer and network security techniques and principles are applicable to network warfare. However, a more formal and structured overview is shown to generate further discussion in the field.

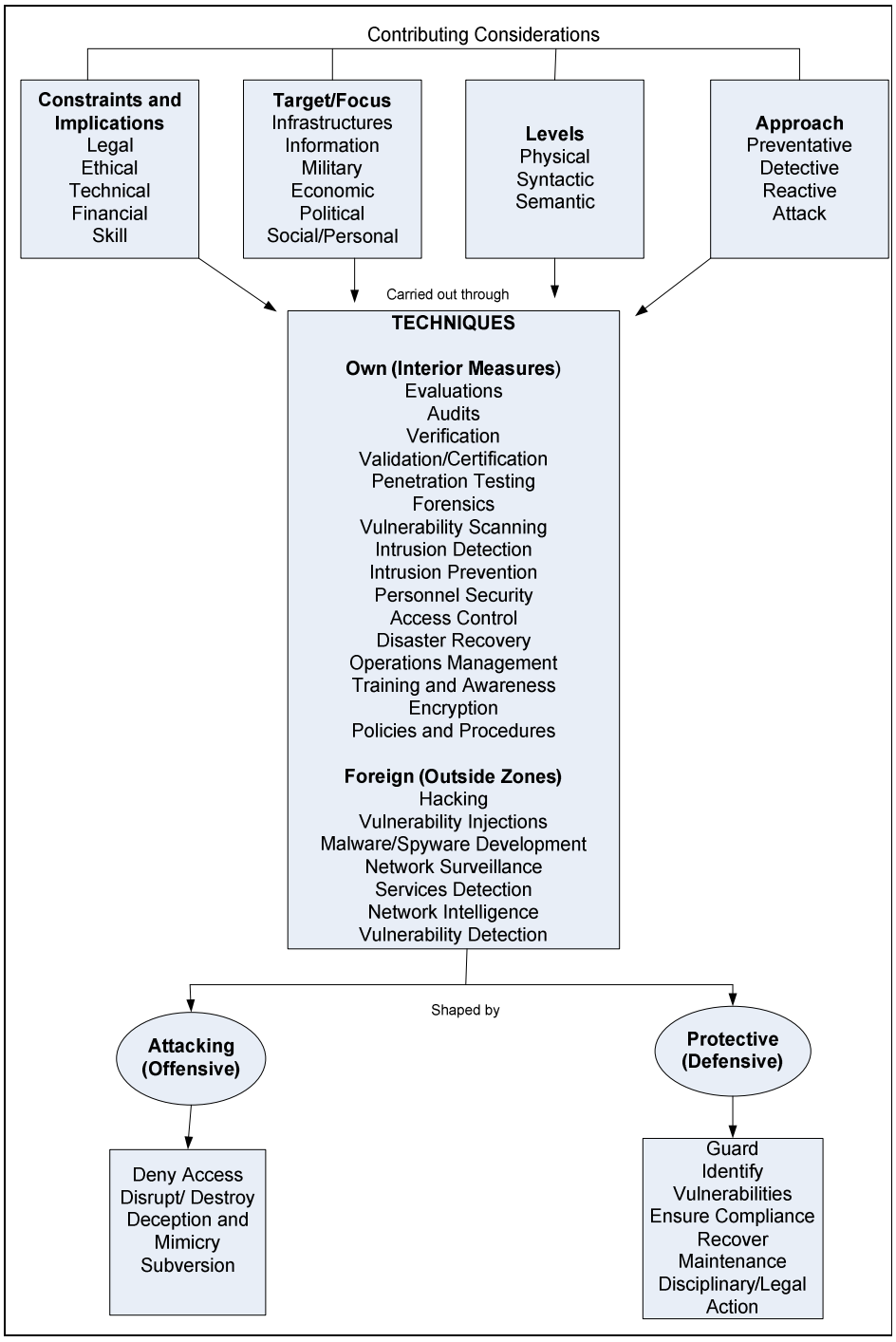

Figure 1: Conceptual Framework for Network Warfare

The network warfare techniques are essential functionality that form part of a network warfare capability. The technique section lists and briefly describes various computer and information security activities that form part of network warfare. Further research and technological development into each of the listed areas is still required.

The framework considers two locations of network warfare activities: own (interior measures) and foreign (outside zone) systems. The techniques described are not all-inclusive but offer examples of the type of activities that will be performed at different sites. The techniques provide an overview of the classes of activities that contribute to a network warfare capability.

Two categories of network warfare objectives are proposed: attacking (offensive) and protective (defensive). This serves to distinguish and classify the motives of the actors in network warfare events. An attacking objective implies an intention of damage, destruction or failure. A protective approach aims to prevent, defend and recover from harmful action. The contribution of the framework lies in the taxonomy of the techniques as well as the overview of the additional considerations. A discussion elaborating on the various components of the framework therefore follows.

5. Contributing Conditions

This Section addresses the groups of contributing conditions that affect network warfare. Later sections will delve into detailed aspects of network warfare. These conditions explain the context of network warfare. Findings are drawn from an overview of literature as well as practical experience that helped identify the different contextual paradigms of network warfare. These conditions present the different approaches to the topic of network warfare as well as influential considerations in the conceptual framework.

5.1 Constrains and Implications

Several factors can constrain network warfare and have associated consequences. These include the legal issues, ethical dilemmas, technical solutions, financial impact and skill/manpower investment. Logical constraints/implications have been grouped together in the discussion that follows.

5.1.1 Legal Ethical Issues

As network warfare becomes more malicious, legal and ethical boundaries can be crossed. Alger proposes network warfare can cause potentially serious social problems and create novel challenges for the criminal justice system [7]. Criminal activities should not be condoned but the underlying causes of crime also needs to be understood. Ethics and morals play a significant role in determining the personality traits of an individual. Users will need to balance ethical dilemmas before engaging in offensive network warfare. Computers and network are powerful tools and great harm can be caused with them. Motive, attitude, values, upbringing, experience and culture can all impact the approach an individual can have when using computer resources. Socially a culture of responsibility and accountability needs to be instilled to ensure that users take precaution when using potentially harmful tools. A moral sense needs to be developed to ensure that users do not engage in malicious activity. On the other hand in the military context, officers will need to be trained to engage in offensive techniques. If one considers the mindset of a terrorist, a soldier, a network administrator or an activist, very different judgements and behaviour will be found. Network warfare is thus a double-edged sword and depending on the context, different actions (sometimes harmful with different legal and ethical implications) will be deemed necessary.

Computers and networks afford global connectivity with the blurring of physical and judicial boundaries. Detection of offences and the enforcing of laws thus becomes complex

with the application of different rules and the difficulty of demonstrating proof aggravating the situation. Network warfare actions can thus cross the legal boundaries, as users participate in various malicious or surveillance tasks. In the military domain, however, different laws may be applicable. The Geneva Convention, and its interpretations allow for different treatment for soldiers, who are protected under its terms, and spies, for whom it offers no such protection [13]. In this way, different legal requirements can exist in the different societal and military domains. Closely linked, is the field of forensics, which seeks to hold users accountable for their actions by identifying and locating fallible evidence of illicit activities. This section seeks to highlight that various legal and ethical issues arise from the different offensive and defensive activities that take place. Globally each country has their own judicial laws and therefore the exact legal implications do not form part of the scope of this paper.

5.1.2 Financial Impact

The release of a single virus can have a serious economic impact. A survey by TrustSecure/ICSA Labs in 2003 determined that the remediation cost of the MS Blaster worm was approximately $475 000 per company [14]. In 2003, hacker-created computer viruses alone cost businesses $55billion- nearly double the damage they inflicted in 2002 [11]. With offensive assaults costing nearly double as previous years, the anticipation of future costs is staggering. The results of the surveyed respondents in the CSI/FBI investigation showed a total loss of over $52 million (in 2006) for the many exploits ranging from viruses, theft and misuse [15]. One need only look at these incidents and figures to realize that the financial implications of security exploits have a considerable impact on the industry. Disruption to services and loss of availability leads to denial of accessibility to business operations or services which in turn has the impact of loss of productivity and thus business and revenue. Restoration; reparation and protection activities require additional resources (tools, hardware, software, etc) and staff, which too have financial costs involved. The financial consequences of security exploits is one of the most significant issues facing businesses when drawing up their IT budgets and business plans as the monetary amount to be spent, has to be determined, as well as factoring in potential losses. The investment in personnel, tools and skill development plays a significant role in any budget.

5.1.3 Technical Solution and Skill/Manpower Investment

Closely related to the financial costs of security exploits is the investment in additional staff and equipment. Defence and protections systems are implemented by network staff. The rising number of security exploits means that additional controls and personnel have been dedicated to preventing, detecting or repairing attacks. A large number of technologies like firewalls, software (anti-virus, anti-spy ware, and intrusion detection), encryption, and biometrics are being utilized. Security evaluation tasks like auditing, penetration testing and monitoring require the use of both tools and human interaction to make informed decisions and actions. Employees will also need to be trained in the use and deployment of the various technologies. As the number of exploits rise sharply so does the requirements for improved security. This will entail the increased investment in the appropriate tools, equipment and employees.

5.2 Target/Focus

Network warfare has been shown to be applicable in various domains and is not just limited to military-based conflict. Information warfare may very soon become relatively commonplace: military, corporate/economic, community/social, and personal [16]. Different focus areas of network warfare are thus evident. Molander et. al also talk of different strategic targets which include information and the different information infrastructures (military, physical, economic, political and social). Social wars are being waged as users maliciously try steal identities, carry out fraud or create disinformation on the World Wide Web. Economic attacks seek to blockade economic information flow and thus impact markets [6]. Politicians seek to maintain friendly relations with allies and protect their reputations. Network warfare thus stretches its reach to various targets that have a global impact due to the organisational, private and peace-keeping efforts.

5.3 Levels

According to Libicki, from an operational point, systems can be attacked at a physical, syntactic and semantic level [5]. This in turn implies the existence of protective mechanisms at these levels. At a physical level, network warfare refers to the destruction of equipment and resources so as to substantially ruin/damage information in a tangible format or to prevent a future reproduction of its contents. Syntactic relates to the conformity to a systematic and orderly arrangement [13]. This implies the disruption to the organisational structures, for example causing a denial of service or interruption in data flow. Semantic affects the meaning of what computers receive from elsewhere [5]. This is linked to the receipt of correct data and the various means in which data can be poisoned and thereafter the continued spread as other devices are infected. Syntactic weapons, like viruses, may be used to corrupt networked systems by destroying or degrading code or data; semantic weapons are used to affect and exploit the trust users have in the information system and the network, as well as to affect their interpretation of the information it contains [11]. The levels represent an aspect of viewing the type of impact network warfare techniques can have.

5.4 Approach

A functional paradigm of defensive information warfare is best described by the following actions: protect, detect and react [17]. Network warfare can thus defensively be approached from a preventative, detective or reactive point of view, as well as an attacking mode when looking at the opposite perspective. An attacking approach will seek to wreak damage, disruption or interruption to the system. Protective mechanisms endeavour to prevent/detect misdemeanours and also formulate a means to stop or recover from attacks. The factors relating to the approach taken to network warfare represent the high-level classification of the objectives. Specific techniques are needed to achieve each approach and individual objectives. This will be discussed next.

5.5 Techniques

The previous section described various conditions that can contribute to network warfare tactics and strategies. By keeping these considerations in mind, an understanding into the application areas of network warfare can be gained.

This section elaborates on specific techniques that can be used to carry out network warfare. Techniques represent the various ways and procedures that are followed in order to accomplish a complex task [18]. Network warfare is thus the complex task that can be carried out through various methods depending on the various contributing conditions and objectives. Although this section is by no means a complete listing of all possible network warfare techniques, it does cover a significant aspect of network warfare practices. A distinction has been drawn between techniques on own systems and those executed on foreign systems. The division is due to the differing strategic goals, information gathering purposes, legal implications and high-level objectives. A closer examination of each technique indicates the underlying goal which differs for interior and exterior requirements. In each case, a different objective is trying to be achieved. The types of objectives will be further explored in next section.

5.5.1 Own (Interior Measures)

Companies, individuals and institutions often implement preventative, detective and reactive measures on their own system to protect, alert and recover from attacks. The International Information Systems Security Certification Consortium (ISC^2) is a corporation that has developed a security certification program for information systems security practitioners worldwide. According to the ISC^2 a number of The Certified Information Systems Security Professional (CISSP) certification as endorsed by ISC^2, consists of domains that make up a Common Body of Knowledge (CBK). The domains that make up the CBK cover security topics like: Management, Cryptography, Operations, Disaster Recovery, Law and Physical Security [19]. The breakdown of security into the various domains is indicative that security has a very wide range of considerations. Evaluations, audits and verifications seek to ensure that specific standards/measures are being adhered to in an effort offer proactive security and thus compliance and certification. Vulnerability scanning and intrusion detection activities aim to find vulnerabilities before/whilst they are being exploited to prevent further damage. Penetration testing is authorised attempts to determine whether the security controls in a system can be bypassed or if exploitable avenues are present. Forensics represents a branch of computer security searching for evidence of wrongful actions which can be utilised to hold users accountable for their behaviour. Disaster recovery planning ensures that crucial data is backed up and that a proper command structure is followed to get critical systems operational again after a crisis. Access control (biometrics, password policies, logon, auditing, physical security) aims to ensure that only authorised users are allowed entry into the systems and networks. Encryption obscures the contents of the data to protect its confidentiality. Policies, procedures, operations management and training seek to guide users to best practices relating to computer, information and network security which in turn will instil awareness on the topic.

Various techniques will be utilised to better protect own systems. From a technological development point of view, research and development will be required in several fields. Network intelligence and creating situational awareness of the network will entail various information gathering techniques. These include network mapping, status monitoring, traffic analysis, vulnerability scanning, intrusion detection, visualisation and reporting of results. Other preventative techniques will include the use of honeypot systems to distract intruders and collect information of their activity. The benefits of honeypots range from providing good situational awareness about the frequency and impact of attacks to revealing strategic information on the attacker [20]. Another area that tries to provide for better compliance is

auditing. Auditing procedures to ensure that policy or standards are being adhered will help ensure system is following best practice.

The discussed techniques demonstrate the various means in which interior security measures can be implemented. Based on different objectives various protective, detective and reactive techniques will be used to establish the capability. Measures taken on foreign systems will be discussed next.

5.5.2 Foreign (Outside Zones)

Hacking attempts are often targeted at outside systems. Motives often stem from profit and fun to political and military intentions. Another harmful netwar technique is vulnerability injections, for example exploiting a database query language vulnerability to insert incorrect data. Further malicious examples of targeting foreign systems include the development of malware and spyware. Security bulletins and web sites are filled with notifications of exploit and patch releases. More passive techniques used on outside systems to gain network intelligence include network surveillance (studying the behaviour of the enemy), services detection (to identify possible critical targets) and vulnerability detection (discover exploitable avenues).

Critical to an offensive mode of operation on foreign systems is the various research and technological areas that need to be explored. These include malware transferral and pay load development. Bypassing firewall, anti-virus and other protective mechanisms will be key considerations during the building of these offensive capabilities. Another aspect from the offensive standpoint, is the development of covert communications tools. Once a machine has been infiltrated, it will be imperative to retrieve data stealthily. Covert communications could be required in real-time or through deceptive techniques like Steganography. Steganography is the art of hiding communication by embedding messages into an innocuous- looking cover medium such as digital image, video, audio and so, while steganalysis focus on revealing the presence of the secret messages and extract them [20]. Thus, hiding the data as well as retrieval of foreign secret communications will require the development of such a capability. Database manipulation is another area through which information can be exploited. Database corruption through SQL attacks represent a vulnerability that can be used to destroy critical data on a host's system. Thus database hacking and manipulation skills will be required to correctly gain access to database. A specialised capability will need to developed to systematically analyse, retrieve and corrupt/destroy data. Network intelligence on foreign systems can also be gained through scanning and interception practices. Collection of data without detection as well as retrieval of data will require analysis and extraction development.

Various techniques have been shown to form part of a network warfare capability. The execution of each task thereof depends on the underlying objective. To provide insight into the intentions of the various techniques, a high-level explanation of network warfare objectives follow.

5.6 Objectives

The previous sections addressed factors that can influence network warfare, as well as various techniques that can be employed to carry out network warfare. This section focuses on the issues of identifying the purpose and reasoning behind network warfare.

The objectives of network warfare have been divided into two categories: attacking (offensive) and protective (defensive). This shows two different mindsets: malicious versus maintaining security. As with any form of warfare, forces may have to attack to create advantage, as well as defend to prevent damage. Bhalla talks of two aspects of information warfare: defensive and offensive [22]. In a similar way network warfare has offensive components and a defensive strategy. The specific objective under each categorisation will be discussed next.

5.6.1 Attacking(Offensive)

"The objectives of information warfare can be masking or unmasking of facts, exploitation, deception (such as disinformation), disruption or denial of service, and destruction of information [18]". This shows that the main aims of an offensive network warfare strategy would be deny access to a service, damage/destroy information, deception/mimicry, and subversion (insertion of malicious data). Denial-of-service attacks try to interrupt the use of specific systems. Breaking into machines (physically and electronically) to delete/alter data are forms of information damage and destruction. Unauthorised modification of data affects the accuracy of its contents. Various malicious modes of subversion have been unleashed in cyberspace (worms, viruses, Trojans, malware, spyware). The attacking objectives described are indicative of the offensive portion of computer and network security and thus shows how these malicious intentions are a core aspect of network warfare as a whole.

5.6.2 Protective (Defensive)

From a protective point of view, network warfare attempts will aim to secure the system from attacks. It is shown that defensive objectives include: guarding, vulnerability identification, recovery, maintenance and disciplinary/legal action. Guarding the system will seek to offer protection and thus prevent (and detect) attacks. In a similar manner, vulnerability identification aims to identify possible ways of exploitation. Maintenance consists of ensuring that the specific technologies are performing their defensive roles as well instilling good practices in users so that they remain aware of the risks of poor security. Disciplinary/legal action ensures that users are held accountable for their actions. Network warfare protective mechanisms/techniques aim to ensure that the system is secure and try to guard against malicious activity.

6. Conclusion

This paper addresses network warfare as an influential consideration facing global users of computers, networks, the Internet and cyberspace in general. Network warfare forms a critical branch of Information Warfare. The focus of Network Warfare lies heavily in the computer and network means through which information can be attacked and the various ways of protecting such resources. Various computer and network security issues form part of network warfare. However, other considerations too were shown to impact the area of network warfare. A more structured means of elucidating the field of network warfare was therefore required. Through an analysis of the topic, it was revealed that network warfare can be executed through various techniques with different objectives, approaches, constraints and target and levels.

This paper took a high-level look into network warfare and a proposed a framework. The framework aims to present a more conceptual and structural examination of network warfare

requirements and techniques. It should therefore provide a good baseline when establishing the capability or determining the practical consequences in any sector.

The framework proposes contributing considerations, techniques and objective. Four groups of contributing considerations are addressed: constraints/implications, target/focus, level and approach. Network warfare is often only linked to its military context. It has been shown that network warfare is applicable to many other domains, including social, political and economic. An investigation of computer and network technologies revealed a number of enabling techniques for network warfare. As network warfare involves a form of conflict, with any battle there exists an offensive component and a defensive aspect. Different offensive and defensive techniques were thus identified and discussed.

Further research into understanding other areas that impact network warfare can be incorporated into the design of the framework. The framework, by itself is a good starting point for placing the concept of network warfare into context. It is hoped that further analysis, can provide the ability to extend the framework.

7. Acknowledgements

The authors wish to thank the organisers of the ISSA 2008 for providing the copyright to this paper. The original manuscript has appeared in the proceedings of ISSA 2008 and through kind permission of the organising committee, a modified version has been allowed to be presented at this IFIP TC9 workshop.

References

[1] A J Elbirt ,Information Warfare, Are you at risk?, , *IEEE Technology and Society Magazine*, 2003/2004.

[2] N Veerasamy & CJ Cheyne, Stealthy Network Transfer of Data, *Proceedings of World Academy of Science, Engineering and Technology*, Vol 25, November 2007.

[3] N Veerasamy & CJ Cheyne, Stealthy Network Transfer of Data, *International Journal of Computer Science and Engineering*, Vol 1 no 3, Summer 2007.

[4] J Arquilla & D Ronfeldt, *Networks and Netwars*, Rand, 2001.

[5] M Libicki, What is Information Warfare? *Strategic Forum Number 28*, May 1995

[6] MR Endsley & WM Jones, Situation Awareness, Information Dominance and Information Warfare, *Tech-Report 97-01* , February 1997.

[7] B Cronin & H Crawford, Information warfare: Its Application in Military and Civilian Contexts, *School of Library and Information Science, Indiana University, Indiana USA*.

[8] Q Dai, Zholgguo Junshi Kexue (China Military Science),On Integrating Network Warfare and Electronic Warfare, February 2002, 112-117 *as translated by the foreign Broadcast Information Service (FBIS) Web site.*

[9] T L Thomas, Chinese and American Network Warfare, *JHQ*, issue 38.

[10] J Arquilla & D Rondfeldt,*The Advent of Netwar*, RAND, 1996.

[11] PT Leeson & CJ Coyne,The Economics of Computer Hacking, *Journal Law, Economics, and Policy*, volume 1, no. 2.

[12] Nortel Networks and Aspen Institute, The Promise of Global Networks, *Institute for Information Studies*, 1999.

[13] , G J Stein, Information Warfare, *Airpower Journal*, No 1, pp 30-39, Spring 1995. [27]

[14] Syntactic and Technique, *The Free Online Dictionary*, Available online from http://www.thefreedictionary.com, Accessed 27 February 2009.

[15] Cert Statistics, *Carnegie Mellon University*, Available online http://www.cert.org/stats/cert_stats.html, Accessed 1 June 2007.

[16] CSI/FBI Computer Crime and Security Survey, *Computer Security Institute (CSI)*, Available online from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf, Accessed 1 June 2007.

[17] S Nitzberg, Conflict and the Computer: Information Warfare and Related Ethical Issues, *in Proceedings of National Information Systems Security Conference*, National Institute of Standards and Technology,1998, Available online from csrc.nist.gov/nissc/1998/proceedings/paperD7.pdf

[18] B Panda & J Giordano, Defensive Information Warfare, *Communications of the ACM*, vol. 42 no. 7, pp 31-32, July 1999.

[19] Revolution in Information Affair, MW Wik, Available online from: http://www.kkrva.se/Links/Infokrig/Wik1.html, Accessed 13 February 2008.

[20] Harris, S, *CISSP All-in-One Certification Guide*, Mcgraw-Hill/Osborne, 2002.

[21] B Scottberg, W Yurcik & D Doss,Internet Honeypots: Protection or Entrapment?, *Symposium on Technology and Society (ISTAS) 2002* , pp. 387-391

[22] XY Luo, DS Wang & FL Liu, A review on blind detection for image steganography, , *Department of Computer Science and Technology, Tsinghua University* , Available online from www.sciencedirect.com.

[23] N Bhalla, Is the Mouse Click Mighty Enough to Bring Society to its Knees? *Computers & Security*, vol. 22, issue 4, pp 322-336, May 2003.