UML Modelling of Network Warfare Examples

N Veerasamy
University of Pretoria
Department of Computer Science
Pretoria, South Africa
nveerasamh@csir.co.za

JHP Eloff
University of Pretoria
Department of Computer Science
Pretoria, South Africa
jan.eloff@cap.com

***Abstract*—The aim of this paper is to clarify the concept of Network Warfare by looking at a typical example that illustrates both the exploitation and protection of information using various aspects of Information and Communication Technology (ICT). By using Unified Modelling Language (UML), the various role players, types of activities and sequences of actions can be represented in an illustrative format. This approach aims to elucidate Network Warfare in a more practical manner. The paper thus deals with four main issues that provide a motivation for modelling, an introduction to the models, the use case collaboration diagram and the sequence diagram of a typical example. The overall goal is to clarify the theoretical field of Network Warfare in a more practical manner.**

Keywords- ICT, Network Warfare, UML

I. MOTIVATION FOR MODELLING

Models provide the ability to explore a topic, show associated concepts and depict links. 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 [1]. Models can thus create understanding of complex topics. Conallen states that models can help to provide understanding of a system by simplifying some of the details, but it is important to determine the correct level of abstraction and detail [2]. Therefore, the use of models to clarify a complex topic like Network Warfare has numerous benefits. However, it is imperative to focus on the relevant details and not to deviate to very low-level internals of a system or problems at hand, such as the exact application to use or precisely how elements integrate. For this reason, as a means of introducing some critical aspects of Network Warfare, this paper uses UML modelling techniques.

A. Introduction to Unified Modelling Language

Unified Modelling Language (UML) has emerged as a dominant standard for modelling, as it meticulously captures and communicates the structure and behaviour of systems. According to Kobryn, the major benefit of this international standardisation is that specifications made in UML can be internationally recognized and accepted. [3]. The evolution of UML has gone through several releases, but its fundamental purpose of describing system interactions remains the same.

Furthermore, Jürjens states that even though UML has been developed to model object-orientated systems, one can also use UML to analyse systems that are not object-orientated by thinking of objects as components [4]. It is for this reason that UML was identified as an ideal means of analysing Network Warfare in further detail.

The UML standard will thus be applied to an example in Network Warfare to show the interaction and sequence of events. Cognisance should be taken of the fact that the modelling process required the formulation of actors and activities such that it would adequately convey a typical Network Warfare example. The diagram types that would be used in this paper are the use case collaboration diagram and a sequence diagram.

II. INTRODUCTION TO MODELS

Before the models of a use case collaboration diagram and sequence diagram can be described, it is important to discuss how the models were constructed. The reasoning behind the construction of the models is thus provided.

Fig 1 provides a summary of the introduction to the models. Firstly, the definition and attributes of Network Warfare are considered. Thereafter, various low-level techniques are **identified**. The low-level techniques will then be **classified** into high-level techniques that provide a level of abstraction. Furthermore, the validity of the high- and low-level techniques will be determined by arguing their **application** to Network Warfare

A. Consideration of Network Warfare Attributes

Network Warfare can be seen as taking place over Information and Communication Technology (ICT) networks to affect information processing capabilities and has the following attributes:

- Spans computer and network security [5], which will consequently be referred to as information security
- Covers both offensive and defensive activities [6]
- Consists of both legal and criminal acts [7]
- Affects both civilian and military domains [8] [9]
- Related to the concepts of infowar, information operations, hacking, hackivism, cyberterrorism and cybotage depending on motivations and techniques [10]

- Encompasses both technological solutions and strategic considerations [11]

While the attributes discuss significant aspects of Network Warfare, it would not be pragmatic to model using UML, as they are fairly high-level and descriptive. The attributes of Network Warfare do not explain the system functionality, behaviour, static representation or dynamic interaction.

Network Warfare needs to be elaborated in order to provide practical aspects that can be better modelled using UML. It is, therefore, proposed that a bottom-up approach be used to look at various low-level techniques that enable Network Warfare.

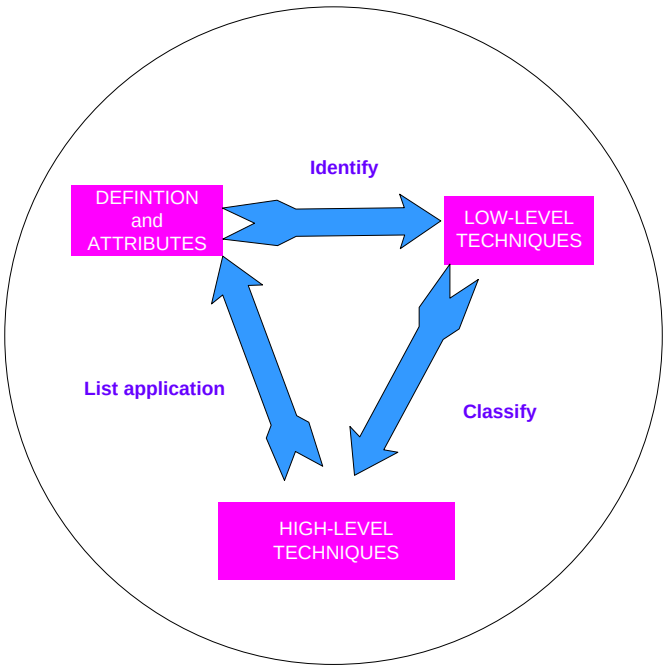

Figure 1. Summary of Introduction to Models

With reference to Fig 1, the low-level techniques will thereafter be classified into high-level techniques. The classification of the high-level techniques provides a level of abstraction that is necessary for modelling. The validity of the high- and low-level techniques will also be assessed against the attributes of Network Warfare to show the relevance of the techniques to the attributes and definition of Network Warfare.

Next the techniques of Network Warfare are identified, after which they are assessed against the attributes. This serves as a prelude to the proposed UML models.

B. Network Warfare Techniques

Information security is a multi-faceted field and plays a pertinent role in Network Warfare. Various techniques of information security exist and should be considered for the UML models. A literature study on information security and Network Warfare techniques was carried out.

Firstly, the works of Williers, Harris and Tittel are considered collectively. Identified techniques of information security and Network Warfare include: 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 [6] [12] [13].

Furthermore, Baker and Harris also discuss techniques like Intrusion Prevention, Personnel Security and Security Awareness as part of information security [14] [12].

Moreover, when considering the works of Theohandou, Tipton and Sowa, the following information security techniques emerge: Risk Analysis, Physical Security, Incident Response, Disaster Recovery Planning, Security Awareness, Legal, Regulations and Compliance [15] [16] [17].

In addition, Williers as well as Qingbao and Anwar discuss more offensive aspects of information security and Network Warfare like Hacking, Vulnerability Injection, Network Attacks, Denial of Capability, Interception and Blockage [6] [18] [19].

Various techniques that are core to information security and to Network Warfare were thus identified. The following summary of the techniques found in Network Warfare is given: Risk Analysis, Intrusion Prevention, Physical Security, Personnel Security, Cyber Forensics, Incident Handling and Emergency Response, Penetration Testing, Security Evaluation, Network Surveillance, Threat and Vulnerability Estimate, Network Attack, Vulnerability Injection, Hacking, Disaster Recovery and Business Continuity, Security Training and Awareness, Denial of Capability, Covert Communications, Interception and Blockage, Legal, Regulation and Compliance, Research, Innovation, Analysis and Maintenance, Attack and Manipulation Development and Software Code Review and Testing

These techniques should be adequately reflected in the study of Network Warfare. However, it would be more suitable to classify these techniques as a means of abstraction for the future models. This is carried out next.

C. Classification of Techniques

Table 1 was generated by listing low-level Network Warfare techniques and thereafter classifying the low-level techniques into high-level techniques. This provides a level of abstraction for the compilation of the UML models. The techniques tabulated were derived from the literature study and review of information security activity that form the basis of Network Warfare in Section II B.

TABLE I. TECHNIQUE CLASSIFICATION

High-level technique classification	Low-level technique
ICT Security	-Intrusion Prevention -Incident Handling & Emergency Response -Forensics -Research, Innovation, Analysis & Maintenance -Hacking -Vulnerability Injection -Interference/Denial of Capability -Covert Communications -Interception & Blockage -Network Surveillance
Risk Management	-Risk Analysis -Threat & Vulnerability Estimate
Disaster Recovery Planning	-Disaster Recovery Procedures -Business Continuity Plans
Personnel Security	-Personnel Security -Awareness & Security Training
Physical Security	-Physical Controls -Safety & Security Measures
Legal, Regulations & Compliance	-Policies, Standards, Laws & Guidelines -Update Safety & Security Measures -Security Evaluation (Aggressive Audit) -Penetration Testing
Application Development Security	-Software Code Review & Testing -Attack & Manipulation Development

In Table 2, a sample mapping is shown of the Network Warfare definition and attributes to techniques. This serves to show the relation between the attributes and techniques. The low-level techniques are ticked in columns of the corresponding attributes as a means of showing their application.

For example, all the low-level techniques span information security and, therefore, a tick is indicated for each of the techniques. Policies, Standards, Laws and Guidelines cover legal aspects and are, therefore, indicated to form part of the Legal and Criminal attribute. Hacking, Interference and Vulnerability Injection could all be criminal activities and could also be ticked for the legal and criminal attribute.

Techniques like Intrusion Prevention and Disaster Recovery Planning are defensive tactics, while Hacking, Vulnerability Injection and Attack and Manipulation Development are more offensive in nature and are therefore shown in the offensive and defensive attribute column. In addition, Forensics, Incident Handling and Emergency Response are relevant in both a military environment, as well as a civilian domain and could, therefore, also be ticked for the civilian and military attribute.

Similarly, Table 2 shows the application of other Network Warfare techniques to its attributes.

Network Warfare behaviour can thus be modeled using the listed techniques. The high-level classifications introduced in this section serve as abstraction for the Network Warfare UML models, which are described next.

TABLE II. APPLICATION TO NETWORK WARFARE

		Spans Info Security	Legal &criminal	Offence &defence	Civilian&Military	Hacking/vism Cybotage,	Infowar, Information Operations,	Technology and Strategy	ICT Infrastructure
ICT Security	Intrusion Prevention	√					√	√	√
	Incident Handling and Emergency Response	√			√			√	√
	Forensics	√			√			√	√
	Research, Innovation, Development and Maintenance	√						√	√
	Hacking	√	√	√				√	√
	Vulnerability Injection		√					√	√
	Interference/Denial of Capability	√	√	√			√	√	√
	Covert Communication	√						√	√
	Interception and Blockage	√	√	√			√	√	√
	Network Surveillance	√						√	√
Risk Management	Risk Analysis	√		√					
	Threat and Vulnerability Estimate	√		√					
Disaster Recovery	Disaster Recovery Planning	√		√	√				
Personnel Security	Personnel Security	√		√				√	
	Awareness and Security Training	√		√				√	
Physical Security	Physical Security	√		√					
Legal and Compliancy	Policies, Standards, Laws and Guidelines	√	√					√	
	Update Safety Measures	√							
	Security Evaluation	√							
	Penetration Testing	√							
Application Development	Software Code Review and Testing	√						√	
	Manipulation Development	√	√				√	√	

III. USE CASE COLLABORATION DIAGRAMS

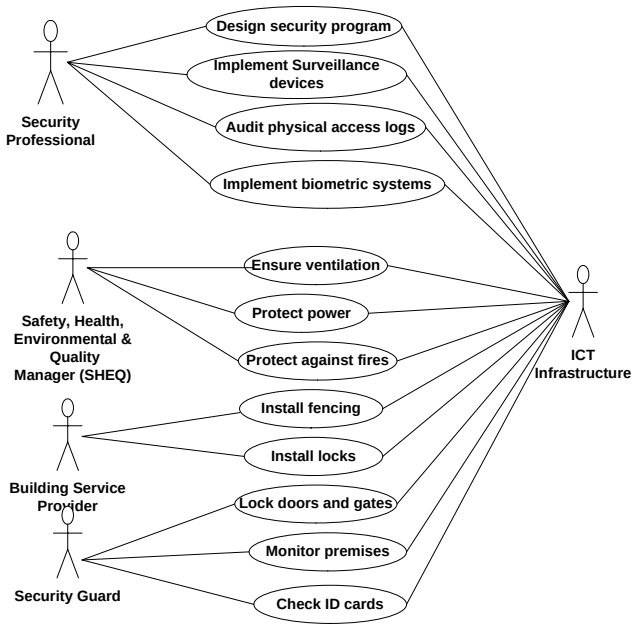

Figure 2. Use Case Collaboration Diagram for Physical Security

It was identified that a use case collaboration diagram would be useful to identify various actors and to show specific Network Warfare activities. Fig 2 shows the graphical representation of the technique of physically securing a network or system.

In the figure the originating actors are indicated on the left, and their activities run down the centre. To illustrate, at a strategic level, a security professional will be responsible for: designing the company's security program, ensuring that the surveillance devices are implemented, auditing the physical access logs and implementing the biometric systems for access control.

From a health and safety perspective, the Safety, Health, Environmental and Quality (SHEQ) Manager will ensure that adequate ventilation exists and that the premises are protected against fire and power disruptions.

At a structural level, the building service provider will address issues relating to the installation of fencing and locks. At an operational level, the security guard will be on duty to lock doors and gates, monitor the premises and checks identify cards. Overall, these activities take place on ICT infrastructure.

As is the case with Fig 2, when analysing most of the high-level techniques in Table 1, it was found that typical low-level techniques could be listed without the need for representation of intricate interaction in a model. However, this was not the case for the high-level technique of ICT Security. This category encompasses the most comprehensive listing of techniques, which in itself contains various activities that interact and overlap each other. It is for this reason that a more detailed use case collaboration and sequence diagram for ICT Security is proposed. Fig 4 shows a use case collaboration diagram representing an example stemming from the high-level technique ICT Security. ICT Security spans a wide range of activities and, therefore, Fig 3 merely tries to capture a snapshot of a typical use case. The use case collaboration diagram in Fig 3 has been constructed so that the diagram does not show the target actor. This is because all the activities take place on ICT infrastructure. Rather to show a range of actors and their responses, the diagram has been set up with offensive actors on the left and the defensive actors on the right. To interpret the diagram, read the activities of the offensive actors from left to right and the activities of the defensive actors from right to left.

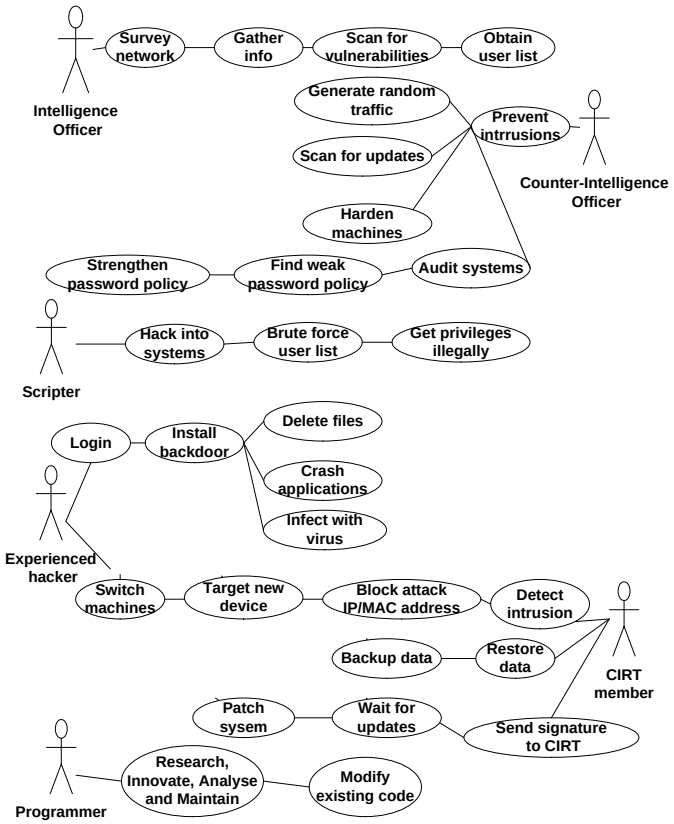

Figure 3. Use Case Collaboration Diagram for ICT Security

The example is loosely based on the hacking scenario of gathering information on a system vulnerability, illegally gaining privilege, installing a back-door, actual behaviour and deleting traces of intrusion [20]. A more detailed explanation follows.

In the military environment, two officers are tasked with intelligence-based activities. These two officers are the Intelligence (Int) Officer and the Counter-Intelligence (Counter-Int) Officer. The Int Officer can be responsible for network surveillance activities like scanning for vulnerabilities. While running a vulnerability scanner, an Int Officer may obtain a user list for the system. The Counter-Int Officer, on the other hand, seeks to deter possible intrusions and may thus

generate random traffic to prevent information leakage or scan for updates to later harden machines against exploits.

As part of a Counter-Int role, the system can also be audited. A poor password policy can be detected and then rectified to prevent password attacks in the future.

The next actor depicted in the model is a scripter. If a user list has already been obtained before the vulnerability is rectified, a scripter could typically write routine scripts to automatically brute force a password list and thus gain privileges to the system illegally.

This type of activity forms an elementary portion of hacking into systems. An experienced hacker will utilise user credentials to log into a system, install a backdoor, delete files, crash applications or infect with a virus.

On the defensive side, a Computer Incident Response Team (CIRT) member can detect an intrusion on the system and proceed to block the Internet Protocol (IP) or Media Access Control (MAC) address of an attacker. An experienced hacker could then switch machines, physically or virtually, and target a new device, like another server. In response to data deletion, a CIRT member could restore data that has been lost and ensure that data is backed up in preparation for a possible future crash. If a system is infected with a virus, a CIRT member can send the signature to a national CIRT centre. Thereafter, the CIRT member can wait for updates to patch the system and prevent future attacks.

IV. SEQUENCE DIAGRAM

Fig 4 shows the sequence diagram for an ICT Security example of hacking into a system and the response thereof. To simplify the model, the model restricts the actors to two, namely, an attacker from an offensive perspective and a LAN Support Personnel (LSP) from a defensive perspective.

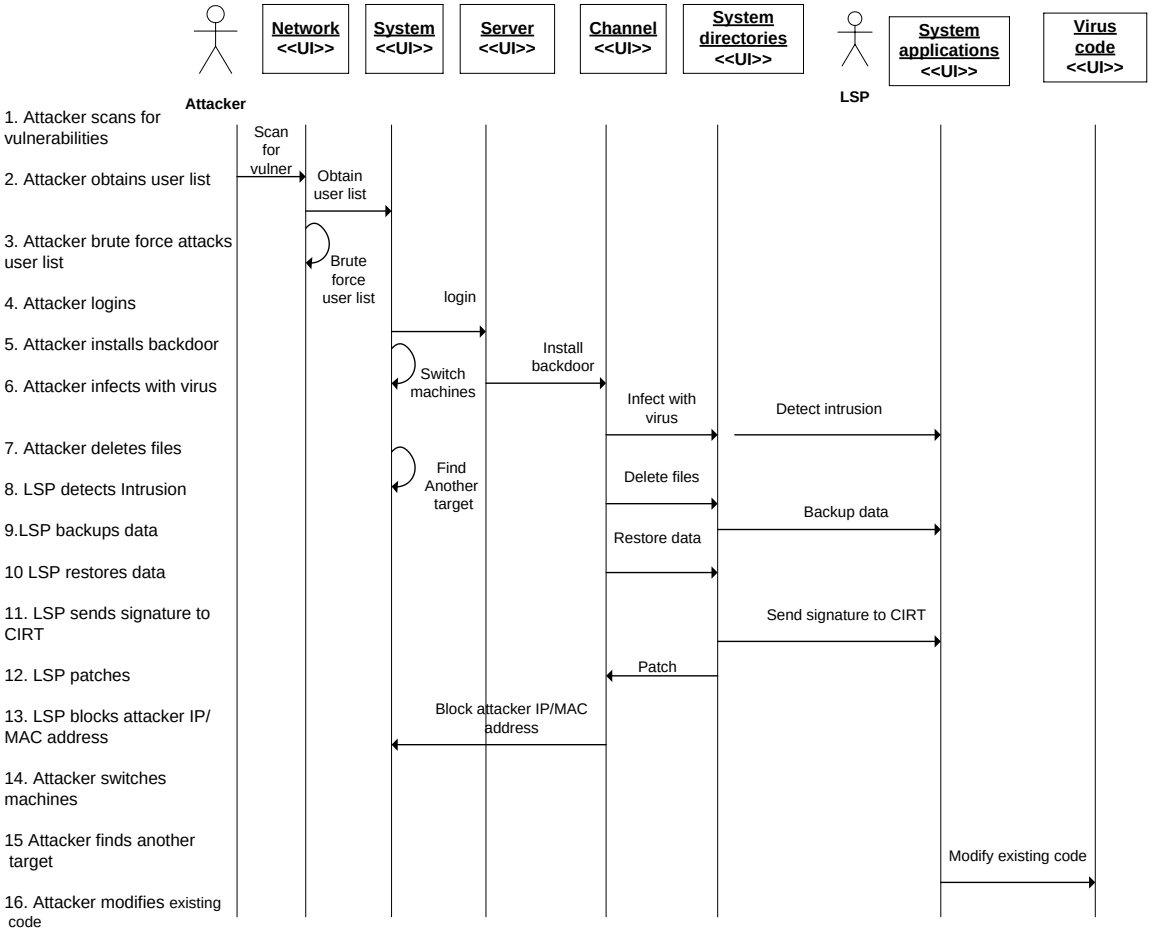

Figure 4. Sequence Diagram for ICT Security Example

An attacker commences his interaction with a network by scanning for vulnerabilities. While scanning, he obtains a user list of the network. He then carries out a recursive brute force attack to compile a complete list with all the users' credentials. An attacker then logs in to a plausible target, like a server, and installs a backdoor. Through this channel, he is able to infect the system with a virus, or delete files. After a LSP detects an intrusion, the data can be restored back to its previous state before the attack was carried out. Concurrently, data will be backed up to ensure that the system can be restored in future. A response to a virus infection would be to send the signature to the CIRT centre and to thereafter patch the system when an update is released. This can bring a system back to its previous state before an attack is carried out. In addition, a LSP can block the IP or MAC address of an attacker on the network. If an attacker can no longer gain access to the system, he could switch machines, either physically or virtually, and find another target. Once a virus signature is captured in an antivirus database, attackers often modify the code to create a new strain of the existing virus. Thus, the cycle of hacking can repeat itself, as an attacker tries to find other ways into the system with the network personnel attempting to prevent, detect and react to such attacks. The examples described have been explained sequentially. However, in practice it is often the case that various activities overlap each other. The aim of the proposed models was to isolate a pertinent example and describe a very basic attack and the response thereof. In this way, the goal was to view, from a high-level, the range of techniques required to establish Network Warfare, as well portray a very specific example.

V. CONCLUSION

This paper dealt with the research topic of studying Network Warfare strategy and techniques. This was achieved through the use of UML models to clarify the field of Network Warfare and the introduction of typical techniques that correspond with strategic and technological requirements. The models proposed a typical Network Warfare example and thus elucidated the field of Network Warfare through the practical example. This paper also introduced a classification of high-level and low-level techniques. This classification can help to determine what strategies and techniques should be applied in a Network Warfare environment and thus contribute to a Network Warfare Capability. The classification will further be used in upcoming research when the problem of determining a Network Warfare Capability will be addressed.

VI. REFERENCES

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

[2] J. Conallen, "Modeling Web application architectures with UML," Communications of the ACM, vol. 42, pp. 63-70, 1999.

[3] C. Kobryn, "UML 2001: A standardization odyssey," Communications of the ACM, vol. 42, pp. 29-37, 1999.

[4] J. Jürjens, Secure systems development with UML, New York: Springer Verlag, 2005, .

[5] A.J. Elbirt, "Information Warfare: Are you at risk?" Technology and Society Magazine, IEEE, vol. 22, pp. 13-19, 2003-2004.

[6] 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.

[7] J. Arquilla and D. Ronfeldt, "Cyberwar is coming!" Comparative Strategy, vol. 12, pp. 141-165, 1993.

[8] G.J. Stein, "Information Warfare," Airpower Journal, vol. 9, pp. 30-39, 1995.

[9] W. Elison, "Netwar: Studying rebels on the Internet." Social Studies, vol. 91, pp. 127-131, 2000.

[10] J. Arquilla and D.F. Ronfeldt, Networks and Netwars: The future of terror, crime, and militancy, Santa Monica, California, USA: Rand Corporation, 2001, .

[11] S. Park and T. Ruighaver, "Strategic approach to information security in organizations," in Proceedings of the 2008 International Conference on Information Science and Security, pp. 26-31, 2008.

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

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

[14] W.H. Baker and L. Wallace, "Is information security under control? Investigating quality in information security management," IEEE Security & Privacy, vol. 5, pp. 36-44, 2007.

[15] H.F. Tipton and M. Krause, Information security management handbook, Auerbach Pub, 2007, .

[16] M. Theoharidou and D. Gritzalis, "Common body of knowledge for information security," IEEE Security & Privacy, vol. 5, pp. 64-67, 2007.

[17] S. Sowa and R. Gabriel, "Multidimensional management of information security–A metrics based approach merging business and information security topics," in International Conference on Availability, Reliability and Security (ARES), pp. 750-755, 2009.

[18] L. Qingbao, G. Hongbo, X. Bing and J. Zhiyong, "Hardware threat: The challenge of information security," in International Symposium on Computer Science and Computational Technology (ISCSCT), pp. 517-520, 2008.

[19] M.M. Anwar, M.F. Zafar and Z. Ahmed, "A proposed preventive information security system," in International Conference on Electrical Engineering (ICEE), pp. 1-6, 2007.

[20] G.Y. Jeong, D. Seo, S.G. Kwon and J.H. Kim, "Intranet security evaluation using hacking techniques," in The 9th International Conference on Advanced Communication Technology, pp. 810-814, 2007.