International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:4, 2008

The Application of Non-quantitative Modelling in the Analysis of a Network Warfare Environment

N. Veerasamy, and JPH Eloff

***Abstract*—**Network warfare is an emerging concept that focuses on the network and computer based forms through which information is attacked and defended. Various computer and network security concepts thus play a role in network warfare. Due the intricacy of the various interacting components, a model to better understand the complexity in a network warfare environment would be beneficial. Non-quantitative modeling is a useful method to better characterize the field due to the rich ideas that can be generated based on the use of secular associations, chronological origins, linked concepts, categorizations and context specifications. This paper proposes the use of non-quantitative methods through a morphological analysis to better explore and define the influential conditions in a network warfare environment.

***Keywords*—**Morphological, Non-quantitative, Network warfare.

I. Introduction

NETWORK ware refers to the branch of Information warfare that deals with the computer and network aspects through which information is exploited and protected. "The core of computer network warfare is to disrupt the layers in which information is processed with the objective of seizing and maintaining control of network space [1]". Network warfare is thus a modern form of conflict in which computers and networks are used as the weapons with information serving as the leverage with control thereof providing a degree of dominating power over the opposition.

Network warfare crosses various domains and field and is nor longer just applicable to the military environment. "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 [2]". Modern forms of network warfare include all the computer and network security means through which computers are attacked and exploited (worms, denial-of-service and bots) as well as all the protective mechanisms being implemented (intrusion detection tools, anti-virus software and firewalls).

Computer and network security in itself is a multi-faceted field. According to the Information System Security Consortium (ISC^2), computer security is made up of various domains including Cryptography, Disaster Recovery, Telecommunications, Networking, Law and Ethics, Physical Security, Management and Operations Security [3]. A pertinent issue is therefore raised: The role of the various domains of computer security in a network warfare environment.

It can thus be seen that a means of conceptualizing and formulating the various strategic considerations and requirements in a network warfare environment would be beneficial in understanding this modern form of conflict in this the Electronic Age.

Modelling is an ideal means of investigating multi-faceted topics as exploratory techniques, free association, contextual information and links can be represented which then provides a credible depiction of the subject matter. These models can then serve the basis for various strategic decisions from policy development to budgetary decisions and technological advancements.

This paper therefore seeks to address the need to generate strategic requirements and capabilities in a network warfare environment by proposing the use of non-quantitative modeling through a morphological analysis. The paper thus provides a proof-of-application argument by providing a basic example. It should therefore capture the complex (contextual and interpretative) nature of the subject matter and impart insight into this pertinent field. Non-quantitative modeling through the use of morphological analysis supports the flourishing of prominent considerations whilst allowing for the logical arrangement thereafter to present and structure the influential findings.

The remainder of this paper is structured as follows:

Section II contains a brief overview of the use of modeling. Section III discusses the application of morphological analysis to the network warfare environment. Section IV addresses the approach used to utilize the non-quantitative modeling technique. Details of the formulated model is given in Section V. Finally we conclude with a brief discussion in Section VI and the conclusion in Section VII.

N. Veerasamy is with the Council for Scientific and Industrial Research in South Africa (+27 128412893; fax: +27 12841 5025; e-mail: nveerasamy@csir.co.za).

J. Eloff is the Head of Deparment and full professor at the Department of Computer Science, University of Pretoria.

The authors wish to thank the Council for Scientific and Industrial Research, The National Research Foundation and the ICSA research group at the Department of Computer Science at the University of Pretoria for its financial support.

II. Background

This section contains a brief overview of the functionality provided by modeling techniques in elucidating complex areas of study. The aim in this section is therefore merely to provide context and rationale to the use of models to represent the current positioning of the field of network warfare.

Models provide a means of reflecting both the ontological and epistemological components of any system/subject matter. As research topics can be very diverse and complex it may be necessary to adequately capture its depth and intensity whilst providing sufficient background information. Zwicky is said to have been developed General Morphological Analysis (MA) as a method for structuring and investigating the total set of relationships in a multi-dimensional, non-quantitative, problem complexes [1]and[4]. Non-quantitative modeling methods are thus one such means of providing inclusive views by encapsulating interlinking and influential considerations.

MA is a general method for structuring and analyzing complex fields which are inherently non-quantifiable, contain non-resolvable uncertainties (both antagonistic and non-specified uncertainty); cannot be causally modeled or simulated and require a judgmental approach [5]. Morphological modeling therefore seeks to enable the use of fair reasoning to reflect on and eventually describe the components in an intricate field of study. A morphological analysis thus serves to better decompose a multi-faceted area and thus expose its constituents for better study and understanding.

Non-quantitative models help create a better understanding of a topic as they allow for the relative exploration as a whole which can reveal objectives, consequences, dependencies and techniques amongst various other avenues of examination. By allowing the concepts to migrate in particular directions (sequentially or randomly) using non-quantitative techniques, a detailed inspection of the topic can be carried out. A morphological analysis provides a valuable and constructive means of representing complex relationships so that insight into the area can be gained, that otherwise could have been overlooked due to the intricate associations.

Ontological refers to existence in reality. In reference to computer science, ontology is the rigorous and exhaustive organization of some knowledge domain (that is usually hierarchical) and contains all the relevant entities and their relations [6]. Thus through a morphological analysis, all considerations that are real to network warfare can be meticulously identified and thus a focus on the essential requirements can be created.

Computer Aided Morphological Analysis offers the ability to capture and model areas of study for deeper insight and understanding of its complexity. The ability to encapsulate ideas and show relationships can be critical to elucidating a subject matter so as to emphasize the core elements and links. Computer Aided Morphological Analysis provides this ability that is so vital to decomposing a complex area into simpler concepts.

The rest of the paper will look at the application of Computer Aided Morphological Analysis to the field of network warfare. More specifically, the outcomes of influential considerations will be discussed to demonstrate the clarity and detail that can be provided once a social, political and technical topic like network warfare is explored. However, a motivation for the relevance of using non-quantitative modeling techniques to analyze network warfare is given firstly.

III. Motivation

The reasoning behind the use of morphological analysis to analyse network warfare will be elaborated in this section. Firstly Zwickly proposed that use of the concept of morphological analysis include not only the study of the shapes of geometrical, geological, biological and general material structures but also to study more abstract structural interrelations among phenomena, concepts and ideas, whatever their character may be [1]. Thus it can be seen that the application of morphological analysis is ideally suited to investigating (somewhat) intangible yet conceptual relationships between ideas relating to network warfare which by themselves encompass various contextual properties.

Secondly, a core aspect of network warfare entails the various computer and network security mechanisms and techniques that can be utilized to carry out network warfare. However, network warfare is not only concerned with the various technological solutions but also the contemplation of different requirements, strategic goals, directions and sub-functions that each specialized area in information security should deliver. “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 [7]”. Affecting human beings and their decisions, necessitates strategic, tactical, operational and managerial assessments to identify requirements and thereafter to evaluate the strengths and weaknesses of possible forms of action. Thus, formulating core requirements and strategic focus areas will be beneficial in establishing the baseline in a network warfare environment. A morphological analysis provides the capability to break down high-level concepts and focus on essential criteria to be evaluated. “Morphological analysis is a method for rigorously structuring and investigating the internal properties of inherently non-quantifiable problem complexes, which contain any number of disparate parameters [8] .”Morphological analysis thus provides a useful platform to explore the network warfare field to decompose the considerations and identify relationships by allowing for the hypotheses of different conditions and the generation of associated factors.

The justification of the application of morphological analysis to network warfare therefore lies in providing the ability to describe the more abstract (yet interlinked) field,

whilst revealing core components that can affect various strategic, tactical and technological decisions. It is hoped that by demonstrating the application of morphological analysis to network warfare, more clarity on the latest emerging trend, in this the Electronic Age, can be gained.

IV. Approach

In this section the approach of applying the non-quantitative modeling technique of a morphological analysis will be elucidated. Later sections will discuss the results of the analysis.

Zwicky summarises the five steps of the process as: (1) Problem to be solved must be very concisely formulated (2) Localise and analyse all relevant parameters (3) Construct the morphological box/matrix (contains solutions) (4) Scrutinize and evaluate solutions (5) Select and apply optimal solutions [1].

A similar technique was utilized during the study of network warfare using Computer Aided Morphological Analysis.

Both chaotic and organized thought processes can be catered for, due to the framework provided by the analyses technique. Ideas can be initially formulated and utilizing the spiral effect, spin-off concepts can be generated freely. Thereafter, stepwise breakdown allows for arrangement and control of the concepts to ensure that the model encompasses the topic as a whole. Thus, using morphological analysis, reflective views can be incorporated, whilst the model can also be based on verified data to eliminate interpretive inconsistencies. Computer Aided Morphological Analysis could be ideally applied to network warfare as the non-quantitative modeling technique allowed for the exploration of the various computer and network security factors, as well as the identification of objectives which help define the strategic directions needed in the field. During the application of morphological analysis, both reflective (authors' observations) and established views were incorporated to demonstrate the merging of outlooks to build a rational representation of the field.

After identifying the relevance of using morphological analysis techniques to investigating network warfare, the high-level issue to be addressed by the model, was formulated. Since network warfare could be implemented through various computer and network security practices, with different purposes, it was identified that clarity on specific objectives, techniques and motives would help define the field more appropriately. The problem statement and parameter specification therefore entailed defining the categories of objectives (and sub-objectives) together with the individual motives, high-level techniques and practical examples of each technique implementation. This served to demonstrate an overall network warfare methodology and motivation which covers much of the current state of computer and network security. The morphological matrix, depicting the relationships, was constructed and completed though a detailed analysis and research effort that consisted of investigating the current views on network warfare as well as applying the relevant computer and network security concepts. The pertinent fields in each category were therefore determined through an evaluation and study process that was based on substantiated data as well as private input to ensure that the model captured the essence of the field. Through a study of the concepts constructed in the matrix, relationships and dependencies could be identified. In this way, a methodical process (allowing for multi-lateral development) was followed.

After describing the approach of completing the model, a more detailed description of the findings will be given in the next section to help elucidate the field of network warfare.

V. Model/s

In this Section, a description of the results of the application of morphological analysis to network warfare will be given.

It should be noted that this paper depicts the practical use of morphological analysis to investigating network warfare and due to the detailed intricacies in the model, suitable examples of the results are given to demonstrate the applicability and functionality. This model is by no means a complete characterization of the field. However, key considerations have been captured and new parameters can be incorporated as they are identified.

The models to be provided in the next few sections are merely a demonstration that by using morphological techniques, relationships between messy problems can be better clarified. By using Computer Aided Morphological Tools the dependencies and associations can be captured and studied. In this paper, an example of a single relation that can be captured from each perspective is given. The construction of the matrix occurs initially and these are shown in the figures in the next two sections.

Arquilla and Rondfeldt discuss of the blurring of offense and defense in network warfare [2]. Similarly, the model also reflects these two (sometimes merging) perspectives: an offensive and a defensive outlook. In several cases, the activities of each side can overlap, for example network surveillance can be performed on a company's own networks to detect abnormalities whilst it can also be carried out to capture data from the opposition. However, in this model the two viewpoints have been separated due to the differing objectives. Explanations of each perspective follow in the next few sections.

A. Offensive Perspective

Elbirt summarizes the types of information warfare attacks as exploitative, manipulative (modification, corruption, deletion) and disruptive (denial-of-service [10]. These three categories of attacks were used as the underlying objectives of the offensive perspective. Thereafter various sub-objectives were identified and placed in the model (see Fig. 1).

Objective	Sub objective	Motive/Method	Technique	Practical Means/ Examples
Exploitation / Manipulation	Deception, Mimicry Subversion	Web (sites and application) vandalism	Web application vulnerabilities	SQL injection
				Cross site scripting
				Command Execution
				File /Directory Traversal
				Bad state management
			Hacking	
	Information Gathering	Target selection and attack means	Reconnaissance Surveillance	Port scanning, Services Detection
				Wireless sniffing
				Vulnerability Scanners
				Probing
				Traffic capture
		Disinformation campaigns	Smear drives on Bulletin boards, Anonymous emails, Blogs, Online forums, Adverts	Postings, Spoof emails, Online chatting
	Modification Corruption Deletion	Technical espionage	Virus(covert channel)	Coding
				Remote connection
				Sniffer programs
	Invasion of privacy	Smuggling of weapon	Viruses, Trojans, Worms Malware	
	Sabotage, Competitive /Economic Advantage	Infiltration by army	Social Engineering	Password cracking, Brute force
		Overpower	Privilege escalation	
		Bombing		
		Insider abuse	Phishing Fraud	
Denial of service	Resource abuse/ wastage Financial gain	Interference	Message Flooding Bots Jammers	
	Disrupt Prevent operation	Denial-of-capability(Hostage)	Physical disconnection,	Wireless encryption cracking
			Failure in network/computer	
			Deletion/Theft of critical data	

Fig. 1 Morphological Analyses Example of Offensive Perspective of Network Warfare

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 [9]". The unmasking of facts is represented as information gathering in the model. Deception, mimicry and subversion (malicious insertion) are sub-objectives for exploitative activities. Elbirt also goes on to condense the motivation driving these attacks by explaining that they may vary from financial gain to malicious destruction of data and property to invasion of privacy [10]. In essence, considerations from various sources were captured in the model to form the high-level framework.

Thereafter, the motive and method of the various objectives are given. Bhalla's review of offensive aspects of information warfare was incorporated into the model as they capture the essence of offensive motives/methods. These include: Web vandalism, disinformation campaigns, technical espionage, smuggling of weapons, infiltration by army, overpower,

bombing, interference, denial-of-capability (hostage) [11]. Furthermore the specific techniques and practical means were elaborated on to depict the functional implementation of these methods. The techniques and practical aspects of the model were based on various computer and network security technologies and practices. For example web vandalism makes use of web application vulnerabilities and hacking techniques which include SQL injection, bad state management, cross-site scripting, directory traversal, command execution, etc [12]. In addition these techniques can also be used to smuggle though weapons, or gather information to identify potential targets. In this way, various techniques extend beyond specific categories and through the use of morphological analysis the cross-domain extensions can be accurately captured.

The explanation given in this sub-section provides a brief overview of the offensive perspective of network warfare. Techniques and practical examples are often multi-functional and thus valid for various network warfare motivation/means categories. With the use of morphological analysis these cross-relations can be encapsulated and the model can easily be used to describe the complexity. In the next sub-section, the details of the defensive aspect of network warfare will be given.

Objective	Sub objective	Motive/Method	Technique	Practical Means/ Examples
Prevent	Guard Expose and eliminate weaknesses	Increase understanding of threats/ vulnerabilities	Security training	Good practices and security awareness
			Reverse engineering	Code reviews, (firewalls, audit trails
			Audits	Scanning tools
Detect	Identify Vulnerabilities	Develop strategy of deterrence	Network surveillance	Reconnaissance
		Implement an effective defence-in-depth strategy	Policies, guidelines, doctrine	Scanning Tools (vulnerability , intrusions)
		Risk Management	Implement technology to mitigate risks	Sniffer programs
	Security Assurance Ensure Compliance	Checking of security measures	Audits, Verifications, Certifications	Check and verify system
Recover		Emergency response and alarms	Intrusion detection, security tools (firewalls)	Patch updates, testing, roll-outs
		Develop capacity for reconstitution	Penetrating testing	Specify backups, chain-of-command & procedures
	Maintenance	Patch vulnerability		Examine evidence files
	Instil good practices	Develop a capacity for damage mitigation	Disaster Recovery Planning	
		Resumption of critical services	CERT	
		Damage assessment	Forensics	
	Ensure technologies are operational	Documentation of the incident	Analyse Audit and Intrusion Detection Data	
	Disciplinary/ Legal Action	Finding evidence of unauthorised activity		
		Users held accountable		

Fig. 2 Morphological Analyses Example of Defensive Perspective of Network Warfare

B. Defensive Perspective

Most institutions and individuals use a defensive mode of network warfare in their global cyber and network battles to protect data and resources. Fig. 2 shows a morphological analyses example of a defensive approach to network warfare. A functional paradigm of defensive information warfare is best described by the following actions: protect, detect, and react [13]. By using these three higher level objectives, the framework of the defensive perspective of network warfare was built into the model. Most practices and technologies try to guard against attacks, identify vulnerabilities, check for compliance, create awareness in users and in general ensure control mechanisms are operational.

Furthermore, Bhalla also summarises information warfare practices from a defensive perspective. These include: increase understanding of threats/vulnerabilities, develop a strategy of deterrence, implement an effective defence-in-depth-strategy, emergency response and alarms, develop a capacity for reconstitution, patch vulnerability, develop a capacity for damage mitigation, resumption of critical services, damage assessment, documentation of the incident [11].

Moreover, specific techniques and practical aspects of defensive network warfare are given. For example to prevent attacks and identify vulnerabilities, scanning and other monitoring tools can be used. Monitoring tools are also used to detect intrusions and thus can be shown to be an Emergency response and alarm method. A scanning tool can also be used in the basic steps of penetration testing to determine a vulnerability to exploit. The data can also be studied to determine the sequence of actions. In this way, an individual technique has been shown to be carried out by several practices across categories. Similar to the offensive network warfare approach, the defensive activities are also multi-functional. The use of the morphological analyses thus enables the depiction of interlinked references and relationships in an expedient and informative representation.

This section summarises the defensive network warfare paradigm by describing the pertinent motivations and techniques used to carry out protective objectives.

VI. Discussion

This paper covered some of the most pertinent aspects of network warfare. Additional issues or factors may be identified through further reflection of the topic. However, the description in this paper does demonstrate the application, use and support provided by the use of non-quantitative modeling tools.

Network warfare is, often compared to computer and network security, which itself consists of various domains. Through the use of the morphological techniques further strategic, tactical and operational issues relating to network warfare can be addressed whilst incorporating the technological solutions.

The model developed should therefore provide the basis to understanding the complex and inter-linked field of network warfare. The model seeks to facilitate the more structured breakdown of the encompassing topic to provide a more detailed and meticulous overview that provides insight in various decision making processes.

VII. Future Work

An introduction into the use and application of non-quantitative modeling techniques was given in this paper. The paper has merely served as an introduction to the use of morphological analyses in structuring the field of network warfare. However, more research will help build a better model to clarify the field of Network Warfare. Whilst, constructing the proof-of-application model, various shortcomings were already identified. Through, further study more refined and robust concepts can be captured with the described non-quantitative techniques, to more appropriately represent the field. More insight can be gained through further iterations of concept capture and relationships representation. Through the use of wider expert opinion or authoritative text a more extensive picture of the area of Network Warfare can be gained. Future work will entail, improving the model by evaluating initial categorization, concepts and relationships and the formulation of more comprehensive descriptions.

VIII. Conclusion

This paper considered the application of non-quantitative modeling in the analysis of a network warfare environment. Network warfare is a complex field comprising of various aspects of computer and network security. In addition, various strategic requirements also form a strong basis in the foundation of network warfare. Whilst building the model, it would often be discovered that a particular objective or technique did not strictly belong into one category. This discovery suited morphological modeling quite aptly as the functionality of this non-quantitative technique allows for showing the interrelations between abstract concepts.

In addition, in several cases, reasoning and background knowledge could be incorporated into the model with the support of rational judgment in morphological analysis. The model is quite inter-linked in that various techniques, motives and objections overlap across categories. However, by decomposing the system into the constituent objectives and techniques an overview of the field is provided.

Further research can be incorporated into the model as new techniques and practical implementations of the objectives are identified. This could reveal entirely new aspects that have not yet been explored. However, the description in this paper does demonstrate the functionality and support provided by the use of morphological modeling techniques in clarifying the intricate field of network warfare.

REFERENCES

[1] Zwicky, F. Discovery, "Invention, Research - Through the Morphological Approach", Toronto: The Macmillan Company, New York, 1969.
[2] Arquilla J & Rondfeldt D, "The Advent of Netwar", RAND, 1996.
[3] Harris, S," CISSP All-in-One Certification Guide", Mcgraw-Hill/Osborne, 2002.
[4] Zwicky, F. & Wilson A. (eds.), "New Methods of Thought and Procedure: Contributions to the Symposium on Methodologies", Berlin: Springer, 1967.
[5] Ritchey T, "Modelling Complex Socio-Technical Systems Using Morphological Analysis", Adapted from an address to the Swedish Parliamentary IT Commission, Stockholm, December 2002.
[6] The Free Dictionary, "Ontology", Available online from http://www.thefreedictionary.com/ontology, Accessed 14 march 2008.
[7] G J Stein, "Information Warfare", Airpower Journal, No 1, pp 30-39, Spring 1995.
[8] Ritchy T, "General Morphological Analysis", Adapted from the paper "Fritz Zwicky, Morphologie and Policy Analysis", presented at the 16th EURO Conference on Operational Analysis, Brussels, 1998.
[9] Wik MW, "Revolution in Information Affair", Available online from: http://www.kkrva.se/Links/Infokrig/Wik1.html, Accessed 13 February 2008.
[10] Elbirt AJ, "Information Warfare: Are you at risk? ", IEEE Technology and Society Magazine, 2003/2004.
[11] Bhalla N, "Is the Mouse Click Mighty Enough to Bring Society to its Knees", Computers & Security, vol. 22, issue 4, pp 322-336, May 2003.
[12] Sensepost Training Providers, "Hacking by Numbers: Cadet Edition", Adapted from the Cadet Training Edition course slides, November 2007.
[13] Panda B & Giordano J, "Defensive Information Warfare", Communications of the ACM, vol. 42 no. 7, pp 31-32, July 1999.

Namosha Veerasamy has obtained a BSc: IT Computer Science degree and a BSc. Computer Science (Hons) degree with distinction from the University of Pretoria. She is currently completing her Masters in Computer Science and is employed as a researcher at the Council for Scientific and Industrial Research (CSIR) in Pretoria.

Jan Eloff received a PhD (Computer Science) from the Rand Afrikaans University, South Africa. Since October 2002, he is Head of Department and full professor at the Department of Computer Science, University of Pretoria. He has published extensively in a wide spectrum of accredited international subject journals and organized various international and national conferences were. He has delivered papers at leading information security conferences on an international level.