Cyber War Retaliation Decision:
A Fuzzy Multi Criteria Decision Making Approach

Mhamed Zineddine, ALHOSN University Abu Dhabi, Abu Dhabi, UAE

ABSTRACT

Information Communication Technology (ICT) has become a core part of every organization. Any disruption in ICT's main infrastructure may have severe impacts and lead to huge losses. Governmental and military institutions' facilities, networks, and infrastructure are no exception. Defending the ICT military and public installations and infrastructure is vital in both times of peace and war. This study proposes a decision model using the appropriate criteria and fuzzy multiple criteria decision making to select the right action after a cyber-attack. The results show that the fuzzy multiple criteria model constructed in this study could indeed mitigate the inadequacies and uncertainties surrounding the decision to retaliate after a cyber-attack.

Keywords: *Cyber War, Decision Making, Fuzzy Logic, IT Security, Multiple Criteria*

INTRODUCTION

Information Communication Technology (ICT) has become a core part of every business. As Bruce (1998) explains, IT has become a salient enabler of business strategies in areas of mass customization, competitive differentiation, quality improvements, and process automation and improvement. ICT affects the entire spectrum of retail, manufacturing, service, defense, and military institutions. ICT provides critical support for the developed economies through support of civil infrastructure, public safety, and national security. Nowadays, organizations operate in a dynamic, fast-changing environment due to a number of factors, such as technical innovations, new and creative ideas, strategic alliances, acquisitions and mergers and a culture of continuous change (Ekstedt et al., 2005). On one hand, "The interconnectedness of economies, rapid dissemination of news, and improved access to communication and information of all types" via ICT has given more power to individuals and fostered globalization (Fritz, 2008). On the other hand, the information assets of organizations have been stored and exchanged mostly in a digital format, which makes these assets vulnerable. As Qu (2001) points out, these assets include the intellectual property, products, as well as classified and private information about business partners and customers. Modern business practices require that these assets have to be available, reliable and accessible by customers, employee and partners on-site and at a distance. The digital world in

DOI: 10.4018/ijcwt.2011100102

which these assets are stored (cyber-space) is as vulnerable to attacks, as it is accessible.

It is worse if these assets are of a military kind. Military information and communication infrastructure in cyberspace has become a vital part of modern warfare and therefore has to be trusted and resilient. For instance, companies involved in military hardware making are a potential target for cyber-attacks. The recent attack on "Mitsubishi Heavy" and other military hardware makers in Japan (Kelly et al., 2011) is a living example. The infection of U.S. unmanned vehicles operating in Afghanistan and other warzones is also alarming (Schachtman, 2011). The aim of planning, designing, and implementing ICT security best practices is not only to ensure the confidentiality and the integrity of the data produced and used, but also to sustain the availability of the Information Systems (IS) (Davies, 1986; Forcht, 1994; Pfleeger, 1997). Wars of the 21st century will be much different from older ones (Arquilla & Ronfeldt, 1997). ICT will play a dual role in future wars; it will be beneficial and risky at the same time.

The remainder of this paper is structured as follows. The second (following) section relates to the background of the study, which reviews some of the recent studies relating to cyber war. The third section looks at the problem/research questions, while the fourth section states the research design and methodology adopted in the study; the exploration and selection of the suitable model and the numerical application of the model. The fifth section gives recommendations. The sixth section presents limitations and assumptions. The seventh section concluded the paper.

BACKGROUND OF THE STUDY

In a world without peace, the approach to war is changing fast. In the near future traditional warfare may become as outdated as wars with horses and swords. Today's wars are still bloody for both sides. Nuclear warfare has been proven to be disastrous for human kind. The main aim of past wars is to destroy the enemy's infrastructure such as dams, factories, military installations, etc. Currently, one country's social, military, economic, telecommunications, financial, and other systems in which IT is embedded have to be protected and defended. The enemy's systems has to be studied and analyzed to be attacked and taken down or used for intelligence gathering in case of war. Many indicators suggested that cyber war may be the future. Historically, spies, clerical mistakes, and simple human foils have consistently weakened technically strong military security systems (Stallings & Brown, 2008). Nowadays, extensive use of telecommunications systems connected to the cyber space made these systems remotely vulnerable. When wars strategies and tactics are a secret, cyber war in Estonia, although, short lived, proved to be effective to inflict and hurt the Estonian economy (Laudon & Traver, 2008). IT security is often thought of as securing digital assets such as data, services, etc., against hackers and crackers. IT is embedded in what made up the core of most societies. A well-orchestrated and sophisticated attack conducted by professionals/e-military can inflict serious damage and impact the way of life of the targeted countries. The United States of America is planning to control their side of the cyber space using a kill switch. However, this approach is debatable. According to the Department of Homeland Security, "Section 706" is one of the authorities the President would rely on if the nation were under a cyber-attack (Lieberman & Collins, 2010).

ICT has been changing the nature of the strategies, tactics, military structure and doctrines that will be adopted in future conflicts. Competing on a global scale without the use of ICT related technologies might cause financial and significant military disadvantage (Fritz, 2008). A conflict involving ICT infrastructure might have a significant financial and military impact. Arquilla and Ronfeldt (1997) pioneered two terms for these types of conflicts and issues: cyber war and netwar. Cyber war refers to knowledge based military oriented conflicts; netwar refers to societal issues often involving