Chapter III
Information Warfare: Survival of the Fittest

Pamela Ajoku
University of Pittsburgh, USA

ABSTRACT

Even though weapons and money are considered important factors for running a modern world, at the end of the day, it is all about controlling and exploiting information for political, military, economic, and commercial advantage. The objective of this chapter is to present a basic understanding of the concept of Information Warfare (IW) and the need for relevant strategies to aid its successful implementation. IW is an important topic in this electronic era and within enterprises, security strategies, tools, and processes are essential in order to maintain a competitive advantage against an adversary or group of adversaries. In this chapter, a Survival of the Fittest IW (SFIW) conceptual framework is presented based on the adaptive nature of IW, and a case study is used to discuss its validity.

INTRODUCTION

Various groups provide definitions for Information warfare (IW) based on their own contexts. For example, IW within a military context is any action to deny, exploit, corrupt, or destroy the enemy’s information and its functions while exploiting internal information functions. Although it has been defined in several different ways, the term has appeared increasingly in books, articles, professional military journals, and official publications (DiNardo & Hughes, 1995). In the mid-nineties, the IW concept became popular within certain circles of the U.S. defense establishment as a result of the indisputable fact that information and information technologies (IT) are increasingly important to national security in general, and warfare specifically (Libicki, 1995). There are techniques to mastering IW, and those who do master these techniques will find themselves at an advantage over those who have not.

IW is based on the assumption that information technologies have developed to the point where they can now be employed as a weapon in their own right, and thus wars can be won or lost without shots being fired (Ryan, 1995). The driving forces behind IW include the increasing recognition of information as a strategic asset and the continuing evolution of technology. As stated in a comment by the Washington Post, Schwartau (1996) reports that information warriors could modify credit reports, bank accounts, driving records, and plane reservations. Such malicious acts could bring the stock exchange to a halt. Nothing is safe, and our vulnerabilities come through loud and clear. The possibilities are enough to induce paranoia. As a result, IW is increasingly important to the military, business, and intelligence community. However, eradicating information attacks is not a realistic expectation. A more pragmatic approach would be to protect information and other resources by thoroughly understanding IW and developing formal frameworks to ensure its successful implementation.
**Information Warfare**

IW involves strategies and multilayered attacks. Most of the time, these strategies and attacks are complex. Recently, in view of an increase in terrorist activities, governments are beginning to expand computer network attack capabilities in a silent information war. The inherent vulnerability and accessibility of the Internet makes such a war very possible and easy to achieve. Advanced IW methodologies include creating huge networks of remote-controlled machines or “botnets” that attack corporate or government Web sites or send out false messages. News reports also confirm the significance of IW in the 21st century. For example, the Washington Post (Wolf, 2006) stated that the U.S. Airforce was setting up what would become a new four-star command to fight in cyberspace, and stated that the U.S. had already come under attack from China among others. Other recent headlines, like one from the New York Times (Markoff, 2007), confirm that botnets are secretly installing themselves on millions of personal computers and using the collective powers of the evolved network to commit Internet crimes.

The problem of cyberwarfare is not only for well-known or relatively large countries. Cyrus Farivar (2007) in a recent article described the small, wired country of Estonia, in which parking meters can be paid for via cell phone, Wi-Fi can be accessed at every gas station, and national elections can be voted for via personal computers, but is the first government to get targeted for large-scale cyberwarfare. Also, there are various levels and scopes associated with information warfare. Thus, in studying the details surrounding IW, it is important to acquire background information on the topic, and thus the following section provides a background for foundational IW-related elements. A Survival-of-the-Fittest IW framework is then presented, Followed by an analysis of the proposed framework, while the chapter concludes in with framework limitations and a summary.

**BACKGROUND**

Information has become a strategic and valuable resource, as predicted by Arquilla and Ronfeldt (1993). Whoever controls information flow has a tremendous advantage: “perfect information” for oneself, and imposed ignorance—through either denial or corruption—for an enemy (Meilinger, 1999). As a strategic resource, information can be managed, lost, transferred, deleted, edited, interrupted, fabricated, or enhanced. The availability of information in a digital format makes it more powerful as a weapon. Information plays critical roles in:

- The elimination of ignorance or the creation of awareness
- The creation of actual or implied safety
- The reduction of uncertainty
- The elimination, minimization, or structuring of complexity

These roles take effect on the physical domain, which in turn controls various economic, political, military, and business realms and decision-making.

As a result of the critical roles information plays, it has been employed in a modern type of warfare, now popularly termed Information Warfare (IW). Based on its growing popularity, there is a lot of debate on what IW actually is. At this time, IW may be considered a conceptual framework that enables some degree of information superiority. It uses technology and other methods such as electronic jammers and deception to achieve or promote specific objectives over a well-defined adversary or group of adversaries. Countries, organizations, and individuals engage in IW with the main objective or goal of diminishing the adversary’s power, control, and/or competitive advantage. IW is either used for defensive or offensive purposes, and is practiced at a local, national, and global scale within military, political, and business contexts.

The players in IW scenarios can take on offensive, defensive, or dual roles. Offensive IW may include (and is not limited to) eavesdropping, psychological operations (PSYOPs), distortions, computer break-ins, viruses, worms, Trojan horses, hoaxes, fabrication, and harassment. On the other hand, defensive IW may focus on cryptography, codes and passwords, biometrics, access controls, filters, and firewalls. IW is also known as I-War or Cyberwar. The Internet, with its ubiquitous characteristics, has also gone a long way to promote IW. The past few years have seen governmental, military, and commercial organizations widely adopt Web-based commercial technologies because of their convenience, ease of use, and ability to take advantage of rapid advances in the commercial market (Jajodia, Ammann, & McCollum, 1999). However, with the increasing reliance on internetworked computer resources comes an increasing vulnerability to IW.

The concept of an information war may seem a bit over the top. However, the origin of the term “Information Warfare” dates back to the early and mid-nineties...
Related Content

Privacy Preserving and Efficient Outsourcing Algorithm to Public Cloud: A Case of Statistical Analysis
[www.igi-global.com/article/privacy-preserving-and-efficient-outsourcing-algorithm-to-public-cloud/201507?camid=4v1a](www.igi-global.com/article/privacy-preserving-and-efficient-outsourcing-algorithm-to-public-cloud/201507?camid=4v1a)

A Hybrid Concept of Cryptography and Dual Watermarking (LSB_DCT) for Data Security
Ranjeet Kumar Singh and Dilip Kumar Shaw (2018). *International Journal of Information Security and Privacy (pp. 1-12).*

Behavioral Advertising Ethics
[www.igi-global.com/chapter/behavioral-advertising-ethics/46345?camid=4v1a](www.igi-global.com/chapter/behavioral-advertising-ethics/46345?camid=4v1a)

Overview of Knowledge Discovery in Databases Process and Data Mining for Surveillance Technologies and EWS
Inci Batmaz and Güser Köksal (2011). *Surveillance Technologies and Early Warning Systems: Data Mining Applications for Risk Detection (pp. 1-30).*
[www.igi-global.com/chapter/overview-knowledge-discovery-databases-process/46802?camid=4v1a](www.igi-global.com/chapter/overview-knowledge-discovery-databases-process/46802?camid=4v1a)