Chapter III
Ten Information Warfare Trends

Kenneth J. Knapp
United States Air Force Academy, USA

William R. Boulton
Auburn University, USA

ABSTRACT

This chapter discusses the rapid entry of information conflicts into civilian and commercial arenas by highlighting 10 trends in information warfare. The growing societal reliance on cyber technologies has increased exposure to dangerous sources of information warfare threats. Corporate leaders must be aware of the diversity of potential attacks, including from high-tech espionage, organized crime, perception battles, and attacks from ordinary hackers or groups sponsored by nation-states or business competitors. Based on a literature review conducted by the authors, we offer an information warfare framework that contains the ten trends to promote a greater understanding of the growing cyber threat facing the commercial environment.

INTRODUCTION

Commonly regarded as a military concern, information warfare is now a societal issue. While the bulk of the cyber war literature addresses the military dimension, information warfare has expanded into non-military areas (Cronin & Crawford, 1999; Hutchinson, 2002). After reviewing 16 years (from 1990 to 2005) of literature, this chapter identified ten important trends. While individually the trends are not surprising, we integrate the trends into a framework showing how information warfare has moved beyond the military dimension and into the commercial world as well. This expansion into the commercial world presents a growing threat to information managers who are responsible for protecting commercial information assets.

Given the high availability of Internet-based, low-cost cyber weapons that can target civilian information assets, there is a growing threat to the economic stability of modern societies that depend on today's commercial infrastructures. Because conventional military missions are often not available and do not

traditionally include the defense of commercially operated infrastructures (Dearth, 1998), business managers should accept this responsibility and plan to defend themselves against growing cyber threats. The trends described in this chapter together provide an integrated framework that helps us understand the ways which information warfare is spreading into civilian and commercial arenas.

INFORMATION WARFARE IN CONTEXT

Information warfare is a relatively new field of concern and study. The late Dr. Thomas Rona reportedly coined the term *information warfare* in 1976. Since then, many definitions emphasized the military dimension. Libicki (1995) offered seven categories of information warfare that are replete with military terminology: command and control warfare, intelligence-base warfare, electronic warfare, psychological warfare, hacker warfare, economic information warfare, and cyber warfare. Webster's New World Dictionary defines *conflict* as (1) a fight or war and as (2) a sharp disagreement, and defines *warfare* as (1) the action of waging war; armed conflict and as (2) a conflict or struggle of any kind. In this chapter, we use *conflict* and *warfare* interchangeably.

Today, we use the terms *information war* and *cyber war* to explore a range of conflict types covering political, economic, criminal, security, civilian, and military dimensions. Testifying before Congress in 1991, Winn Schwartau stated that poorly protected government and commercial computer systems were vulnerable to an "electronic Pearl Harbor" (Schwartau, 1998, p. 56). Others describe information warfare as the 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). Cronin and Crawford (1999) proposed an information warfare framework that extends beyond military dimensions. They argue that information warfare will intensify, causing potentially serious social problems and creating novel challenges for the criminal justice system. Cronin and Crawford (1999) consider four spheres where information warfare may become commonplace: military, corporate-economic, community-social, and personal.

Table 1. Information warfare framework

Information Warfare Characteristic	1990	2005
1. Computer-related security incidents reported to CERT/CC	252 incidents	137,529 incidents (year 2003)
2. Entry barriers for cyber attackers	High barriers	Low barriers
3. Forms of cyber-weapons	Few forms, lower availability	Many forms, high availability
4. Nations with information warfare programs	Few nations	> 30 nations
5. Economic dependency on information infrastructures	Partial, growing dependency	Heavy dependency
6. Primary target in information conflicts	Both military & private targets	Increasingly private targets
7. Cyber technology use in perception management	Global TV, radio	Ubiquitous, global multi-media
8. Cyber technology use in corporate espionage	Less substantial	Substantial & increasing
9. Cyber technology use in organized crime	Less substantial	Substantial & increasing
10. Cyber technology use against individuals & small businesses	Less substantial	Substantial & increasing