CYBER-WARFARE THREATENS CORPORATIONS: EXPANSION INTO COMMERCIAL ENVIRONMENTS

Kenneth J. Knapp and William R. Boulton

KENNETH J. KNAPP is an assistant professor of management at the U.S. Air Force Academy, Colorado. He earned his doctorate in management information systems at Auburn University, Alabama. He can be reached at kenneth.knapp@usafa.af.mil.

WILLIAM R. BOULTON (D.B.A. — Harvard University) is the C.G. Mills Professor of Strategic Management at Auburn University, Alabama. He is widely published and has conducted numerous technology benchmarking studies for U.S. government agencies.

On the basis of a review of information warfare literature from 1990 to mid-2005, this article presents a framework of 12 important trends. These trends demonstrate the transformation of information warfare from primarily a military issue into a major commercial issue as well. Corporate IS managers need to understand the growing cyber-war threats and implement appropriate strategies to mitigate risk.

COMMONLY REGARDED AS A MILITARY concern, information warfare is now a societal issue. Although the bulk of the cyber-war literature addresses the military dimension, information warfare has expanded into non-military areas (Cronin, 2002a, 2002b; Cronin and Crawford, 1999; Hutchinson, 2002). After reviewing almost 16 years (from 1990 to mid-year 2005) of information warfare literature, we identified 12 important trends. Although 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 shift into the commercial world presents a growing threat to information managers who are responsible for protecting organizational information assets.

The high availability of Internet-based, low-cost cyber-weapons that can target civilian information assets is a growing threat to the economic stability of modern societies that depend on today's information infrastructures (Bush, 2003). A survey of Fortune 1000 companies found an annual 64 percent growth rate in cyber-attacks being carried out through the Internet (Bagchi and Udo, 2003). 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 these growing threats.

Despite the increasing information warfare threat, business managers often do not understand or take the actions needed to provide

The 12 trends described in this article provide the impetus for developing an integrated framework that helps us understand the ways in which information warfare is spreading into civilian and commercial arenas.

appropriate information security (Austin and Darby, 2003; Porter, 1996). In a 2004 survey, 874 Certified Information System Security Professionals (CISSPs®) ranked top management support as the most critical information security issue facing organizations today. It even outranked other important security issues such as malware (malicious software), spam, patch management, business continuity, and network security concerns regarding firewalls and intrusion detection (Knapp, Marshall, Rainer, and Morrow, 2004).[1]

The 12 trends described in this article provide the impetus for developing an integrated framework that helps us understand the ways in which information warfare is spreading into civilian and commercial arenas. To aid practitioners, this article outlines appropriate cyber-strategies for effective information security management. For academics, a research agenda is recommended.

DEFINING INFORMATION WARFARE AND ITS 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 information warfare definitions have emphasized the military dimension. Libicki (1995) offered seven categories of information warfare that are replete with military terminology: command and control warfare, intelligence-based 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 (2) a sharp disagreement, and defines *warfare* as (1) the action of waging war; armed conflict, and (2) a conflict or struggle of any kind. In this article, 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 (1998, p. 56) stated that poorly protected government and commercial computer systems were vulnerable to an "electronic Pearl Harbor." 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, 2002a). In the *National Strategy to Secure Cyberspace* (Bush, 2003), the complex cyber-challenge is divided into five levels of security problems: home users and small businesses, large enterprises, critical infrastructure sectors, national vulnerabilities, and the global information grid of networked systems.

LITERATURE REVIEW APPROACH

Although other published information warfare frameworks exist (e.g., Friman, 2001), few focus on the changing context from military to commercial environments. An exception is the framework proposed by Cronin and Crawford (1999), who argue that information warfare extends beyond military associations into communities that understand the consequences of pervasive computing in society. They consider four spheres where information warfare may become commonplace: military, corporate–economic, community–social, and personal. In the present study, we build on Cronin and Crawford's framework by searching the literature for detailed evidence of the expanding context of information war. Based on an extensive literature review of both scholarly and practitioner outlets, we first identify 12 major trends indicating how cyber-warfare has expanded into civilian and commercial environments. Our integrated framework of these 12 trends is presented in the following section.

CYBER-WARFARE TRENDS

A review of the cyber-warfare literature for major trends suggests that a paradigm shift has taken place. The framework of 12 trends illustrated in Table 1 demonstrates that information warfare has moved beyond the military arena and into civilian contexts in a way consistent with the Cronin and Crawford (1999) framework. The following paragraphs describe each of the 12 trends in detail.

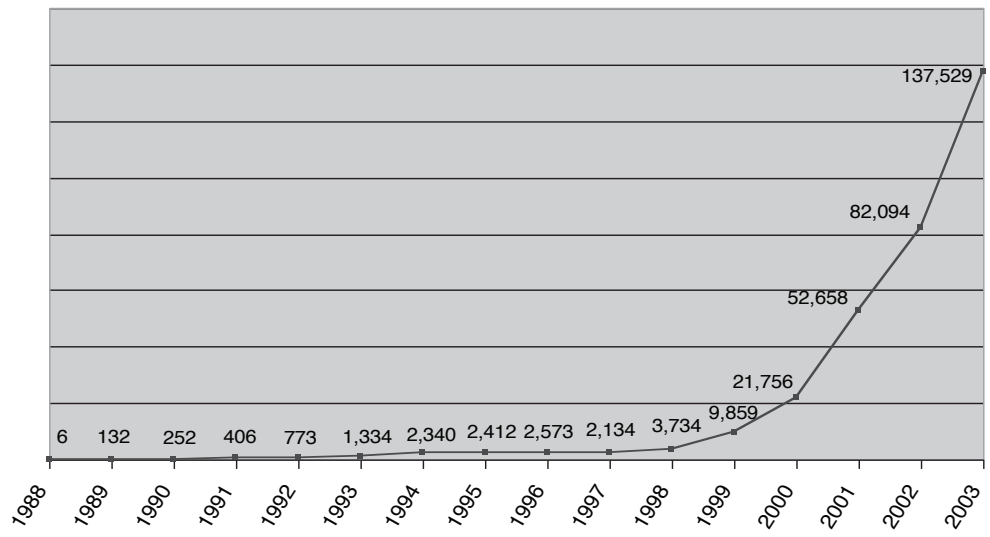
Computer-Related Security Incidents Are Widespread

Two highly referenced security incident measures come from the CERT/CC[2] and the annual CSI/FBI[3] survey. Based on CERT and CSI information: (1) security incidents are prevalent, (2) private institutions are the target of a large number of cyber-attacks, and (3) many incidents receive no public acknowledgment. Figure 1 illustrates the growing number of incidents reported to the CERT/CC from 1988

TABLE 1 Cyber-Warfare Framework

Cyber-Warfare Characteristic	1990	By 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 multimedia
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
11. Cyber-insurance market	Low demand	Moderate demand; >20 insurance offerings
12. Information security professionals	Low demand; few certifications	Higher demand; >35,000 CISSPs

FIGURE 1 Incidents Reported to CERT/CC, 1988–2003



to yearend 2003. Note the significant rise since 1998.

Although the security incident numbers appear large, they may actually be underreported. Respondents to the annual CSI/FBI survey indicate that more illegal and unauthorized cyberspace activities occur than many corporations admit to their clients, stockholders, and business partners or report to law enforcement. For example, based on the 2002 survey report, 90 percent of respondents, primarily from large corporations and government agencies, had detected computer security breaches, but only 34 percent of these respondents reported such intrusions to law enforcement agencies. In 2005, although fewer intrusions were reported, only 20 percent of respondents reported them to law enforcement, primarily because of concerns with negative publicity (Computer Security Institute, 2002; Gordon, Loeb, Lucyshyn, and Richardson, 2005; Richardson, 2003).

Entry Barriers Are Low for Cyber-Attackers

Early generations of cyber-weaponry (i.e., hacker tools) required technical knowledge for effective use. For instance, some hackers of the 1960s were students at MIT (*PCWorld*, 2001).

The hacker environment began changing in the early 1990s.

In the 1970s, system hackers were profiled as highly motivated, bright people with technical knowledge who often worked in university or business computer centers (Parker, 1976). Robert Morris, Jr., a graduate student at Cornell University and son of a chief scientist at the National Security Agency, developed the 1988 Internet worm that infected 6,200 computers, costing an estimated $100 million in cleanup (Zviran and Haga, 1999). Compare this to the teenage hacker typified by the main character in the popular 1983 movie *WarGames*. Although this teenager stereotype may hold some truth, much of the early hacking required advanced skills, such as knowledge about computer operating systems or network protocols.

The hacker environment began changing in the early 1990s. Technical barriers began to fall as downloadable and graphic-interfaced tools became widely available.[4] A notorious incident occurred in the late 1990s. In a series of events labeled Solar Sunrise, a group of teenage hackers, under the guidance of an 18-year-old Israeli mentor, gained access to numerous government computers, including 11 at U.S. Air Force and Naval bases (Key, 2004). Solar Sunrise served as a warning that serious hacking capabilities are within the grasp of relative non-experts.

Testifying before Congress in 1999, CIA Director George Tenent stated that terrorists and others are recognizing that information warfare tools offer a low-cost way to support their causes. Many of these tools are Windows-based, require minimal technical understanding, and are available as freeware. By 2002, one IS security professional had amassed a database of more than 6,000 hacker sites believed to contain only a part of the better hacker tools (Jones, Kovacich, and Luzwick, 2002).

Today, networked organizations employ sophisticated defensive devices such as firewalls, intrusion detection systems, and proxy servers (Sequeira, 2003). Unfortunately, many network devices are either improperly configured or have known vulnerabilities, leaving significant opportunities for even low-skilled hackers using prepackaged tools. Additionally, intruders often cleverly dupe employees into giving away information (social engineering), such as important passwords, and then use this information to hack into the heart of corporate networks (Mitnick, 2003). It no longer takes a technically competent person to assault an information system. Organizations must be vigilant against a wide variety of sophisticated *and* unsophisticated threats executed by technical and nontechnical hackers.

Dangerous Forms of Cyber-Weapons Have Emerged

The first electronic message boards for hackers appeared around 1980. Once available, these boards allowed the rapid sharing of hacker tactics and software, including distributed denial-of-service (DDoS) tools. This software was responsible for the February 7, 2000, attack that effectively shut down major Internet sites such as Yahoo, EBay, Amazon, E*Trade, and CNN.

Over the past 20 years, wide ranges of formidable cyber-weapons have become more affordable and available, from keystroke and eavesdropping devices to high-energy radio frequency (HERF) and electromagnetic pulse (EMP) generators. An attacker can build an E-bomb, designed to "fry" computer electronics with electromagnetic energy, for as little as $400 (Wilson, 2001). A demonstration of an E-bomb occurred in 1994. According to a London *Sunday Times* report, the Defense Research Agency believed HERF guns initially blacked out computers used by London's financial houses. Cyber-terrorists then extorted millions of British pounds by threatening to totally knock out these financial computer systems (*Sunday Times*, 1996). As technology advances, we can expect smaller and more dangerous cyber-weapons to emerge.

Many Nations Have Information Warfare Capabilities

In the early 1990s, few nations had an organized information warfare capability. By 2001, more than 30 nations were believed to have information warfare programs, including India, China, Taiwan, Iran, Israel, France, Russia, and Brazil (Adams, 2001). In the 2003 CSI/FBI survey, 28 percent of respondents identified foreign governments as a likely source of attack against their systems.

China is an example of a nation that is improving information warfare capabilities (Rhem, 2005). Some attribute the following 1995 statement to Chinese Major General Wang Pufeng:

> In the near future, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness. This trend will be highly critical to

TABLE 2 Key U.S. Federal Agencies and Assigned Sectors

Lead U.S. Federal Agency	Designated Infrastructure Sector
Environmental Protection Agency	Water supply
Department of Treasury	Banking and finance sectors
Department of Energy	Power, oil, gas production
Department of Commerce	Information and communications
Department of Transportation	Aviation, highways, mass transit, pipelines, rail, waterborne commerce
Department of Justice/FBI	Emergency law enforcement

> achieving victory in future wars. (Jones et al., 2002, p. 221)

To advance China's capabilities, research institutes are focusing on nontraditional warfare strategies. These Chinese institutions employ thousands of researchers investigating ways to exploit weak spots in technologically superior foes using computer attacks, electronic interference, and other information warfare techniques (Associated Press, 2002). This is notable considering that Chinese "hackivists" — that is, hackers who are also social activists — have attacked U.S. Internet sites in the past (Denning, 1999). In a related area, some are concerned about the potential for a dangerous information war across the Taiwan Strait (Bolt and Brenner, 2004).

Just as militaries are concerned with state-sponsored information warfare programs, commercial businesses should pay attention as well. With at least 30 countries suspected to be actively pursuing cyber-weaponry, business and government executives alike should assess their vulnerabilities from a concerted attack. This line of thinking extends Drucker's (2002) admonishment of executives to look outside their organizations for business opportunities and information. Likewise, executives should seriously look outside their organizations for cyber-threats as well. In this light, managers should pay special attention to security concerns when considering *outsourcing* or *offshoring* IT functions to organizations located in foreign nations (Pruitt, 2004).

Increased Economic Dependency on Information Infrastructures

Our society has evolved from an agrarian to an industrial to an information-based culture. References to the "digital economy" and "third wave" (Toffler, 1981) describe our growing dependence on IT. With rising anxiety about potential disruptions (Meall, 1989), the U.S. Government seriously addressed the deepening economic dependency on computers in the National Research Council's 1991 report, *Computers at Risk*. This report expressed government concern over a dependence on computers that "control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records" (National Research Council, 1991, p. 7). The United States later established the National Infrastructure Protection Center (NIPC) to help protect these critical infrastructures. In 2003, NIPC was merged into the U.S. Department of Homeland Security.

With an increasing reliance on IT, there is a growing need to protect it. In 1998, presidential decision directive (PDD) 63 designated federal agencies to initiate the development of protective measures for specified infrastructures. Table 2 shows the responsibilities of some key agencies. In cooperation with the private sector, each agency is developing an information sharing and analysis center to identify existing and emerging vulnerabilities. Private sector owners establish each ISAC to gather, analyze, and disseminate information about the threats and vulnerabilities faced by that sector. In 1999, the banking and finance sectors launched the first information sharing and analysis center. By 2003, more than a dozen centers had been established (Department of Homeland Security, 2005).

The 2003 *National Strategy to Secure Cyberspace* report set three strategic objectives:

1. Prevent cyber-attacks against critical infrastructures.
2. Reduce the U.S. vulnerability to cyber-attacks.
3. Minimize damage and recovery time from cyber-attacks that do occur.

> The report recognized that:
>
> By 2003, our economy and national security became fully dependent upon IT and the information infrastructure. A network of networks directly supports

Some response areas can benefit from government–industry cooperation to include the sharing of defensive strategies.

> the operation of all sectors of our economy—energy, transportation, finance and banking, information and telecommunications, public health, emergency services, water, medical, defense industrial base, food, agriculture, and postal and shipping. (Bush, 2003, p. 6)

Although this report promotes government–industry cooperation, it states that the private sector is better equipped to respond to the evolving cyber-threat. However, some response areas can benefit from government–industry cooperation to include the sharing of defensive strategies. For example, *defense in depth* has been a key element of the U.S. Nuclear Commission's safety philosophy. It employs a framework of successive and redundant measures to prevent accidents at nuclear facilities. This philosophy has served the nuclear power industry well (Garrick and Powers, 2000) and is being used as an effective architectural model for securing industry cyber-defenses (Shaurette, 2003).

Private Sector Is the Primary Target

Many high-profile cyber-attacks initially targeted the military. The 1986 Cuckoo's Egg incident had Clifford Stoll tracking German hackers who were scouring American military systems (Stoll, 1989). In 1994, hackers infiltrated Griffis Air Force Base computers to launch attacks at other military, civilian, and government organizations.

With the growing economic dependency on IT, civilian infrastructures are increasingly the primary targets of cyber-attacks. Headline-grabbing cyber-attacks such as SQL Slammer, MyDoom, MSBlast, and Sasser have targeted widely used commercial products and Web sites. Slammer penetrated an Ohio nuclear power plant's computer network and disabled a safety monitoring system for nearly five hours. This attack prompted a congressional call for U.S. regulators to establish cyber-security requirements for the 103 nuclear reactors operating in the United States (Poulsen, 2004).

Some scholars are concerned that an enemy of the United States will launch an information warfare attack against civilian and commercial firms and infrastructures (Strassmann, 2001). Seeking to avoid a direct military confrontation with U.S. forces, foreign attackers can shift their assaults to the private sector and infrastructure in a way that can make military retaliation very difficult. The private and public sectors now form the front line of 21st-century warfare, and private citizens and commercial infrastructures are likely to be the primary targets (Adams, 2001).

Cyber-Technology Is Increasingly Used in Perception Management

Perception management has been called a catchall phrase for the actions aimed at influencing public opinion, or even entire cultures (Callamari and Reveron, 2003; Jones et al., 2002). Examples of perception management cross the spectrum of corporate, political, civilian, and military realms and can include activities such as psychological operations, state-sponsored propaganda, or corporate marketing campaigns.

An emerging characteristic of modern perception management is the key role of technology in influencing public perception through new technologies that increase the speed of media reporting. The rise of global television and Internet technologies makes perception management a crucial dimension in many types of conflicts (Rattray, 2001). The Chinese government has made extensive use of perception management tools (Callamari and Reveron, 2003). The Somalis, Haitians, and Bosnian Serbs successfully used global television as a political instrument to reverse U.S. policy decisions (deCaro, 1998).

Perception wars target the courts of public opinion. For example, a Fortune 500 company will take notice when Web sites critical of the company appear highly ranked on popular search engine results.[5] Consider the electronic perception battles during the Iraq War. In 2003, anti-war activists used the Internet to organize and promote marches and rallies. Embedded wartime reporters traveling with military units provided favorable news coverage for the campaign. The Qatar-based news agency Al-Jazeera transmitted images of dead and wounded Iraqi civilians to the Arab world. Al-Jazeera then launched an English Web site in part to counter what some believed to be U.S. military censorship of the American-based media. At one point, the Al-Jazeera Web site itself was hacked and taken offline (Svensson, 2003). In 2004, images propagated on the Internet of prisoner abuse at Abu Ghraib influenced world opinion regarding American conduct. One report called the Internet dissemination of a video depicting terrorists beheading western hostages a new form of cyber-terrorism that comes right into the home (Smith, 2004). The use of technology

to manipulate public perceptions will assuredly persist.

In one case, Russian cyber-gangs targeted nine betting companies in a denial-of-service attack coinciding with a major sporting event.

Cyber-Technology Is Increasingly Used in Corporate Espionage

Although forms of espionage have been around for thousands of years, increased global competition, advances in IT, and the proliferation of tiny, embedded storage devices have added considerably to espionage dangers. For example, some security analysts note that the French government has engaged in significant high-technology espionage. They claim that French authorities have placed hidden copying devices in paper shredders conveniently available in French hotels frequented by foreign business travelers (Jones et al., 2002). In March 2001, former U.S. Defense Secretary William Cohen identified the former director of French intelligence as publicly admitting that French intelligence secretly collects and forwards to French companies information about their competitors in the United States and elsewhere. He gave several examples of French espionage against American companies. One incident involved the theft of proprietary technical data from a U.S. computer manufacturer by French intelligence, who then provided it to a French company (Cohen, 2001). Whereas the average cost to a company of a hacking attack or denial of service is roughly $150,000, according to the FBI, the average loss from a corporate espionage incident is much larger (Cohen, 2001).

Espionage can occur in e-mail communications between employees of business competitors. Market research firm NFO InDepth Interactive surveyed 498 employees in a variety of organizations. In a 2002 report, 40 percent of those surveyed admitted to receiving confidential information about other companies via the Internet, a 356 percent increase since 1999 (Rosenoer, 2002). In 2004, the U.S. Justice Department announced that Operation Web Snare identified a wide range of criminal activity on the Internet, including credit card fraud and corporate espionage. Investigators identified more than 150,000 victims, with losses in excess of $215 million (Hansell, 2004). As organizations open their internal networks and make more company information available to employees and vendors, the occurrence of corporate espionage will likely increase.

Cyber-Technology Is Increasingly Used by Organized Crime

The Internet explosion has introduced innovative forms of cyber-crime. In May 2003, the U.S. Justice Department announced Operation E-Con to help root out some leading forms of online economic crime (Federal News Service, 2003). The Justice Department claims that Internet fraud and other forms of online economic crime are among the fastest growing crimes. One type of crime involves Web site scams. For example, Australian scammers targeted Bank of America customers by implementing a look-alike Web site. Customers were sent scam e-mails that linked to a fake site that requested an account name and password. This *phishing* scam compromised nearly 75 customer accounts (Legard, 2003).

Other forms of global cyber-crime include extortion schemes from gangs often based in Eastern Europe and Russia (O'Rourke, 2004). In one case, Russian cyber-gangs targeted nine betting companies in a denial-of-service attack coinciding with a major sporting event. The Russian Interior Ministry, which fights cyber-crime, broke up the extortion ring after two of the victimized companies agreed to pay the gangs U.S. $40,000 each (*The Australian*, 2004). In another area, anti-virus researchers are reporting large increases in organized virus and worm development activity. This underground criminal activity is powering what some call an underground economy specializing in identity theft and spam (Verton, 2004). To help counter this problem, The Millennium Project, a futurist group associated with the United Nations University, has called for a "declaration of information warfare" against transnational organized crime to encourage businesses and nations to take organized cyber-crime more seriously (Ascribe, 2003).

Cyber-Technology Is Increasingly Used against Individuals and Small Businesses

The *National Strategy to Secure Cyberspace* defines the first level of cyberspace as the home user and small business. Although not part of the critical infrastructure, systems at this level are increasingly being subverted to attack vital systems (Bush, 2003, p. 38). As a result, private citizens and small organizations ought to be increasingly vigilant to cyber-warfare threats.

One growing threat is the use of spyware and adware. These monitoring programs can be legitimate computer applications that a user

One recent study stressed that small businesses face many of the same vulnerabilities of the larger corporations.

agrees to or can be from third parties with illegal intentions (Stafford and Urbaczewski, 2004). An estimated 7,000 spyware programs reportedly exist and, according to Microsoft, are responsible for half of all PC crashes (Sipior, Ward, and Roselli, 2005). One study indicates that 91 percent of home PCs are infected by spyware (Richmond, 2004).

Another growing problem is identity theft, which has been called a new form of cyber-terrorism against individuals (Sterling, 2004) and often takes the form of a Doppelgänger: the pervasive taking of a victim's identity for criminal purposes (Neumann, 1998). This crime affects individuals and businesses alike. The U.S. Federal Trade Commission reported that 9.9 million Americans in 2003 were victims (Gerard, Hillison, and Pacini, 2004). The majority of cases result from cyber-thieves using an individual's information to open new accounts, with the average loss at $1,200 (Sterling, 2004). Falsified accounts have cost businesses $32.9 billion and consumers $3.8 billion (DeMarrais, 2003).

In addition to vulnerabilities linked to identity theft, one recent study stressed that small businesses face many of the same vulnerabilities of the larger corporations. The leading perceived threats by small businesses include: internal threats (intentional and accidental), Trojans, hackers, viruses, password control, system vulnerabilities, spyware, and malware (Keller, Powell, Horstmann, Predmore, and Crawford, 2005). Likewise, many of the cyber-warfare threats discussed in this article should concern smaller organizations as well (e.g., organized crime, espionage).

Growing Demand for Cyber-Insurance

Considering societal reliance on IT, the growing cyber-threat is highlighting the need for risk mitigation strategies such as cyber-insurance. In 2002, at least two dozen insurance companies offered cyber-policies, including such firms as Chubb, Lloyd's of London, Zurich North America, and American International Group. Cyber-insurance policies often have higher premiums and deductibles because of the uncertainties in assessing cyber-risk (Kolodzinski, 2002). *USA Today* (Swartz, 2003) reported that the average cost for cyber-insurance ranges from $5,000 to $30,000 per year for $1 million in coverage.

After only three years in the market, network risk insurance or "hacker insurance" coverage reached about $100 million in 2002 and was expected to reach $2.5 billion by 2005, according to insurance industry projections (Keating, 2003). The United States' *National Strategy to Secure Cyberspace* report recommends insurance "as a means of transferring risk and providing for business continuity" (Bush, 2003, p. 24). The 2001 Code Red Worm incident cost its victims and insurance companies an estimated $2 billion in damage. The research organization Computer Economics estimates that damages caused by The Love Bug, Melissa, Code Red, and other incidents have exceeded $54 billion in downtime, removal expenses, and repairs (Geralds, 2003). A survey of 500 U.S. companies showed an increase in reported financial losses of 21 percent, or $455.8 million, in 2002. In addition, those losses are increasingly the result of organized, planned cyber-attacks (Richardson, 2003). According to Ernst and Young, security occurrences can cost companies between $17 and $28 million per incident (Garg, Curtis, and Halper, 2003). There are hundreds of millions of Internet-connected computers worldwide, nearly two billion Internet-enabled mobile devices, and one billion users of Internet messaging. These growing numbers suggest that companies will have a host of new security concerns (Gross, 2003). As cyber-related incidents continue, demand for insurance to cover losses related to electronic theft, vandalism, and extortion will likely increase.

Growing Demand for Information Security Professionals

For years, systems security was a backburner issue among IT executives (Straub and Welke, 1998). With the changing threat environment, however, security is moving to the forefront. A recent survey of IT executives placed security and privacy as the third top issue (Luftman and McLean, 2004). Skilled specialists are now in high demand by organizations wishing to protect their information resources. Certified professionals act as organizational leaders in security. They help senior management in the important roles of security education, awareness, risk assessment, and the promotion of a security-minded culture (Dutta and McCrohan, 2002). The dramatic growth in the number of CISSPs attests to this need. This certification program has grown from 2,000 certifications in 1999 to more than 35,000 in 2005 [International Information Systems Security Certification Consortium ([ISC]$^{2®}$), 2005]. Other certification bodies have experienced similar growth.

Security-trained employees should understand that cyber-threats come from not just the stereotypical hacker but business competitors, foreign institutions, and organized crime.

For example, the Information Systems Audit and Control Association (ISACA) got its start in 1967 and now claims more than 35,000 members in more than 100 countries (ISACA, 2005). Additionally, curricula in information security and assurance are appearing throughout academia. The 2005 [ISC]² Resource Guide lists numerous institutes of higher learning that now offer various types of information assurance and security management programs.

IMPLICATIONS AND RECOMMENDATIONS

This article demonstrates the rapid entry of information conflicts into civilian and commercial arenas by highlighting 12 trends of cyber-warfare. Implications for practitioners and researchers are suggested.

Practitioners: Develop and Maintain an Organizational Cyber-Security Strategy

For practitioners, strategies exist that can help organizations safeguard their critical information. Flowing from this article's thesis, two primary strategies are recommended to mitigate the cyber-warfare threat: an architectural strategy and a managerial strategy.

First, an *architectural strategy* should promote layers of security to increase the time and resources necessary for attackers to penetrate multiple barriers. This defense-in-depth approach is similar to an architectural fortress of high walls and armed guards behind a protective moat (Tucker, 2004). Although each barrier alone does not ensure sufficient protection, taken together, a layering of firewalls, with anti-virus software, combined with intrusion detection and prevention systems can greatly help to repel many of the types of attacks mentioned in this article (Frolick, 2003).

However, many security problems require managerial rather than technical solutions (Panko, 2004). The *managerial strategy* flowing from the thesis of this article includes four parts:

- Hiring certified security officers
- Training employees
- Assessing risk
- Managing policy

The first part of the managerial strategy is to hire certified security professionals as the commissioned officers of the cyber-war. Besides bringing knowledge of industry best practices and standards (notably ISO/IEC 17799), security officers must also be leaders with the authority to take required actions. With this authority, they can implement the second part of the strategy: the effective training and motivating of the cyber–foot soldier. Employee training has been a recognized task for effective computer security since the proliferation of the microcomputer (James, 1992). Given that every employee is part of the security team, an untrained employee is a high-risk asset (Mitnick, 2003). Security-trained employees should understand that cyber-threats come from not just the stereotypical hacker but business competitors, foreign institutions, and organized crime.

The third part of the managerial strategy is to mandate periodic risk assessments to identify the most serious cyber-threats. After identifying threats, managers can allocate resources necessary to mitigate the most serious risks (Austin and Darby, 2003). Industry guidelines such as the Australian-New Zealand Risk Management Standard 4360 can help ensure a strong program.

The fourth part of the strategy is to develop and enforce a solid security policy. Policies are the primary building blocks of every information security effort; they provide official statements of managerial direction and support (Wood, 1996). Yet, the best policies are wasted efforts if employees disregard them. Effective enforcement of enterprise security policies through monitoring and auditing can substantially reduce security risks (Straub and Welke, 1998).

Researchers: Conduct Further Studies in Cyber-Warfare

Based on the 12 trends identified from this literature review, a research agenda exists that explores information warfare's expansion into civilian and commercial environments. Future studies can explore particular trends in our framework or suggest additional trends to the ones provided. Our research call is consistent with that of Cronin and Crawford (1999), who recommended further study into the long-term social effects of pervasive computing and information war.

CONCLUSION

Historically, information security concerns have not had a high priority with most managers. Many seemed willing to risk major losses by permitting their information systems to be either lightly protected or wholly unprotected (Straub, 1990). Yet, the growing reliance on IT

A clearly written and enforced security policy will promote good discipline in the organization.

has increased exposure to diverse sources of cyber-war threats. Corporate leaders must be aware of the diversity of attacks, including high-tech espionage, organized crime, perception battles, and attacks from ordinary hackers or groups sponsored by nation-states or business competitors. Top management's awareness and commitment is required to address these security problems (Dutta and McCrohan, 2002). With the average cost of an incident ranging from $17 million to $28 million, large organizations can afford to support the implementation of a cyber-security strategy.

A clearly written and enforced security policy will promote good discipline in the organization. Together with hiring certified professionals, training employees, annually assessing risks, and implementing layered technology architectures, organizations can defend themselves against the expanding domain of cyber-warfare. The cyber-warfare framework presented in this article will promote a greater understanding of the growing cyber-threat facing corporations. ▲

Notes

1. A copy of the referenced top 25 issues report is available by contacting the first author.
2. The Software Engineering Institute at Carnegie Mellon University operates the Computer Emergency Response Team Coordination Center (CERT/CC). Given that attacks against Internet-connected systems have become so commonplace and for other stated reasons, as of 2004, the CERT no longer publishes incident numbers (see www.cert.org/stats/cert_stats.html).
3. The Computer Security Institute (CSI) annually conducts the Computer Crime and Security Survey with participation by the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad (see www.gocsi.com).
4. A list of 75 security tools is provided at http://www.insecure.org/tools.html. This list is derived in part from a hacker mailing list. Many of the listed tools are free hacker tools that have been around for years.
5. Try a Google search on Home Depot, Texaco, or Wal-Mart for a demonstration.

References

Adams, J. (2001). Virtual Defense. *Foreign Affairs, 80*(3), 98–112.

Alger, J. I. (1996). Introduction. In W. Schwartau (Ed.), *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Information Age* (2nd ed., pp. 8–14). New York: Thunder's Mouth Press.

Ascribe. (2003). Millennium Project Calls for Declaration of Global Information Warfare against Transnational Organized Crime; Corruption, Money Laundering, Terrorism Funding by Organized Crime Should Be Treated as National Security Threat. *Ascribe Newswire*, February 10.

Associated Press. (2002). China Boosts Information Warfare Development with Vast Research Centers. *Associated Press Worldstream*, September 27.

Austin, R. D., and Darby, C. A. R. (2003). The Myth of Secure Computing. *Harvard Business Review, 81*(6), 120–126.

The Australian. (2004). Officials Break up Russian Extortion Ring. *The Australian,* Aug 3, p. C03.

Bagchi, K., and Udo, G. (2003). An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the Association for Information Systems, 12*(46), 1–29.

Bolt, P. J., and Brenner, C. (2004). Information Warfare across the Taiwan Strait. *Journal of Contemporary China, 13*(38), 129.

Bush, G. W. (2003). *National Strategy to Secure Cyberspace [Rec.1-4(B)]*, February. Retrieved Aug. 10, 2005, from http://www.whitehouse.gov/pcipb

Callamari, P., and Reveron, D. (2003). China's Use of Perception Management. *International Journal of Intelligence and Counter Intelligence, 16*(1), 1–15.

Cohen, W. (2001). *Former Defense Secretary Cohen's Remarks at the 2001 Summit (March 6)*. George Mason University. Retrieved Aug. 10, 2005, from http://www.gmu.edu/departments/law/////techcenter/programs/summit/cohen's_2001_remarks.html

Computer Security Institute. (2002). *Cyber-Crime Bleeds U.S. Corporations, Survey Shows; Financial Losses from Attacks Climb for Third Year in a Row (Press Release, April 7, 2002)*. CSI, San Francisco. Retrieved April, 2003, from http://www.gocsi.com/press

Cronin, B. (2002a). Information Warfare. *Library Journal, 127*(12), p. 54.

Cronin, B. (2002b). Information Warfare: Peering inside Pandora's Postmodern Box. *Library Journal, 50*(6), 279–294.

Cronin, B., and Crawford, H. (1999). Information Warfare: Its Applications in Military and Civilian Contexts. *Information Society, 15*(4), 257–264.

Dearth, D. H. (1998). Imperatives of Information Operations and Information Warfare. In A. D. Campen and D. H. Dearth (Eds.), *Cyberwar 2.0: Myths, Mysteries, and Reality*. Fairfax, VA: AFCEA International Press.

deCaro, C. (1998). Operationalizing Software. In A. D. Campen and D. H. Dearth (Eds.), *Cyberware 2.0: Myths, Mysteries, and Reality*. Fairfax, VA: AFCEA International Press.

DeMarrais, K. (2003). Identity Theft on the Rise, FTC Warns. *Knight Ridder Business News,* September 4, pp. 1–4.

Denning, D. E. (1999). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.* Nautilus Institute. Retrieved Aug. 10, 2005, from www.iwar.org.uk/cyberterror/resources/denning.htm

Department of Homeland Security. (2005). *Information Sharing and Analysis Centers*. Retrieved Aug 10, 2005, from www.dhs.gov/dhspublic/display?theme=73&content=1375; original content from www.caio.gov, May 2003.

Drucker, P. F. (2002). *Managing in the Next Society (Audiobook)*. Los Angeles: St. Martin's Press/Truman Talley Books.

Dutta, A., and McCrohan, K. (2002). Management's Role in Information Security in a Cyber-Economy. *California Management Review, 45*(1), 67–87.

Federal News Service. (2003). Press Conference with Attorney General John Ashcroft; FBI Director Robert Mueller; and FTC Chairman Timothy J. Muris. *Federal News Service Inc.*, May 16.

Friman, H. (2001). A Systems View of Information Warfare. *Journal of Information Warfare, 1*(1), 25–32.

Frolick, M. N. (2003). A New Webmaster's Guide to Firewalls and Security. *Information Systems Management, 20*(1, Winter), 29–34.

Garg, A., Curtis, J., and Halper, H. (2003). The Financial Impact of IT Security Breaches: What Do Investors Think? *Information Systems Security, 12*(1), 22–34.

Garrick, J. B., and Powers, D. A. (2000). *Use of Defense in Depth in Risk-Information Nmss Activities (Letter to Richard A. Meserve Dated May 25, 2000, Chairman, U.S. Nuclear Regulatory Commission)*. Retrieved Aug. 10, 2005, from http://www.nrc.gov/reading-rm/doc-collections/acrs/letters/2000/4721893.html

Geralds, J. (2003). *Hacker Insurance Set to Rocket*, February 14. Retrieved Aug. 10, 2005, from http://www.vnunet.com/news/1138789

Gerard, G., Hillison, W., and Pacini, C. (2004). What Your Firm Should Know About Identity Theft. *The Journal of Corporate Accounting and Finance, May/June*, 3–11.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2005). *Tenth Annual, 2005 CSI/FBI Computer Crime and Security Survey.* San Francisco, CA (www.gocsi.com): Computer Security Institute.

Gross, G. (2003). Net Attacks Down but Sophistication Is Up. *IDG News Service*, January 30.

Hansell, S. (2004). U.S. Tally in Online-Crime Sweep: 150 Charged. *New York Times*, August 26.

Hutchinson, W. (2002). Concepts in Information Warfare. *Logistics Information Management, 15*(5/6), 410–413.

Information Systems Audit and Control Association (ISACA). (2005). *Overview and History.* Retrieved Aug. 10, 2005, from http://www.isaca.org/template.cfm?section=Overview_and_History

International Information Systems Security Certification Consortium [ISC]²®. (2005). *Press Releases*, Oct. 31. Retrieved Aug. 10, 2005, from https://www.isc2.org/cgi/content.cgi?page=13

ISO/IEC. (2000). *Information Technology — Code of Practice for Information Security Management* (No. ISO/IEC 17799:2000(E)): The International Standards Organization/The International Electrotechnical Commission.

James, P. N. (1992). Education and Training. *Information Systems Management, 9*(2), 15–21.

Jones, A., Kovacich, G. L., and Luzwick, P. G. (2002). *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. New York: Auerbach Publications.

Keating, G. (2003). Hacker Insurance Market Boosted by Cyberattacks. *Reuters*, January 27.

Keller, S., Powell, A., Horstmann, B., Predmore, C., and Crawford, M. (2005). Information Security Threats and Practices in Small Businesses. *Information Systems Management, 22*(2), 7–19.

Key, V. (2004). *What Is Solar Sunrise?* SANS. Retrieved Aug. 10, 2005, from http://www.sans.org/resources/idfaq/solar_sunrise.php

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Morrow, D. W. (2004). *Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)² Survey Results*. Alabama: Auburn University.

Kolodzinski, O. (2002). Cyber-Insurance Issues: Managing Risk by Tying Network Security to Business Goals. *CPA Journal., 72*(11), 10–11.

Legard, D. (2003). *Fake Bank Web Site Scam Reaches U.S.*, May 14. Retrieved Aug. 10, 2005, from http://www.itworld.com/Tech/2987/030514fakebank.

Libicki, M. C. (1995). *What Is Information Warfare?* Washington, DC: National Defense University, Institute for National Strategic Studies.

Luftman, J., and McLean, E. R. (2004). Key Issues for IT Executives. *MIS Quarterly Executive, 3*(2), 89-104.

Meall, L. (1989). Survival of the Fittest. *Accountancy (UK), 103*(1147), 140–141.

Mitnick, K. (2003). Are You the Weak Link? *Harvard Business Review, 81*(4), 18–20.

National Research Council. (1991). *Computers at Risk*. Washington D.C.: National Academy Press.

Neumann, P. G. (1998). Identity-Related Misuse. In D. E. Denning and P. J. Denning (Eds.), *Internet Besieged*. Reading, Massachusetts: ACM Press.

O'Rourke, M. (2004). Cyber-Extortion Evolves. *Risk Management, 51*(4), 10-12.

Panko, R. (2004). *Corporate Computer and Network Security.* New Jersey: Prentice Hall.

Parker, D. B. (1976). *Crime by Computer.* New York: Scribners.

PCWorld. (2001). *Timeline: A 40-Year History of Hacking*. IDG News Service, November 19. Retrieved Aug. 10, 2005, from http://www.cnn.com/2001/TECH/internet/11/19/hack.history.idg/

Porter, T. (1996). Information Warfare — Your Company Needs You! *Computers & Security, 15*, 561–566.

Poulsen, K. (2004). *U.N. Warns of Nuclear Cyber-Attack Risk*. SecurityFocus, Sept. 27. Retrieved Aug. 10, 2005, from http://www.securityfocus.com/news/9592

Pruitt, S. (2004). *When Outsourcing, Don't Forget Security, Experts Say. IDG News Service*, Sept. 21. Retrieved Aug. 10, 2005, from http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,96074,00.html

Rattray, G. J. (2001). *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press.

Rhem, K.T. (2005). *China Investing in Information Warfare Technology, Doctrine*. American Forces Press Service, July 20. Retrieved Aug. 10, 2005, from http://www.pentagon.gov/news/jul2005/20050720_2171.html

Richardson, R. (2003). *Eight Annual, 2003 CSI/FBI Computer Crime and Security Survey.* San Francisco, CA: Computer Security Institute (www.gocsi.com).

Richmond, R. (2004, 22 Jan). Netware Associates to Attack Spyware with New Products. *Wall Street Journal,* p. B5.

Rosenoer, J. (2002). Safeguarding Your Critical Business Information. *Harvard Business Review, 80*(2), 20–21.

Schwartau, W. (1998). Something Other Than War. In A. D. Campen and D. H. Dearth (Eds.), *Cyberwar 2.0: Myths, Mysteries, and Reality.* Fairfax, VA: AFCEA International Press.

Sequeira, D. (2003). Intrusion Protection Systems: Security's Silver Bullet? *Business Communication Review, March*, 36–41.

Shaurette, K. (2003). Security Infrastructure: Basics of Intrusion Detection Systems. In H. F. Tipton and M. Krause (Eds.), *Information Security Management Handbook* (4th ed., Vol. 4, pp. 683–698). New York: Auerbach Publications.

Sipior, J. C., Ward, B. T., and Roselli, G. R. (2005). The Ethical and Legal Concerns of Spyware. *Information Systems Management, 22*(2), 39–49.

Smith, L. (2004, June 30). Web Amplifies Message of Primitive Executions. *Los Angles Times*.

Stafford, T. F., and Urbaczewski, A. (2004). Spyware: The Ghost in the Machine. *Communications of the Association for Information Systems, 14*, 291–306.

Sterling, B. (2004). The Other War on Terror. *Wired,* 12(8), August. Retrieved Aug 10, 2005, from http://www.wired.com/wired/archive/12.08/view.html?pg=4

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. New York: Doubleday.

Strassmann, P. A. (2001). *Government Should Blaze Global Information Warfare Trails*. Retrieved Aug. 10, 2005, from http://www.strassmann.com/pubs/searchsecurity/2001-8.php.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255–276.

Straub, D. W., and Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441–469.

Sunday Times. (1996). Secret DTI Inquiry into Cyber-Terror. *The (London) Sunday Times*, June 9, pp. 1–8.

Svensson, P. (2003). Al-Jazeera Site Experiences Hack Attack. *The Associated Press*, March 25.

Swartz, J. (2003). Firms' hacking-related insurance costs soar. *USA Today,* Feb. 9. Retrieved Aug. 29, 2005, from http://www.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm

Toffler, A. (1981). *The Third Wave*. New York: Bantam Books.

Tucker, T. E. (2004). Leveraging Protection Mechanisms to Provide Defense in Depth. In M. E. Whitman and H. J. Mattord (Eds.), *Management of Information Security.* Boston: Course Technology, p. 408.

Verton, D. (2004). Organized Crime Invades Cyberspace. *ComputerWorld*, August 30. Retrieved Aug. 10, 2005, from http://www.computerworld.com/securitytopics/security/story/0,10801,95501,00.html

Wilson, J. (2001). E-Bomb. *Popular Mechanics, 178*(9), 50–54.

Wood, C. C. (1996). *Information Security Policies Made Easy* (5th ed.): Baseline Software.

Zviran, M., and Haga, W. J. (1999). Password Security: An Empirical Study. *Journal of Management Information Systems, 15*(4), 161–185.