Introduction to Cyber Warfare and Cyber Terrorism

Andrew M. Colarik, AndrewColarik.com, USA
Lech J. Janczewski, University of Auckland, New Zealand

ORIGINS AND DEFINITIONS OF CYBER WARFARE AND CYBER TERRORISM

The number of publicized terrorist attacks started to escalate beginning in the mid-1990s. From the attacks that received wide coverage by the world press, we have arrived to the point where not a single day passes without a terrorist committing such acts. It is the spectacular that is getting first-page coverage by the mass media. The basic mechanics of these attacks is usually through the use of explosives detonated remotely or by a suicidal person intent on taking others with them into the next life.

An obvious question must be asked: Is it easy or difficult to plan and execute such attacks? In 2006, Bruce Schneier set up an unusual competition. The goal of this competition was to write a scenario for a terrorist attack against a major component of the United States' critical infrastructure. After an analysis of the possible plots that were submitted, he came to the conclusion that it is not as easy a task as many might think. The fact is that no major terrorists' attacks have happened on U.S. soil since 9/11, despite the fact that there are myriads of groups around the world with this one major objective. Their failure to inflict another attack may be related to the extensive security measures introduced after the 9/11 events.

As a result, a follow-up question may be formulated: Could the consequential damages (i.e., political, economic, and cultural) of 9/11 be created using information technology? Several studies indicate that in the early 1990s, the American society was not well prepared against electronic attacks. As a result, major information system users such as government agencies, military installations, major banks, and so forth began to prepare for the handing of such electronic attacks.

The word "terrorism" brings to mind a picture of bearded men throwing a pouch filled with explosives. But in the context of IT security, terrorists can come in many forms such as politically motivated, anti-government, anti-world trade, and pro-environmental extremists. If given the opportunity, such activists would gladly disrupt trade and legislative agendas by attacking a facility's communication server, especially if the media were standing by to report what just happened. Also, a terrorist could try to interfere with IT resources controlling critical national infrastructures (like water supply, power grid, air traffic, etc.) through the manipulation of SCADA systems. As a matter of fact, such attacks have already been carried out. In 2000, someone hacked into Maroochy Shire, Australia's waste management control system and released millions of gallons of raw sewage into the town. Given the political orientation, cyber warfare and cyber terrorism are realities that our civilization are now facing.

The term cyber terrorism was coined in 1996 by combining the terms cyberspace and terrorism. The term has become widely accepted after being embraced by the United States Armed Forces. A report generated in 1998 by the Center for Strategic and International Studies was entitled Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo. In this report, the probabilities of such activities affecting a nation were discussed, followed by a discussion of the potential outcomes of such attacks and methods to limit the likelihood of such events. We will use the term cyber terrorism as:

Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets.

Parallel to the term of cyber terrorism is an older term known as information warfare:

Information warfare is defined as a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses.

The practical difference between these two terms is that cyber terrorism is about causing fear and harm to anyone in the vicinity (i.e., bystanders), while information warfare has a defined target in a war (ideological or declared). Along with these terms there is a phenomenon of *cyber crime* used frequently by law enforcement agencies. Cyber crime is a crime committed through the use of information technology. We must point out that the physical forms of cyber terrorism, information warfare, and cyber crime often look very much alike.

Imagine that an individual gains access to a hospital's medical database and changes the medication of a pro-business, anti-environmental executive of a Fortune 100 company to one that he or she is dangerously allergic to and also removes the allergy from his or her digital record. The nurse administers the drug and the patient dies. So, which definition applies? The answer lies not in the mechanics of the event, but rather in the intent that drove the person's actions. If it was intentionally done, for instance as a result of poor relations between these two people, then it would be murder in addition to a cyber crime. If the executor later would announce that he or she is ready to commit more such acts if their demands would not be met, then it could be labeled as cyber terrorism. If the activities were carried out by an agent of a foreign power, then it could be labeled as information warfare. We believe the most important aspect of cyber attacks that have physical consequences is determining the intention of the attacker.

The distinction between these terms is extremely important because there are non-technology-related issues and solutions that will impact any strategy in combating cyber warfare and cyber terrorism. We would like to make it clear to our readers though that this book in no way attempts to cover the issue of what philosophical, political, or religious reasons would lead people to become cyber terrorists or cyber warriors. What we are putting forward is that societal and cultural orientations and their resulting motivations are important towards resolving the people component of such attacks. They cannot be ignored or disregarded just because we are exploring technological and organizational solutions.

CORRELATIONS BETWEEN CYBER AND CORPOREAL CONFLICTS

There are several important correlations between cyber attacks and current national and international corporeal situations. Any IT manager should be aware of the following existing consistencies:

- Physical attacks are usually followed by cyber attacks: Immediately after the downing of an American plane near the coast of China, individuals from both countries began cyber attacks against facilities of the other side. Similarly, an increased wave of cyber attacks was observed during the Pakistan/India conflict, throughout the Israeli/Palestinian conflict, and the Balkans War (i.e., the collapse of Yugoslavia).
- Cyber attacks are aimed at targets representing high publicity value: Cyber attacks are carried out in such way that they could either inflict serious losses and/or generate high publicity. All installations attached to top administrative and military units are primary targets. Apart from government organizations, cyber attacks are launched against the most visible and dominant multi-national corporations. Favorite targets by attackers are top IT and transportation industry companies such as Microsoft, Boeing, and Ford.
- Increases in cyber attacks have clear political/terrorist foundations: Available statistics indicate that any of the previously mentioned conflicts resulted in a steady increase of cyber attacks. For instance, attacks by Chinese hackers and the Israeli/Palestinian conflict show a pattern of phased escalation.

Because no one person can prevent world events, unless you have connections most mortals do not, you need to know why and how cyber warriors and terrorist strike. The follow section offers some context.

WHY AND HOW CYBER WARRIORS AND CYBER TERRORISTS STRIKE?

When building protections against cyber attacks, we must understand why they launch their attacks and what they are counting on. Understanding is the first step in reducing or eliminating attacks. The most probable reasons for cyber attacks are:

- **Fear factor:** The most common denominator of the majority of terrorist attacks is a terrorist wishes the creation of fear in individuals, groups, or societies. Perhaps the best example of this drive was the bombing of a Bali nightclub in 2002. This nightclub was nothing other than a watering hole for foreign tourists (Australians in particular), and inflicting casualties and fear among them was the main objective of the attackers. The influx of foreign tourists to Bali was significantly reduced after this attack. The same applies to attacks against IT installations.
- **Spectacular factor:** Whatever is the actual damage of an attack, it should have a spectacular nature. By spectacular we consider attacks aimed at either creating huge direct losses and/or resulting in a lot of negative publicity. In 1999, the Amazon.com Web site was closed for some time due to a denial of service (DOS) attack. Amazon incurred losses due to suspended trading, but the publicity the attack created was widespread.
- **Vulnerability factor:** Cyber activities do not always end up with huge financial losses. Some of the most effective ways to demonstrate an organization's vulnerability is to cause a denial of service to the commercial server or something as simple as the defacement of an organization's Web pages, very often referred to as computer graffiti.

Cyber attacks may be carried out through a host of technologies, but have an attack pattern that may be modeled. Despite using the most advanced technology, the phases of a cyber attack generally follow the same pattern as a traditional crime. These are as follows:

The first phase of an attack is reconnaissance of the intended victim. By observing the normal operations of a target, useful information can be ascertained and accumulated such as hardware and software used, regular and periodic communications, and the formatting of said correspondences.

The second phase of an attack is penetration. Until an attacker is inside a system, there is little that can be done to the target except to disrupt the availability or access to a given service provided by the target.

The third phase is identifying and expanding the internal capabilities by viewing resources and increasing access rights to more restricted, higher-value areas of a given system.

The forth stage is where the intruder does the damage to a system or confiscates selected data and/or information.

The last phase can include the removal of any evidence of a penetration, theft, and so forth by covering the intruder's electronic trail by editing or deleting log files.

Ultimately, an intruder wants to complete all five stages successfully. However, this is entirely dependent on the type of attack method utilized, the desired end result, and the target's individual defensive and/or monitoring capabilities.

According to the CSI/FBI 2006 Computer Crime and Security Survey, virus attacks continue to be the source of the greatest financial losses. Unauthorized access continues to be the second-greatest source of financial loss. Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74% of financial losses. These types of attacks occurred despite the fact that most of the respondents had security policies and mechanisms in place as part of their prevention and response plans. Just imagine the number of successful attacks that went unnoticed and/or unreported, and by entities that were not even part of the survey.

In general, today's cyber attacks consist primarily of:

- Virus and worm attacks that are delivered via e-mail attachments, Web browser scripts, and vulnerability exploit engines.

- Denial of service attacks designed to prevent the use of public systems by legitimate users by overloading the normal mechanisms inherent in establishing and maintaining computer-to-computer connections.
- Web defacements of informational sites that service governmental and commercial interests in order to spread disinformation, propaganda, and/or disrupt information flows.
- Unauthorized intrusions into systems that lead to the theft of confidential and/or proprietary information, the modification and/or corruption of data, and the inappropriate usage of a system for launching attacks on other systems.

The goals of these attacks can vary. Some are to show the weaknesses inherent in the systems. Some are political statements about the conduct of the entities being attacked, while others are about the theft of information for a variety of reasons. These can include target intelligence, internal process observations, or wholesale theft. As previously stated, the perpetrator's reasons (i.e., why he or she decided to penetrate a system) have a lot to do with the extent of the damages that may be incurred. The perpetrator may wish to have a look around in an attempt to "case" the system, or may simply be looking for high-value data items (i.e., something that satisfies his or her penetration goal) that can be used for other internal and/or external operations. Some intrusions may be to do some damage to a system in that an underlying system or sub-process would be disrupted or modified as the end result of the intrusion or as a step in a series of penetration activities. Intruders may also seek to change important data in an attempt to either cover their tracks (i.e., such as delete/modify an audit log) or to cause people or other processes to act on the changed data in a way that causes a cascading series of damages in the physical or electronic world.

The means (i.e., course, process, etc.) of an attack has a lot to do with the approach taken to execute the attack and its related characteristics. If someone wants to damage a system with a virus, then he or she needs to consider how the virus will be delivered and what capabilities said virus is to be empowered with in order to create the damage done (i.e., delete data, monitor activities, steal intellectual property or identities, etc.). The design of an attack requires an appropriate delivery method and an appropriate device to perform the damage once it is delivered. Because an attacker does not control the basic choice of systems and protective mechanisms of any given network, he or she is left to choose from a variety of approaches that have both advantages and disadvantages for any given attack. At the highest level of these choices is whether to penetrate a system internally or externally.

It is a common fact that insiders can gain greater access to system resources than outsiders in most configured systems and networks. This is because certain service levels within a network rely on users and developers to be attentive to procedures, methods, and policies for the organization's overall benefit. Restrictions on users tend to reduce the overall capability of a given system. Thus, reliance on users to conduct themselves appropriately may lead to vulnerabilities, damaged systems and data, and future attacks. When it comes to access control, system programmers and developers ultimately tend to have the highest level of internal access of systems because it is they who create the hidden structures that provide services to users.

Periodically, operating systems and application programs have overlooked weaknesses built into their software. This is not uncommon, as pressure to reduce the time-to-market development cycle has created many dysfunctions in the computer software industry. The current paradigm of software development is to get the product to the customer as fast as possible with as few defects as feasible, and then to correct the software as defects surface. Would-be attackers may then exploit such weaknesses before they have been fixed. At first glance, this approach would be considered an external attack, except when the vulnerability has been deliberately created by those in the development process. Recently, it was discovered that Aum Shinrikyo cult members, the same cult that killed 12 people and injured 6,000 after releasing sarin gas in the Tokyo subways, had worked as subcontractors for firms developing classified government and police communication hardware and software. As a result, the cult was able to procure and further develop software that allowed them to track police vehicles. In addition, there may yet be undiscovered capabilities that were created as a result of their development contributions to more than 80 Japanese firms and 10 government agencies.

The above example shows that internal systems have an inherent weakness where users must rely on the quality control levels of the supplying company for their foundational security. In today's environment, people are forced to trust the secure operation of fabricated and pre-packaged hardware and software systems. An attack may or may not originate from inside a given network or system, but the execution of the attack is facilitated by the

internal systems such as in the case of an e-mail virus that does some damage but also propagates itself internally and/or to externally connected systems and recipients. The following section presents the facilities that could be the primary target of the attackers.

PRIMARY TARGET FACILITIES

Usage Portals

Usage portals are application programs that comprise the bulk of a user's daily computer usage where he or she interacts with the outside world. These include applications such as e-mail, Web browsers, chat clients, video streaming, remote software, Web-enabled application software, and a host of other applications. These and other usage portals are utilized by attackers to turn a system against itself or hijack its applications to attack its host system or other connecting systems.

E-Mail

It is said that the most ubiquitous application in use for communication today is electronic mail (e-mail). We use e-mail to write letters and send attached files such as pictures and spreadsheets, and depending on the e-mail client's configuration, it can even receive Web page content inside a received e-mail. This particular usage portal reputably caused between US$3-15 billion in damages worldwide when a university student in the Philippines developed and released the Love Bug virus. Now this is no small matter when it is considered that Hurricane Andrew caused US$25 billion in damage when it went through the state of Florida. Essentially, this small e-mail virus was programmed to infect the computer of whoever opened the message and send itself to everyone in the user's address book. The deliverable was a virus, the portal was the e-mail client, the choice of target was anyone associated with an initial victim, and the damage was to distribute itself and then damage the host computer system.

This is but one application of what a virus can do with this portal. Such viruses now are being used to inundate targeted installations (i.e. military, government, corporate, etc.) with tens of thousands of e-mails that are intended to flood the organization's e-mail server with more messages than it can handle while attempting to spread itself to connecting systems (i.e., a cascading damage effect). Because care is not always taken in the proper use of e-mail clients, e-mail servers do not always have properly configured filtering systems, and users are not always selective in what they open and read, e-mail will continue to be a choice portal for conducting attacks.

Web Browsers

Web browsing has allowed the Internet to prosper and flourish by providing a point-and-click approach to informational Web sites about everything from basket weaving to building roadside bombs. With more than 8 trillion Web pages, the statistical probability that some of them are designed to disrupt, hijack, or damage a connecting computer cannot be ignored. Built into a Web browser are the tools and scripts (i.e., small executable programs that execute requested resources such as Install on Demand, Java Script, VB Script, etc.) that can be turned against a user's computer. The same tools that allow a browser to execute the playing of a video at a news site can be used to trigger remote executions of other programs and sub-routines that can allow a Web site's host server to take control of parts of the visitor's system. These tools can then be used to read and execute files on the visitor's system in order to access information such as user account details (i.e., full user name, logon name, e-mail addresses, permission levels, last time a password was changed, IP address, etc.), gather previously accessed sites and files stored in the operating system and application program working folders, determine configuration settings such as version levels and the settings of the operating system and/or application programs, as well as many more details that are stored on a user's computer.

In addition, by using executable code that are stored inside a digital picture, malicious sites can make use of these built-in tools and execute malicious code when a picture is opened and/or viewed. Browsers also have appli-

cation program interfaces and plug-ins to security protocols such as Secure Socket Layer and mechanisms such as digital certificates that enable more secure browsing and communications. When vulnerabilities are discovered in browser applications, caustic Web site servers can be geared to take advantage of these resulting in site redirections, server authenticity spoofing (i.e., deliberate identity falsification), and the installation and execution of malicious code. The above issues and others not mentioned regarding Web browsers can be reduced or eliminated if a Web browser is properly configured and regularly updated, and therefore must be taken seriously. Unfortunately, the inherent design orientation of most Web browsers is geared towards an "open systems approach" for complete compatibility and interconnectivity with available Web services. This fundamental weakness makes this portal ripe for exploitation.

Chat Clients

Computer-user-to-computer-user communications is sometimes facilitated with the use of Internet relay chat (IRC) software such as MSN Messenger, AOL Instant Messenger, mIRC, and a host of others. Some chat clients allow a direct, dedicated connection between two computers, while others utilize a centralized server to log into and chat with others on the server both in individual chat sessions and in the groups forums. An extension of this basic approach is with the inclusion of voice and/or video feed via a microphone and/or video camera. This combined approach combines text messaging, Voice Over Internet Protocol, and video streaming using software such as Apple's iChat AV. The vast majority of the products in this usage portal have no privacy protection (i.e., encryption, IP address obscuring, etc.) and are subject to monitoring, hijacking, and substitution of communication content attacks in addition to any relevant information that can be ascertained from a given conversation.

Also, an intruder can use this class of software to obtain configuration information to remotely use a computer's microphone and video camera at a later date to see/listen in on the room in which the computer resides. Care must be taken in the choice of software, chat server, and those who are to be chatted with when using this portal. However, the basic nature of people to become comfortable with systems and trust previous relationships will lead to this portal being taken advantage of by technical savvy intruders and social engineers.

Remote Software

Remote software allows a user to take control of an existing computer or server remotely through another computer. This is usually accomplished via a modem or network connection. This usage portal is used to remotely manage servers (i.e., similar to telnet) and access limited or shared resources on a network such as databases, application software, work files, and the like. Sometimes, the remote connection is completed in such a way that the user's computer acts as a terminal for keystrokes and screen shots that are being performed on the remote computer using software such as Laplink or pcAnywhere, or the computer being remote is actually a virtually, fully functioned, created desktop that emulates the look and feel of an actual desktop as in the case of Microsoft's Terminal Services. When remote services are enabled and made available, intruders can use the modems and/or network address ports to gain access to the internal structure of a network. These access points tend to be user name and password protected only with little or no privacy protection (i.e., encryption), and therefore can be subject to external monitoring, and brute force (i.e., incremental generation of characters until a match is found) and dictionary password attacks (i.e., a dictionary list of potential passwords). Presumably, this portal is by far the least protected and one of the easiest to penetrate when present in an organization.

Web-Enabled Applications

Everyday applications such as word processors and spreadsheets are designed to be Web enabled to allow the sending and reading of files and work-in-process projects between systems (i.e., integrated applications and collaboration systems). It is quite common to attempt to insert clip art into a document and be prompted if you would like to browse additional clip art at the manufacturer's Web site. Other applications are integrated directly with e-mail and Web browser software as a result of being part of the same software suite such as Microsoft Office so

that these associated applications are launched and executed when specialty functions are requested. Additionally, many applications and utility software periodically check to see if an Internet connection is available and if so may contact the manufacturer's server for update information and/or registration validation. Some software is still more intrusive in that when a connection is not present, it instructs the computer to dial or connect to the Internet without permission from the user.

Web-enabled applications can be used by an intruder's malicious code to transfer information about a system (i.e., via File Transfer Protocol, etc.), execute successive activities of an initial attack (i.e., transitive capabilities), and facilitate the spread of additional malicious code. Care must be taken in the selection and configuration of these types of software, as well as the source manufacturer. The use of shareware and freeware sources for Web-enabled software can sometimes have additional built-in communications and backdoors that can be exploited by its creators and/or are the result of a poor software development process. It is one thing to have software with the ability to access the Web outside of its hosting system; it is another completely different issue when such software is designed to accept connections from the Internet without notifying the user, such as in the case of many of Microsoft's Office products. Because users have been given the ability to integrate applications with the Web (willingly or not), the problems associated with this approach will be around for some time to come.

Updates

As previously discussed, the current software development paradigm is to get a product to market as quickly as feasible. When security faults become known as a result of this paradigm, patches (i.e., software fixes) are usually issued by the manufacturer. Whether the patch is for an operating system, utility program, or application package, a process is required for developing a new patch, notifying users of the patch's existence, making the patch available in a timely manner, and finally delivering said patch. Throughout this process, vulnerabilities can be created and/or bypassed by users and intruders alike. As an example, most antivirus software has provisions for updating the virus definition files to protect against new viruses as they are developed and deployed. Some attacks are directed at the virus software itself in that if the virus scanner can be disabled in some way, then a greater threat can be activated without the user being made aware of it. Therefore, updating the definition files and antivirus software is critical to maintaining a good virus defense. When the update process is circumvented (i.e., not renewing the subscription, disabling part of the update process, corrupting the software or definition files, etc.), a host of security issues emerge usually resulting in a breached system.

With regards to operating systems and enterprise level software such as SAP, the update process has additional complexities that provide additional opportunities for intruders. One method of corruption that continues to be utilized is to send a system administrator an official-looking e-mail detailing an actual new security vulnerability that provides a link to download the appropriate patch. This patch may actually be a piece of malicious code such as a worm, the actual patch with the addition of an attached malicious program (i.e., virus), or a combination of the two. Care must be taken not only to install patches in a timely fashion, but also to secure the entire process. Since system administrators tend to be very busy, they may not take the time to check the authenticity of the e-mail or the integrity of the patch itself before installing it. Even when an administrator is knowledgeable enough not to fall for this ploy, he or she may delay in getting the new patch, and as a result, not install a needed security patch quickly enough. The Code Red I and II worms and others like them have disabled as many as 25% of Internet servers in one attack because of poor patch management.

DELIVERABLES

Using the mechanisms described above, attackers try to infect the attacked systems with malicious code which will be used next to carry out their malicious intentions. These deliverables have enormous implications for the results of an attack. The deliverable may seek to gain information on the intended target system. It may create a backdoor into the penetrated system that can be exploited at a later date for a variety of purposes. The deliverable may also be used to force a system to execute malicious code or instructions to modify or delete data and other programs. For internal penetrations (i.e., internal usage with outbound capabilities), the vast majority of deliverables will be

viruses, worms, and executable scripts (i.e., program instructions). Other attack deliverables having more external nature will be discussed later in the chapter.

Viruses and Worms

Viruses have been plaguing systems since the 1960s. Essentially, a computer virus is a self-replicating program that attaches itself to another program or file in order to reproduce. When a given file is used, the virus will reside in the memory of a computer system, attach itself to other files accessed or opened, and execute its code. Viruses traditionally have targeted boot sectors (i.e., the startup portion of a computer disk) and executable files, and have hidden themselves in some very unlikely memory locations such as in the printer memory port. Like computers, viruses have evolved in capabilities. These include the ability to conceal an infection by letting an executable program call the infected file from another location or by disabling the definition file (i.e., digital fingerprint used to detect a virus), by encrypting itself to prevent a discernable virus "signature," and/or by changing its digital footprint each time it reproduces (i.e., polymorphism).

Worms are a type of malicious software that does not need another file or program to replicate itself, and as such, is a self-sustaining and running program. The primary difference between viruses and worms is that a virus replicates on a host system while a worm replicates over a network using standard protocols (i.e., a type of mobile code). The latest incarnation of worms make use of known vulnerabilities in systems to penetrate, execute their code, and replicate to other systems such as the Code Red II worm that infected more than 259,000 systems in less than 14 hours. Another use of worms that are less destructive and more subversive has been designed to monitor and collect server and traffic activities, and transmit this information back to its creator for intelligence and/or industrial espionage.

Trojans

A Trojan horse is a malicious program that is intended to perform a legitimate function when it in fact also performs an unknown and/or unwanted activity. Many viruses and worms are delivered via a Trojan horse program to infect systems, install monitoring software such as keyboard loggers (i.e., a program that records every keystroke performed by a user) or backdoors to remotely take control of the system, and/or conduct destructive activities on the infiltrated system. It is very common for intruders to make available free software (i.e., games, utilities, hacking tools, etc.) that are in fact Trojan horses. In the commercial realm, it is also not unheard of to attach monitoring software (i.e., spyware) to a 30-day trial versions of "free" software that reports the activities of the user back to the manufacturer with the consent of the user when they agree to the terms and conditions when the software is first installed. The notification of the so-called intended monitoring is buried deep within such agreements. This spyware can also be monitored and hijacked by intruders to gather additional intelligence about a potential target, and in our opinion should be considered a Trojan horse regardless of the licensure agreement.

Malicious Scripts

Throughout the course of using the previously mentioned portals, a user will encounter the usage of scripting languages and macros that automate various calls and functions with connecting software modules and components. These scripts are designed to run in the background, and provide a means to communicate and execute legitimate code seamlessly between connecting/communicating modules and systems. These include Java Applets, Active X, and application software macros. Java Applets are programs designed to be executed within an application program such as a Web browser and do not get executed by the user's operating system directly. This allows applets to be operating system independent and instead rely on the application program to execute the commands through its resident operating system. Active X is a combination of Object Linking and Embedding (OLE) and Component Object Model (COM) technologies that allow information to be shared between applications, and can perform any action a user would normally be able to perform. This allows applications to use Active X to eliminate the restrictions imposed by application-specific formats for the processing and storage of data (i.e., they can be

automated regardless of program dependencies). Macros are a series of stored keystrokes that can be sequentially executed at one time and repeatedly re-executed. This allows redundant tasks within applications to be automated and executed. Java Applets, Active X, macros, and similar scripting mechanisms have become a regular part of Web browsing, multi-player gaming, and business automation, and provide a foundation for streamlining computing functions for improved services.

When the above technologies are used for executing commands and activities that are unwanted by a user, they can be considered malicious scripts. When Java Applets are misused, they can be employed to read the system properties directories and files of the user's machine, create a socket to communicate with another computer, send e-mail from the user's account, and a host of other functions. When Active X is misused, it can be utilized to instruct accounting software to write an electronic check to someone's bank account, and a host of other automated attack sequences. Macros have been used by attackers from their beginnings to perform virus-like functions and as a result have been dubbed macro viruses. These are executed whenever an infected document is opened. They reproduce by adding themselves to the application's "normal" or base blank document. Whenever a new or existing document is opened, the macro duplicates itself into that document. It is then transported to new systems when an infected file is transferred and opened on another machine.

EXTERNAL PENETRATION

In this section, an examination of the more common approaches to penetrating a system externally will be presented.

Social Engineering

When we were young, there was a standard notion that stated it never hurt to ask a question. If one is being polite, sounds as if they are well versed in a topic or environment, and can communicate a sense of purpose in their voice, questions asked in a professional environment can be used to hurt organizations and individuals by convincing them to disclose confidential details. This information in turn can be used for future attack attempts. The aim of social engineering is to get people to disclose confidential information such as user names, passwords, points of entry, working hours, and so forth as the first step in penetrating a system. Traditional approaches to social engineering have included official-sounding telephone calls from so-called bank personnel or an intruder posing as an employee or system administrator, or even an official visitor using an employee's phone to call technical support while the employee steps out of his or her office for a few minutes. The knowledge gained from this type of deception may very well bring an intruder much closer to gaining an initial access point into an information system or network. Such information can also greatly enhance other methods discussed in previous sections as well as later in this section.

Physical

The simplest access method to system resources may very well be physical access. Because of the small size of computers, it is not uncommon to have a computer server placed directly within easy reach for maintenance by a given department or individual. This is especially true of small to medium-sized businesses that give more responsibility to individuals directly involved in using and managing the system. As a result, an intruder or visitor may be able to access the terminal while in proximity of it. This allows for the quick installation of software such as a keyboard logger or a monitoring device such as a wireless transmitter attached to a keyboard or video screen. The information collected by whatever means can be retrieved or transmitted to the intruder for supporting later intrusion activities. Such an approach is not the only means that physical access can be used. Physical access can also provide the following opportunities to an intruder:

- **Primary unit:** The intruder may unplug a computer unit's peripherals (i.e., monitor, keyboard, etc.) and walk away with it. Once this equipment has been examined and/or modified, it may be able to be plugged back into the system and used for future surveillance and/or attacks. This is one reason why better-organized facilities keep such systems in restricted, locked rooms and govern the access of their facility by guests and intruders alike by enforcing security policies and alarms.
- **Cabling:** The physical cabling of an organization's network is another point of vulnerability that must be carefully considered. Transmission wires come in twisted-pair telephone wire, coaxial cable, and fiber optic. In many cases these internal wires traverse through walls and conduits, and eventually terminate at wall plugs and/or switch racks or hubs. The ability to tap into these wires is related to their ease of access in the case of twisted pair and coaxial, and a higher level of skill and equipment in the case of fiber optic. In many cases they are encased in conduits, but in many other cases they are openly exposed. Also, these wires eventually must exit a building, and as such, become susceptible to outside splicing.
- **Equipment disposal:** The proper disposal of older equipment is an aspect of physical security. Hard drives contain details and configuration settings of a once operational computer that was connected to an internal network. In many cases, these retired computers are given away to employees or tossed in a dumpster after their hard drives have been reformatted. The problem with this approach is that computer forensic techniques that are readily available today can recover lost or formatted data of a hard drive that has been formatted up to six times. What is required is permanent eraser software that writes and re-writes a hard drive repeatedly in a fashion that makes such a recovery impossible. In addition, old backup tapes and CD-ROMs must also be securely disposed.

Having physical access to facilities and equipment provides a huge advantage in gaining additional access to a system. User histories, activities, and data can be retrieved in a major step towards additional penetrations. Therefore, physical intrusions will continue to be an effective step in gaining additional access and knowledge by intruders.

Wireless Communication Medium

Wireless devices are appearing everywhere a landline, cable, or cord served the same purpose. Wireless devices utilize laser, radio frequencies, and infrared technologies to imprint data on its frequency wave as a means of transmission. These technologies range from line-of-sight connectivity as in the case of laser transmissions, radio frequencies as in the case of cellular phones and networking equipment, to satellite control systems and broadcast transmissions. The basic nature of wireless communications makes this transmission medium accessible from any point within its broadcast range or point-to-point path. This is both its greatest strength and weakness. Generally, when two devices initially wish to connect, a handshake protocol establishes the two devices' connection and/or any security mechanisms that will be used throughout the connection. This link is maintained until discontinued or interrupted. Devices communicating via a wireless link sometimes experience environmental conditions that cause signal degradation and/or data corruption that can result in the retransmissions of previously sent data. These two issues provide intruders with the foundation for piercing such systems and any security that may be present or prevent the communication connection from being maintained. While there are numerous standards in existence for securing wireless communications, the underlying notion that the transmission can be openly monitored makes this transmission medium vulnerable to eavesdropping. Research conducted in 2004 in Auckland, New Zealand, showed that more than 60% of wireless office systems work without any protection—that is, anybody with a laptop and wireless antenna would be able to use a network as an authorized user. This allows an intruder to observe and record communications for examination of content, security keys, and/or decryption of the transmission. Such communications are also subject to jamming devices that flood the wavelengths with "white noise" and therefore preventing a device-to-device connection.

One last major security vulnerability of wireless devices has to do with having its source location ascertained. A transmitting device can have its physical location be deduced through a host of detection methods (i.e., triangulation, etc.) because all such devices have a point of origin for their transmission. While military versions of

wireless devices have additional protective security mechanisms such as frequency hopping and spread spectrum, most commercial facilities continue to be shown as vulnerable to disruptions, monitoring, and intrusion.

User Access Points

Users of data communications utilize data pathways to access systems and resources on computer systems. In nearly all cases, users are assigned user accounts that specify the level and domains that the user is permitted to access. These accounts may be generic as in the case of an anonymous user or based on an access control list (i.e., a predetermined list of users and their corresponding access levels). The user traditionally enters his or her user account name and a password. The connecting computer then establishes a session (i.e., the period of time that a communication link is maintained) with the connected system. All activities that occur on the connected system are performed at the access control rights assigned to the user account. Therefore, one of the fundamental attack methods by intruders is to identify any user names and passwords to access a system.

One method of achieving this information is through the use of packet sniffing. As previously discussed, packet sniffing is a method of examining every packet that flows across a network in order to gain information on the communication content. When a sniffer is placed on an attached computer within a network, that computer may then anonymously monitor the traffic coming and going on that particular network. Essentially, a sniffer creates a socket stream on the network, has its network interface card configured to promiscuous mode, and begins reading from the open socket stream. When data is sent over communication channels in clear text form, reading it becomes quite simple. When a user seeks to connect to a system, that system usually prompts the user for a user name and password. This information is then entered and transmitted over the communication channel to the server for authentication. It is at this point that a sniffer may capture this information for later use by an intruder if not encrypted. The attacker can then gain access to the system with all the access rights of the legitimate user, and may even be capable of elevating these access rights once he or she has access to a given system or network. Because not all systems encrypt these transactions, sniffers continue to be an issue in securing user accounts.

Another approach that is used by intruders is to use direct attacks on the password of a user account. Sometimes, a user name is known or can be deduced from other transactions (i.e., social engineering, similar formatting of other users, etc.). All that is then needed is the corresponding password. This can be accomplished using brute force and dictionary attacks on the user's account. Brute force attacks rely on sheer computing power to incrementally try all of the possible password combinations for a given user account name. Dictionary attacks utilize the most common words that can be found in a dictionary such as names, places, and objects as the password for any given user account. Both approaches are typically automated using cracker exploit software. More secure systems provide a user a limited number of attempts at entering a correct password before they disable the account for a specified period of time. After this delay, a user account may generally then be logged into when the correct password is entered. However, many systems still do not provide or activate this security feature, leaving it open to such attacks.

Another well-established user access point is the dial-up connection to an Internet service provider (ISP) such as AOL or AT&T. Throughout the intruder community, it has been very common to trade accessible or cracked user accounts for other software cracks and specialty exploits. Gaining access to such an account grants the user the capability to use the account for spamming (i.e., unsolicited mass e-mailing), anonymous browsing, penetrating other accounts without direct traceability to the intruder, and also the use of the account's access rights within the ISP. In order to check for e-mail, initiate a session outside the ISP, or other seemingly harmless activities of a legitimate user, the user account must be granted certain access rights within the ISP in order to view files and execute activities. These access rights while restricted are still greater than non-subscriber rights, and assume a measure of responsibility and accountability on behalf of a legitimate user. When an account has been hijacked, such responsibility fails to influence activity decisions. Use of such an account by an intruder may allow the intruder to view other subscribers' e-mails, access server folders and configuration settings in order to elevate access rights, reconfigure various system components to attack other networks, or even turn the breached system into a proxy server as an anonymous staging point for other remote activities and/or attacks.

DNS and Routing Vulnerabilities Attacks

Domain name system (DNS) is a mechanism of recognizing Internet addresses. One can imagine the consequences if messages would be forwarded to the wrong IP address. The existing technology and system procedures have limited authentication capabilities, and a well-designed DNS attack can create havoc to the world network. Due to the lack of strong authentication within DNSs, the mechanisms controlling the flow of packages could be changed and therefore unauthorized information may be received and/or acted upon.

STARTING POINTS FOR PREPARATIONS

Awareness of the possibility of such attacks can lead to the preparation of a program of activities aimed at setting up effective defenses against potential threats. These fortifications generally fall into the following four categories:

- Physical defenses that control physical access to facilities
- System defenses that limit the capabilities of unauthorized changes to data stored and transmitted over a network
- Personnel defenses that limit the chances of inappropriate staff behavior
- Organizational defenses that create and implement an information security plan

Physical Defenses

Physical security as it applies to information security considers the activities undertaken, and the equipment installed to accomplish the following objectives:

- **Protection against unauthorized persons to penetrate the designated off-limit areas of the company premises:** This definition implies that there may be several classes of "unauthorized persons" and the company premises may have security zones with different access rights. Some areas, like the reception area, could be open to virtually anybody, while other areas are accessible only to a limited number of company employees.
- **Protection against the theft of company IT equipment, especially that containing sensitive information:** This protection extends to company equipment that may be physically outside the company's premises.
- **Protection against the physical destruction of company IT equipment:** This can include the protection against such acts as the planting of explosives within company premises. This also covers the protection measures against such events as fire, floods, and earthquakes.
- **Protection against unauthorized reading of information, regardless of its form (i.e., visual, acoustic, or analog signals):** Security measures have to prevent unauthorized persons from reading sensitive data from a computer screen, the interception of spoken messages, the tapping of telephone lines, or similar acts.

The security measures discussed here do not include security breaches such as the unauthorized system access to data through a broken password subsystem or the breaking of a cryptographic message. It also does not cover the breaches resulting from wrongly deployed mobile telecommunications systems, such as a mobile local area network.

System Defense Mechanisms

Firewalls

As part of the basic defense for intrusions within a system, firewalls provide basic barriers against penetrations. Firewalls tend to be a combination of hardware and software that acts as a partition between an internal network

and the outside electronic world. Essentially, a firewall performs two primary functions. The first of these is hiding the IP address of the internal network from any connecting telecommunication networks that may wish to observe and/or connect to a system inside the firewall. This is like making all of the telephone numbers and mailing addresses of a business unlisted. In this way, an intruder must first know the destination IP address before proceeding to additional steps in an attack. The second function that a firewall performs is the control of packets through its communication ports in both directions. A port is the end point to a logical connection in a communication path, and as such, can be set to accept packets that are inbound, outbound, and/or both for a given port. For instance, if a system administrator wanted to prevent files from being transferred in an outbound direction, then ports 20 and 21 (i.e., used for File Transfer Protocol) would need to be configured to reflect these wishes among other additional ports (i.e., there are many ways of transferring files indirectly). Firewalls are commonly remotely accessed using a username and password from a specified IP address in order to configure and maintain them. This makes them susceptible to previously discussed attacks. Also, because many firewalls are not self-contained systems and therefore use a given system's operating or network operating system, any vulnerability that exists in the operating system provides a means for bypassing some of its protective mechanisms.

Virus Scanner

The name implies what the virus scanner does: search for all malicious software. Various scanners are available on the market. They operate on one or many principle likes these:

- Search for a given type of code, indicating existence of malicious software
- Search for unauthorized changes to the original software
- Detect unauthorized activities of a given system operating under given conditions

Due to the fact that everyday brings definitions of new malware, any virus scanner to operate properly must be updated frequently.

Vulnerabilities and Penetration Tools

This is a vast group of products which work as automated systems for collection end evaluation of information about properties of devices connected to the network. These devices, extremely useful for a security manager. must be used extremely carefully. Launching such a system without proper authority may result in official persecution. Such a case was reported during 2005 in the UK. A security expert noticed a strange occurrence regarding a charity Web site, to which he is a donator. As an interested party, he launched a vulnerability diagnostic tool and ended up facing several thousands of British pounds in penalties that were imposed by the court. There are now countries where even the possession of such software may lead to persecution, such as is the case in New Zealand.

Personnel Defenses

The importance of security issues relating to personnel policies has and continues to be a factor in the overall protection of organizational systems. These are mainly the security issues related to contractual agreements between companies and their employees, plus their implications. These include:

- Personnel screening prior to employment
- Application of the security policy and establishing confidentiality agreements
- Establishment and execution of a user training program in security
- Establishment and execution of a policy dealing with handling security incidents and malfunctions

Organizational Defenses

All the defense mechanisms outlined above must be implemented in an organized way. This means every organization should set up a plan on how to develop and implement security measures. An integral part of that procedure is formulating an information security policy—a document that would inform the staff what security measures are introduced and what is expected staff behavior. We would also like to emphasize that when dealing with cyber terrorist and cyber warfare attacks, the most effective mode of operation is the system approach, when all major decisions are done from the point of overall advantage to the whole of an organization.

PLANNING SECURITY SYSTEMS, OVERALL PRINCIPLES

To protect installations against possible attacks, including terrorist attacks, we must define all the possible threats, estimate the potential losses resulting from the materialization of these threats, design a line of defense, and implement it.

Cyber terrorism and information warfare are becoming new and important threats against information technology resources and must be a part of the overall planning, design, and implementation process aimed at providing overall protection. The most significant part of building an overall protection plan is founded in risk management analysis. It is feasible to secure all assets from all parties given highly restrictive access and unlimited resources. However, the real world must embrace a set of priorities that has a rational foundation to deciding priorities and any subsequent decisions based on that rationale.

This process is derived from a basic understanding that is easiest to explain by asking some simple questions such as:

- How important is it that our operations not be disrupted?
- How much is our proprietary and personal information worth to us and others?
- What will it cost to replace our systems and information?
- What are the consequences of not protecting our systems?
- How much are we willing to spend to protect our assets?

The reality is that it is nearly impossible to fully assess the business loss in value resulting from information being destroyed or made public. This is due to two reasons:

1. It is hard to associate value to an event which may not happen and has never happened before. Imagine a case where a company's marketing plan was stolen. This is a first occurrence, and as such, who can predict the financial consequences of such a theft even though there will likely be far-reaching consequences?
2. The intent of the act can greatly impact the loss-in-value factor. At the beginning of the 1990 Gulf War, a laptop containing detailed information on the Allied Forces' plans for the liberation of Kuwait was stolen. Fortunately, the information on the machine did not reach the Iraqi government. One can imagine the possible costs of changing battle plans or human losses resulting from the Iraqi military acquiring these plans.

All of the above leads us to a conclusion that prior to launching the development of any security program, a thorough information technology risk analysis must be performed. It should be performed to justify the implementation of controls; provide assurance against unacceptable risk; assess compliance with regulations, laws, and corporate policy; and balance the controls of the risks. The results of the risk analysis are then used to develop and implement organizational security programs, including issues related to countering cyber terrorist and cyber warfare threats.

CONCLUSION

The end of the 20th century and the beginning years of the next century have brought a rising wave of terrorist attacks. These attacks are influencing the IT domain, and the most probable attacks now are collateral effects (i.e., destruction of a building housing the organization's HQ resulting in the destruction of its IT facilities). Up until now, we have not witnessed any spectacular, worldwide cyber terrorist attacks, but the probability of such attacks continues to be on the rise. This real threat is forcing us to find answers to obvious questions:

- "To what extent is my installation vulnerable to cyber warfare and cyber terrorist attacks?"
- "What do I need to do to protect my systems from this growing threat?"

These are unknown territories. Finding the answers to these questions may be done by following the line of thoughts of terrorists and examining their connections between traditional terrorist attacks and cyberspace.

The threat of cyber terrorism and cyber warfare still may not change the procedures of a typical risk analysis, nor may it result in introducing new security controls. However, these threats have brought a new dimension to classical risk analysis and have elevated some issues related to information security that were not very popular in the past.

Traditional risk assessment analysis examines the results of possible activities carried out mainly by individuals driven by curiosity, a lust for wealth, and/or individuals having a grudge against a given organization. Cyber terrorists add a new dimension to this process. We must predict the foundational nature of their actions and setup a plan to deal with it.

In this chapter, among the other items brought forward, we have outlined the possible behavioral drivers of the attackers. We think that the predominant wish of a terrorist of any type is to create fear and harm among the widest possible spectrum of society. We also suggested some of the more important activities that should be undertaken to reduce the possibility of cyber-based attacks and/or their resulting consequences. We have identified the most probable types of cyber warrior and cyber terrorist attacks, and hope that this will serve as a foundation to understand and effectively take action in a prevention, detection, and responsive manner.

REFERENCES

CAIDA. (2005). *Analysis of Code Red.* Retrieved from http://www.caida.org/analysis/security/code-red/

Center for Strategic and International Studies. (1998). Cybercrime, cyberterrorism, cyberwarfare, averting electronic Waterloo.

CERT Coordination Center. (2000, December). Results of the Security in ActiveX Workshop. Software Engineering Institute, Carnegie Mellon University, USA.

Colin, B. (1996). The future of cyberterrorism. *Proceedings of the 11th Annual International Symposium on Criminal Justice Issues*, Chicago.

Computer Security Institute. (2006). *2005 CSI / FBI computer crime and security survey.* Retrieved from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Convention on Cybercrime, Council of Europe. (2001). Proceedings of Convention.

Denning, D. (1999). *Information warfare and security*. Boston: Addison-Wesley.

Elmusharaf, M. (2004). *Cyber terrorism: The new kind of terrorism computer*. Retrieved April 8, 2004, from http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism

Journal of Information Warfare, Australia, since 2001.

Molander, R., Riddle, A., & Wilson, P. (1996). *Strategic information warfare, a new face of war*. Rand National Defense Institute.

National Security Telecommunications and Information Systems. (n.d.). Security policy no. 11. Retrieved from http://niap.nist.gov and http://nistissc.gov

President's Critical Infrastructure Protection Board. (2002). National strategy to secure cyberspace.

Schneier, B. (2006). *Counterpane Newsletter,* (April).

ADDITIONAL READINGS

Alexander, D., Arbaugh, W., Keromytis, A., & Smith, J. (1998). Safety and security of programmable network infrastructures. I*EEE Communications Magazine*, (October).

Alvey, J. (2002). Digital terrorism: Hole in the firewall? *Public Utilities Fortnightly*, (March).

Anagnostakis et al. (2002, April). Efficient packet monitoring for network management. *Proceedings of the IEEE/IFIP Network Operations and Management Symposium.*

Bih, J. (2003). Internet snooping. *IEEE Potentials*, (October/November).

Burge et al. (1997, April). Fraud detection and management in mobile telecommunications networks. Proceedings of the European Conference on Security and Detection.

Chakrabarti, A., & Manimaran, G. (2002). Internet infrastructure security: A taxonomy. *IEEE Network*, (November/December).

Colarik, A. (2003, November). *A secure patch management authority*. PhD Thesis, University of Auckland, New Zealand.

Crocker, S. (2004). Protecting the Internet from distributed denial-of-service attacks: A proposal. *Proceedings of the IEEE, 92*(9).

Dotti, P., & Rees, O. (1999, June). Protecting the hosted application server. *Proceedings of the IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.*

Edwards, M. (2001, March). *FBI finds secret U.S. source code on computer in Sweden*. InstantDoc #20178.

Ernst & Young. (2004). Global information security survey 2004. Assurance and Advisory Business Services.

Harper, H. (2002). Cyberterror: A fact of life. *Industrial Distribution*, (January).

Haugh, R. (2003). Cyber terror. *Hospitals & Health Networks*, (June).

Institute for Information Infrastructure Protection. (2003, January). *Cyber security research and development agenda*.

Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee. (2002, October). Statement for the record by Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency.

Karrasand, M. (2003, June). Separating trojan horses, viruses, and worms: A proposed taxonomy of software weapons. *Proceedings of the 2003 IEEE Workshop on Information Assurance.*

Langnau, L. (2003). Cyberterroism: Threat or hype? *Material Handling Management*, (May).

Levack, K. (2003). The E-Government Act of 2002: A stab at cyber security. *EContent*, (March).

Magoni, D. (2003). Tearing down the Internet. *IEEE Journal on Selected Areas in Communications, 21*(6).

Mavrakis, N. (2003). Vulnerabilities of ISPs. *IEEE Potentials*, (October/November).

Maxion, R., & Townsend, T. (2004). Masquerade detection augmented with error analysis. *IEEE Transactions on Reliability, 53*(1).

McCollum, T. (2003). Report targets U.S. cyber-security. *The Internal Auditor,* (February).

Mearian, L. (2002). Wall Street seeks cyberterror defenses. *Computerworld*, (March).

Misra, S. (2003). High-tech terror. *The American City & Country*, (June).

Mukhtar, M. (2004). *Cyber terrorism: The new kind of terrorism.* Retrieved April 8, 2004, from http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism

Nasir, B. (1994, October). Components, modeling and robustness of network management for telecommunications systems. *Proceedings of the IEE Colloquium on Network Management for Personal and Mobile Telecommunications Systems*.

NATO Parliamentary Assembly, Science and Technology Sub-Committee on the Proliferation of Military Technology. (n.d.). Draft interim report: Technology and terrorism. Retrieved from http://www.nato-pa.int/publications/comrep/2001/au-121-e.html#3

NATO Parliamentary Assembly, Science and Technology Sub-Committee on the Proliferation of Military Technology. (n.d.). *Draft report: Technology and terrorism: A post-September 11 assessment.* Retrieved from http://www.nato-pa.int/publications/comrep/2002/av-118-e.html#3

Ollmann, G. (2004, September). *The phishing guide: Understanding & preventing phishing attacks.* NGSSoftware Insight Security Research.

Pescape, A., & Ventre, G. (2004, April). Experimental analysis of attacks against routing network infrastructures. *Proceedings of the 2004 IEEE International Conference on Performance, Computing, and Communications.*

President's Critical Infrastructure Protection Board. (2002, September). *The national strategy to secure cyberspace.*

Reed, M., Syverson, P., & Goldschlag, D. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications, 16*(4).

Rennhard, M., Rafaeli, S., Mathy, L., Plattner, B., & Hutchinson, D. (2002, June). Analysis of an anonymity network for Web browsing. *Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises.*

Rietscha, E. (2003, September). *Buffer overrun vulnerabilities in Microsoft programs: Do you really need to apply all of the security patches?* SANS Institute.

Sabeel, A., Rajeev, S., & Chandrashekar, H. (2002/2003). Packet sniffing: A brief introduction. *IEEE Potentials*, (December/January).

Shimeall, T., Williams, P., & Dunlevy, C. (2001/2002). Countering cyber war. *NATO Review*, (Winter).

Solomon, H. (2003). War in Iraq could cripple Internet, IDC. *Computing Canada,* (January).

Spencer, V. (2002). Cyber terrorism: Mass destruction or mass disruption? *Canadian Underwriter,* (February).

Thibodeau, P. (2001). War against terrorism raises IT security stakes. *Computerworld*, (September).

Thuraisingham, B. (2000). Understanding data mining and applying it to command, control, communications and intelligence environments. *Proceedings of COMPSAC 2000.*

U.S. Commission on National Security. (1999, September). *New world coming: American security in the 21st century: Major themes and implications.*

U.S. General Accounting Office. (2003, January). *Critical infrastructure protection: Efforts of the financial services sector to address cyber threats.*

Vatis, M. (2001, September 22). *Cyber attacks during the war on terrorism: A predictive analysis.* Institute for Security Technology Studies at Dartmouth College.

Verton, D. (2002). Experts predict major cyberattack coming. *Computerworld*, (July).

Voyiatzis, A., & Serpanos, D. (2003). Pulse: A class of super-worms against network infrastructure. *Proceedings of the 23rd International Conference on Distributed Computer Systems Workshops.*

Wan, K., & Chang, R. (2002). Engineering of a global defense infrastructure for DDOS attacks. *Proceedings of the 10th IEEE International Conference on Networks.*

Weaver, N., Paxson, V., Staniford, S., & Cunningham, R. (2003). A taxonomy of computer worms. *Proceedings of the 2003 ACM Workshop on Rapid Malcode.*

Wheatman, V., & Leskela, L. (2001, August). *The myths and realities of 'cybersecurity' in China.* Gartner.