Chapter Ten

EMERGING CHALLENGE: SECURITY AND SAFETY IN CYBERSPACE*

Richard O. Hundley and Robert H. Anderson

With more and more of the activities of individuals, organizations, and nations being conducted in cyberspace,[1] the security of those activities is an emerging challenge for society. The medium has thus created new potentials for criminal or hostile actions, "bad actors" in cyberspace carrying out these hostile actions, and threats to societal interests as a result of these hostile actions.

POTENTIAL HOSTILE ACTIONS

Security holes in current computer and telecommunications systems allow these systems to be subject to a broad spectrum of adverse or hostile actions. The spectrum includes: inserting false data or harmful programs into information systems; stealing valuable data or programs from a system, or even taking over control of its operation; manipulating the performance of a system, by changing data or programs, introducing communications delays, etc.; and disrupting the performance of a system, by causing erratic behavior or destroying data or programs, or by denying access to the system. Taken together, the surreptitious and remote nature of these actions can make their detection difficult and the identification of the perpetra-

*Richard O. Hundley and Robert H. Anderson, "Emerging Challenge: Security and Safety in Cyberspace," *IEEE Technology and Society*, pp. 19–28 (Winter 1995/1996).

tor even more difficult. Furthermore, new possibilities for hostile actions arise every day as a result of new development and applications of information technology.

The bad actors who might perpetrate these actions include: hackers, zealots or disgruntled insiders, to satisfy personal agendas; criminals, for personal financial gain, etc.; terrorists or other malevolent groups, to advance their cause; commercial organizations, for industrial espionage or to disrupt competitors; nations, for espionage or economic advantage or as a tool of warfare. Cyberspace attacks mounted by these different types of actors are indistinguishable from each other, insofar as the perceptions of the target personnel are concerned. In this cyberspace world, the distinction between "crime" and "warfare" in cyberspace also blurs the distinction between police responsibilities, to protect societal interests from criminal acts in cyberspace, and military responsibilities, to protect societal interests from acts of war in cyberspace.

We call protecting targets in cyberspace, such as government, business, individuals, and society as a whole, against these actions by bad actors in cyberspace, "cyberspace security." In addition to deliberate threats, information systems operating in cyberspace can also cause unforeseen actions or events— without the intervention of any bad actors—that create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded. Such safety hazards can result from both software errors and hardware failures. We call protection against this additional set of cyberspace hazards "cyberspace safety." In the new cyberspace world, government, business, individuals, and society as a whole require a comprehensive program of cyberspace security and safety (CSS) [1]-[5].[2]

CONSEQUENCE CATEGORIES

We have used four categories to define the consequences of cyberspace attacks, categories based on the degree of economic, human, or societal damage caused. From the least to the most consequential, they are:

1) *minor annoyance or inconvenience*, which causes no important damage or loss, and is generally self-healing, with no significant recovery efforts being required;

2) *limited misfortune*, which causes limited economic or human or societal damage, relative to the resources of the individuals, organizations, or societal elements involved, and for which the recovery is straightforward, with the recovery efforts being well within the recuperative resources of those affected, organizations, or societal elements;

3) *major or widespread loss*, which causes significant economic or human or societal damage, relative to the resources of those involved, and/or which may affect, or threaten to affect, a major portion of society, and for which recovery is possible but difficult, and strains the recuperative resources of the affected individuals, organizations, or societal elements; and

4) *major disaster*, which causes great damage or loss to affected individuals or organizations, and for which recovery is extremely difficult, if not impossible, and puts an enormous, if not overwhelming, load on the recuperative resources of those affected.

We assert that it is not always possible to measure human or societal damage in purely economic terms.

PAST INCIDENTS

CSS incidents constituting a minor annoyance or inconvenience have been a frequent occurrence across the entire spectrum of target categories. For some targets (e.g., the AT&T Bell Labs computer network or the unclassified Pentagon network) such minor annoyances can occur one or more times every day. For many computer installations, such incidents have become so commonplace that they are no longer reported.

CSS incidents constituting a limited misfortune—e.g., computer installations disrupted for limited periods of time, or limited financial losses (relative to the resources of the target)—have occurred less frequently, but nevertheless numerous examples exist across the entire spectrum of targets. A number of these are reported in [1] and [4].

There have even been a few cases of incidents which many observers would class as major or widespread loss to the target(s) involved. Examples include the "AIDS Trojan" attack in December 1989, which caused (among many other things) an AIDS research center at the University of Bologna in Italy to lose 10 years of irreplaceable data [4]; the AT&T network failure on January 15, 1990, due to a software error, which disrupted and virtually shut down a major portion of the U.S. nationwide long-distance network for a period of about nine hours [1], [4]; the almost total disruption of the computers and computer networks at the Rome (NY) Air Force Base for a period of 18 days in early 1994, during which time most (if not all) of the information systems at Rome were "disconnected from the Net" [6]; and the MCI calling-card scam during 1992–1994, in which malicious software was installed on MCI switching equipment to record and steal about 100,000 calling card numbers and personal identification codes that were then sold to hackers throughout the U.S. and Europe and posted on bulletin boards, resulting in an estimated $50 million in unauthorized long-distance calls[7].

We know of no clear examples to date of a CSS incident constituting a major disaster.

POTENTIAL FUTURE INCIDENTS

Whatever may have happened in the past, we expect cyberspace security and safety incidents to become much more prevalent in the future, due to the facts that more and more people are becoming "computer smart" all over the world; bad actors of many different types are becoming more and more aware of opportunities in cyberspace; connectivity is becoming more widespread and universal; more and more systems and infrastructures are shifting from mechanical/electrical control to electronic/software control; and human activities in cyberspace are expanding much faster than security efforts.

Recent data support this expectation[8].

Accordingly, we expect that, in the future, CSS incidents constituting a minor annoyance or inconvenience will become commonplace across the entire spectrum of targets; incidents constituting a limited misfortune could also become a common occurrence; CSS incidents

constituting a major or widespread loss are quite possible for all targets in cyberspace; and CSS incidents constituting a major disaster are definitely possible for some targets in special cases.

Some examples of special cases in which major disasters may be possible include the following:

- *Physical and functional infrastructures*, such as the air traffic control system, possibly leading to the crashes of one or more aircraft.
- *Military and national security*. For example, if a cyberspace-based attack were to bring down an essential military command and control system at a critical moment in a battle, it might lead to the loss of the battle. If the battle were pivotal, or the stakes otherwise high enough, this could ultimately lead to military disaster.
- *Other societal organizations and activities*. With medical care becoming increasingly dependent on information systems, many of them internetted, a perpetrator could make changes to data or software, possibly resulting in the loss of life.

Other examples of possible cases leading to major disasters may occur to the reader. Today these examples are all hypothetical. Tomorrow one or more of them could well be real. Our impression is that CSS incidents will become much more prevalent; they will impact almost every corner of society in the developed nations of the world; and the consequences could become much greater.

INFRASTRUCTURE FRAGILITY

There are many uncertainties associated with this projection of future cyberspace security and safety incidents. Attacks on vital infrastructures are one of the things most likely to cause widespread repercussions for society. Accordingly, one of the most important uncertainties has to do with the degree of robustness of current and future infrastructures: Are the key physical and functional infrastructures in various nations highly robust, due to built-in redundancies and self-healing capabilities? Or do some infrastructures have hidden fragilities that could lead to failures having important consequences?

Conventional wisdom regarding these questions is not always correct. For example, prior to 1990, the AT&T long distance network in the U.S. was usually thought to be very robust, with many alternative paths for long distance calls to take, going through different switching centers. But all of these switching centers use the same software, and when new software was introduced in 1990, every long-distance switch had the same bad line of code. So at the software level, there was no redundancy at all, but rather a fragility that brought a large part of the AT&T long-distance network down[1], [4].

The message is clear: many infrastructures may not be as robust as they seem; a detailed look at vulnerabilities of specific infrastructures is needed.

ACTORS RESPONSIBLE FOR INCIDENTS

By far the greatest portion of past cyberspace security incidents have been perpetrated by "hackers": individuals satisfying a variety of personal agendas, which in their view do not include criminal motives [9], [10]. This continues to be the case regarding current incidents.

In recent years, the role of criminals in cyberspace incidents has increased. According to law enforcement professionals consulted by the authors, this has come about not as a result of the criminal element becoming more aware of opportunities in cyberspace, but rather primarily as a result of computer hackers "growing up" and some (small) fraction of them realizing and exploiting the financial opportunities open to them via criminal acts.

There are no known cases in the open literature of cyberspace security incidents perpetrated by terrorists or other malevolent groups, commercial organizations, or nations. However, there are plenty of rumors of business organizations and intelligence agencies outside the U.S. that have mounted cyberspace-based attacks against companies in other nations as a means of industrial or economic espionage.

In addition, police authorities in Europe have recently begun to discern a number of potentially more dangerous actors manipulating and guiding some malicious hacker activity. This appears to include

professional hackers, who are often the source of the penetration tools used by the "ordinary" hackers; information brokers, who frequently post notices on European hacker bulletin boards offering various forms of "payment" for specific information; private detectives, who also often use the European hacker bulletin boards as a means of obtaining information regarding targeted individuals or organizations; foreign embassies, who appear to have been behind the bulletin board activities of at least some European private detectives and information brokers; and organized crime.

Whatever may have happened in the past, in the future we expect all five of our classes of bad actors to continue participating in cyberspace security incidents.

MECHANISMS: PAST AND FUTURE

A number of mechanisms have been prevalent in past cyberspace security and safety incidents and are likely to be prevalent in future incidents as well. Many incidents involve more than one of these mechanisms, which include:

- *Operations-based attacks,* taking advantage of inadequate or lax security environments. Exploitation of deficient security environments has been a feature of many/most past successful cyberspace penetrations and is likely to continue to be prevalent in the future—as long as lax security continues to be commonplace.
- *User authentication-based attacks,* which bypass or penetrate login and password protections. Such attacks are a common feature of many/most past cyberspace security incidents and are also likely to be prevalent in the future.
- *Software-based attacks*, exploiting software features (e.g., maintenance backdoors), programmatic flaws, and logical errors or misjudgments in software implementation, as well as the insertion of malicious software.
- *Network-based attacks*, which take advantage of network design, protocol, or topology in order to gather data, gain unauthorized system access, or disrupt network connectivity. This can include alterations of routing tables, password sniffing, and the spoofing of TCP/IP packet addresses. Attacks of this type have not been

common in the past. However, beginning in 1994 hackers have been detected penetrating Internet routers to install password sniffers, etc.; TCP/IP packet address spoofing was first detected in early 1995. Such attacks—including attempts to disrupt Internet connectivity—could become much more common in the future, unless Internet security is markedly improved.

- *Hardware-based attacks or failures*, exploiting programmatic or logical flaws in hardware design and implementation, or component failures. These have not been a feature of past cyberspace security incidents (i.e., deliberately perpetrated incidents), but have played a role in occasional safety hazards (i.e., accidental incidents). This is likely to continue in the future.

ADDITIONAL KEY FACTORS

There are a number of additional factors impacting on the cyberspace security problem and of necessity shaping any effective protective strategies.

Increasing Transnationalism

As is well known, cyberspace does not respect national boundaries. In recent years more and more nations throughout the world have become "connected" to the world network, and within those nations connectivity has become more and more universal.

Every year greater numbers of individuals and organizations in the U.S. are taking advantage of this increasing worldwide connectivity to become involved, via cyberspace, in economic or social activities with individuals and organizations in other nations. These transnational activities are becoming increasingly important to the U.S. individuals and organizations involved; they will not willingly give them up.

Since threats in cyberspace pay no regard to regional or national boundaries, knowledge of computer hacking techniques has spread around the globe, and the perpetrator of a security incident can just as well be on the other side of the world as across the street.

For both of these reasons—the nature of activities in cyberspace and the nature of threats—cyberspace has become effectively transnational. No nation has effective sovereignty over cyberspace. Any effective cyberspace protective strategy must take this into account.

Current Security Inadequate

The information processing systems and telecommunications systems currently in use throughout the world are full of security flaws, and new security flaws are being uncovered almost every day, usually as a result of hacker activity. As new developments and applications of information technology become available and as human activities in cyberspace continually expand, security efforts appear to be lagging behind. There is currently no effective way to police cyberspace. Considering the rapid increase in the number of reported security incidents in recent years, along with the apparent increase in the severity of these incidents, it does not appear that the "good guys" are winning; they may not even be holding their own.

Current security operations in cyberspace are inadequate. This is not the result of a lack of security technology. Rather, it reflects a very limited application of available technology; most of the available computer security technology is not used in most of the computers in the world.

Acceptance Lacking

The U.S. has had a computer security program since the 1960s. In spite of these efforts, the U.S. is full of insecure computers today. There are several reasons for this. A primary reason is that user acceptance and utilization of available computer security safeguards has been reluctant and limited. There are several causes of this lack of user acceptance.

- Typically, user interfaces accompanying security features are awkward. As a result, the secure systems are more difficult to use than the nonsecure systems. Many users are not motivated to take the extra effort.
- Users have not considered security features as adding value, and therefore are reluctant to pay extra for such features.

- Computer hardware and software manufactures have not perceived the security market as being attractive. Rather, it has usually been considered a limited, niche market. Therefore the largest commercial manufacturers (Microsoft, Apple, etc.) have not included many security features in their primary product lines.
- Many individual users do not understand the need for a communal role in cyberspace security and do not accept responsibility for such a role.
- Most users don't take computer security seriously until something bad has happened to them or to their immediate organization.

For reasons such as these, most of the computer security technology currently available is not used on most of the computers in the world. A typical computer on the Internet uses a garden variety Unix operating system with few additional security safeguards. Similarly, a typical desktop computer uses the MS-DOS, MS-DOS plus Windows, or Macintosh operating systems, once again with few additional security safeguards. The various secure operating systems, multilevel security systems, and Orange Book[3] compliant software systems that have been developed are primarily used in restricted, niche applications.

Isolation Disappearing As Option

Twenty or thirty years ago there was a simple solution to this problem: the physical isolation of computer systems, what is now called an "air gap." This is no longer a viable option. As more and more human activities move into cyberspace to take advantage of the efficiencies provided by interconnection, organizations and individuals who fail or refuse to connect will increasingly fall behind the pace of economic and social activity, will become increasingly noncompetitive in their area of activity, and will have difficulty accomplishing their missions. This idea is stated succinctly in a report of the Joint Security Commission appointed by the U.S. Secretary of Defense and the Director of Central Intelligence to develop a new approach to security to meet the challenges facing the Department of Defense and the Intelligence Community in the post–Cold War era [13]:

> Those who steadfastly resist connectivity will be perceived as unresponsive and will ultimately be considered as offering little value to their customers. . . . The defense and intelligence communities share this imperative to connect.

Roles and Missions Blurred

By their nature, developments in cyberspace blur the distinction between crime and warfare, thereby also blurring the distinction between police responsibilities to protect U.S. interests from criminal acts in cyberspace, and military responsibilities to protect U.S. interests from acts of war in cyberspace.

In addition, providing protection against transnational threats in cyberspace, and apprehending their perpetrators, frequently goes well beyond the reach and resources of local and regional authorities.

These two characteristics of security in cyberspace—the blurring of the distinction between crime and warfare, and the transnational nature of many security incidents—raise new questions regarding the proper roles and missions in cyberspace security and safety. Some of the agencies, organizations, and institutions that have essential roles to play, from the viewpoint of one living in the U.S., include:

- *U.S. federal government*, including intelligence agencies, the Department of Defense, federal law enforcement agencies; civilian regulatory agencies; and other civilian agencies;
- *U.S. State and local governments*, including law enforcement agencies and regulatory agencies;
- *Nongovernmental organizations* such as CERTs, business and professional associations, vendors, industry standard-setting bodies, and private businesses;
- *Governments of other nations, i*ncluding intelligence agencies, ministries of defense, and law enforcement agencies;
- *International organizations* such as the United Nations, supranational governing bodies, Interpol, and international standards bodies.

Today this is "everybody's" problem, and therefore "nobody's" problem. It falls into all of the cracks.

USEFUL METAPHORS

These various characteristics of the current security situation in cyberspace suggest three metaphors which may stimulate thinking about protective strategies.

"Wild West" World

Cyberspace has many similarities to a Wild West world.

- In the Wild West almost anything could occur. There was no one to enforce overall law and order, only isolated packets of local law. The same is true in cyberspace.
- There were both "good guys" and "outlaws" in the Wild West, often very difficult to tell apart. "Friends" were the only ones a person could trust, even though he or she would frequently have to deal with "strangers." This is also true in cyberspace.
- Outside of the occasional local enclaves of law and order, everyone in the Wild West was primarily dependent for security on their own resources and those of their trusted friends. This is also true in cyberspace.

The message of this metaphor for cyberspace security is clear: If there is no way to enforce law and order throughout all of cyberspace, which appears to be the case, one must rely on local enclaves of law and order, and trusted friends.

Medieval World

The medieval world depended on local enclaves for security: castles and fortified cities, protected by a variety of fortifications—moats, walls, and drawbridges. Communication and commerce between these fortified enclaves was carried out and/or protected by groups of armored individuals.

This metaphor also suggests a message for cyberspace security: cyberspace fortifications (i.e., firewalls) can protect the local enclaves in cyberspace, just as moats and walls protected the castles in the medieval world.

We have found the security concepts suggested by these two metaphors—local enclaves and firewalls—to be very compelling, and usable as part of a basic paradigm for cyberspace security.

Biological Immune System

The problems faced by biological immune systems have a number of similarities to the challenges confronting cyberspace security. This suggests that the "security" solutions employed by immune systems could serve as another useful model for cyberspace security. For example:

- Higher-level biological organisms are comprised of a large number of diverse, complex, highly interdependent components. So is cyberspace.
- Biological organisms face diverse dangers (from microbes) that cannot always be described in detail before an individual attack occurs, and which evolve over time. Organisms cannot defend against these dangers by "disconnecting" from their environment. The same is true of information systems exposed to threats in cyberspace.
- Biological organisms employ a variety of complementary defense mechanisms, including both barrier defense strategies involving the skin and cell membranes, and active defense strategies that sense the presence of outsiders (i.e., antigens) and respond with circulating killers (i.e., antibodies). The cyberspace firewalls are an obvious analogue to the biological barrier defenses. But what about the active defenses? Perhaps software agents could be created providing a cyberspace active defense analogue to biological antibodies.

The biological agents providing the active defense portion of the immune system employ certain critical capabilities: the ability to distinguish "self" from "nonself"; the ability to create and transmit

recognition templates and killer mechanisms throughout the organism; and the ability to evolve defenses as the "threat" changes.

Software agents providing a cyberspace active defense analogue to these biological antibodies would need the same capabilities.[4]

The message of this metaphor is clear: Cyberspace security would be enhanced by active defenses capable of evolving over time.

We find this third metaphor as compelling as the first two; however, we are not as far along in exploiting it in our analysis.

SECURITY STRATEGY

These enclaves can be of various sizes, some of them can be nested, and the firewalls can be of various permeabilities. The enclaves have protected connections to other trusted enclaves, and limited connections to the rest of cyberspace.

In this architectural concept, no attempt is made to maintain centralized law and order throughout all of cyberspace. Each authority maintains local law and order in its own enclave. Everything outside of the enclaves is left to the "wild west."

These enclaves can come in a variety of sizes, ranging from an individual computer to a complete network. The firewalls protecting these various size enclaves come in several different types, with different degrees of permeability.[5]

In the most extreme case, one can have an air gap, i.e., the absence of any electronic connection between the interior of the enclave and the outside world. Within this overall category, there can be various degrees of permeability, depending upon what software and/or data are allowed in and out, on diskettes, tapes, etc., and how rigorously this software and data are checked.

When electronic connections are allowed, a firewall computer stands between the world outside the enclave and the internal machines. Two main categories of variations are possible:

1) Different services can be allowed to come in or to go out, depending on the permeability desired of the firewall. Typical ser-

vice categories include electronic mail, file transfer (e.g., FTP), information servers (e.g., World Wide Web browsers), and remote execution (e.g., Telnet). Of these four categories, electronic mail is the safest to interchange with the outside world and remote execution is the most dangerous—in the sense of providing opportunities that hackers can exploit to penetrate the firewall barrier and gain control of internal machines. Accordingly, even the tightest firewalls usually allow the passage of electronic mail in both directions, whereas only the loosest firewalls allow the passage of remote execution services, particularly in the inward direction.

2) Some allowed services can terminate (or originate) at the firewall machine, while others can go right through the firewall to the internal machines (incoming services) or to the outside world (outgoing services). The fewer services that pass through the firewall, the tighter it is.

These variations in the permeability of electronic firewalls can be tuned to the circumstances of the particular enclave.

Protective Techniques and Procedures

In addition to firewalls, there are a number of other protective techniques and procedures which have important roles to play in our strawman protective strategy. These include:

- Improved access controls, including one-time passwords, smart cards, and shadow passwords.
- More secure software. This could include expanded use of software independent verification and validation (IV&V) techniques, to find and eliminate software bugs and security holes in widely used software, as well as more secure operating systems.
- Encrypted communications, both between and within protected enclaves.
- Encrypted files, for data that is particularly sensitive.
- Improved capabilities to detect penetrations, including user and file-access profiling.

- Active counteractions, to harass and suppress bad actors. This is something that is woefully lacking today; almost all current computer security measures are either passive or counteractive, leaving the initiative to the perpetrator.
- Software agents, perhaps acting in a manner similar to a biological immune system.

Motivating Users

The best protective strategy in the world and the best set of protective techniques and procedures will be ineffective if users do not employ them. Necessary (and hopefully sufficient) ways to motivate users include:

1) A vigorous program of education and training, of both users and managers concerned with information systems in potential target organizations—education, so that people will understand the magnitude of the risk to their interests and the importance of cyberspace security, and training, so that people will know how to protect themselves.
2) Proactive programs to demonstrate vulnerabilities—sometimes called "red teams"—and thereby to increase organizational and individual awareness of cyberspace vulnerabilities. The Vulnerability Analysis and Assistance Program (VAAP) of the U.S. Center for Information Systems Security (CISS) is a good example of such a proactive program [20].
3) Mandates, tailored to different societal elements. These can include mandatory security procedures established by an organization for all of its employees or members to follow, mandatory security standards that a computer host must meet in order to be permitted to connect to a network, security standards and procedures that organizations and individuals must adhere to in order not to incur legal liability, and even possibly laws mandating certain minimum levels of security standards for information systems engaged in certain types of public activity.
4) Sanctions, to enforce the mandates.

Complete Protective Strategy

In addition to the elements we have discussed thus far, a complete cyberspace protective strategy needs at least two additional elements.

1) A set of prescriptions governing the application of the basic security paradigm and the set of protective techniques and procedures to different security situations: for protecting different elements of society; for countering different actors; and for determining what role various agencies and organizations should play in cyberspace security, in which situations. These prescriptions—in particular those associated with the assignment of roles and missions in cyberspace security—may well differ from nation to nation.
2) A built-in mechanism or mechanisms to continually update the protective techniques and procedures, and the overall strategy, as information technology continues to evolve and its applications to expand, and as new threats emerge.

These elements remain to be developed.

OPEN QUESTIONS, KEY ISSUES

A number of open questions and key issues should be resolved in process of proceeding further. These include:

- *What specific organizations and activities comprise what we will call the "National Interest Element" in the U.S. or any other nation?* That is, what organizations, information systems, and activities play such vital roles in society that their disruption due to cyberspace attacks would have national consequences, and their protection should therefore be of national concern?
- *Which organizations (in each nation) should play what roles in the protection of the National Interest Element?*
- *How robust or fragile are essential infrastructures contained in the National Interest Element of each nation?* This is one of the key uncertainties in our current understanding of the cyberspace se-

curity situation. A detailed look at the vulnerabilities of specific infrastructures in various nations is needed to resolve this issue.

- *How does one protect against the trusted insider?* Our basic security paradigm of local enclaves protected by firewalls protects against malicious outsiders, but not necessarily against malicious insiders, individuals inside the firewall with all of the access privileges of a trusted member of the enclave. As knowledge of hacker techniques spreads throughout the population, adverse actions by malicious insiders is becoming more and more of a problem. We have not discussed this here, but it is an important threat with which any complete cyberspace security strategy should deal. It becomes particularly important for very large protected enclaves, encompassing large numbers of individuals; the more people within an enclave, the greater the probability that at least one of them might be a bad actor.

INCREASINGLY COMPLEX WORLD, EXPANDING SECURITY CONCERNS

A number of points are worth emphasizing:

Fifty years after ENIAC, the network has become the computer (paraphrasing the Sun Microsystems slogan "The Network Is the Computer").

In the future, cyberspace security and safety incidents in this networked environment will become much more prevalent; cyberspace security and safety incidents will impact almost every corner of society; and the consequences of cyberspace security and safety incidents could become much greater.

Local enclaves protected by firewalls appear promising as a basic cyberspace security paradigm, applicable to a wide range of security situations.

We're all in this together; weak links in the net created by any of us (software developers, end users, network providers, etc.) increase the problem for all of us.

Much more attention must be paid to user motivation, for all classes of users, with different approaches required for each class. Inade-

quate user acceptance and utilization of security techniques and procedures has been the bane of most previous attempts at cyberspace security.

No one's in charge; the problem transcends all usual categories. The question of "roles and missions" is an important one, both philosophically (e.g., do we need more centralized control, or are there decentralized effective solutions) and pragmatically (what roles do we give DoD versus FBI versus CIA; UN versus U.S.; Interpol versus whom?).

The world has become much more complex. It is useful complexity, but with this complexity has come security and safety problems that we are only beginning to understand and appreciate.

REFERENCES

1. P. Neumann, *Computer Related Risks.* Reading, MA: Addison-Wesley, 1994.

2. P.J. Denning, *Computers Under Attack: Intruders, Worms, and Viruses.* Reading, MA: Addison-Wesley, 1990.

3. K. Hafner and J. Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* New York, NY: Simon & Schuster, 1991.

4. P. Mungo and B. Clough, *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals,* New York, NY: Random House, 1992.

5. P. Wallach. "Wire pirates," *Sci. Amer.,* vol. 270, pp. 90–101, Mar. 1994.

6. Presentation by Air Force Computer Emergency Response Team (AFCERT), Kelly AFB, at Sixth Ann. Computer Security Incident Handling Wkshp., hosted by the Forum of Incident Response and Security Teams (FIRST), Boston, MA. July 25–29, 1994.

7. R.E. Yates, "Hackers stole phone card numbers in $50 million scam," *Chicago Trib.*, pp. 1,6. Nov. 2, 1994.

8. Data Presented by Computer Emergency Response Team (CERT), Carnegie Mellon University, at Sixth Ann. Computer Security Incident Handling Wkshp., hosted by the Forum of Incident Response and Security Teams (FIRST). Boston, MA. July 25–29, 1994—supplemented by CERT 1994 Ann. Rep. web homepage (http://www.sei.cmu.edu/SEI/ programs/cert/1994_CERT_Summary.html).

9. S. Levy, *Hackers, Heroes of the Computer Revolution,* Anchor, 1984.

10. D.G. Johnson, *Computer Ethics,* 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1994.

11. B. Hoffman, "Responding to terrorism across the technological spectrum," RAND, Rep. P-7874, 1994.

12. *DOD Trusted Computer System Evaluation Criteria (TCSEC),* DoD 5200.28-STD. Washington, DC: U.S. Government Printing Office, Dec. 1985.

13. "Redefining security," report by the Joint Security Commission, Washington, DC 20525, Feb. 28, 1994.

14. S. Forrest, A.S. Perelson, L. Allen and R. Cherukuri, "Self-nonself discrimination in a computer," in *Proc. 1994 IEEE Symp. Res. in Security and Privacy,* 1994.

15. J.O. Kephart, "A biologically inspired immune system for computers," in *Artificial Life IV, Proc. Fourth Int. Wkshp Systhesis and Simulation of Living Systems,* R.A. Brooks and P. Maes, Eds. Cambridge, MA: M.I.T. Press, 1994, pp. 130–139.

16. W.R. Cheswick and S.M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker.* Reading, MA: Addison-Wesley, 1994.

17. S. Garfinkel and G. Spafford. *Practical UNIX Security,* Sebastopol, CA: O'Reilly & Associates, 1991.

18. *Proc. 17th Nat. Computer Security Conf.,* vols. 1 and 2, National Inst. of Standards and Technology/National Computer Security Center, Oct. 11–14, 1994.

19. M.R. Higgins, "Threats to DoD unclassified systems," DoD Center for Information Systems Incident Support Team (ASSIST), 1994.

20. R.L. Ayers, "Center for Information Systems Security, Functions and Services," Center for Information Systems Security, Defense Information Systems Agency, 1994.

NOTES

[1]As one consequence of the electronic digitization of information and the worldwide internetting of computer systems, more and more activities throughout the world are mediated and controlled by information systems. The global world of internetted computers and communications systems in which these activities are being carried out has come to be called "cyberspace," a term originated by William Gibson in his novel *Neuromancer*.

[2]In addressing questions of cyberspace security and safety, we have relied on a variety of anecdotal information obtained from a number of sources. The anecdotal data by no means constitute a comprehensive statistically valid sample. In principle, one could develop such a sample from databases from the various computer emergency response teams (CERTs), law enforcement databases, and private sector incident data. However, we have yet to find anyone who has done so.

There are a number of reasons for this. One is that many if not most cyberspace security incidents apparently go unreported to authorities, particularly in the financial community. It is therefore unclear if the incidents that are reported are "the tip of the iceberg," or all there is to the problem.

Lacking a comprehensive sample, the total quantitative dimensions of the cyberspace security problem are unclear. Therefore, we present here our qualitative impressions of the problem.

[3]The "Orange Book" is a common term for the DOD Trusted Computer System Evaluation Criteria (TCSEC) [12].

[4]We are not the first to be intrigued by this metaphor. Forrest *et al*. [14] and Kephart [15] discuss software implementations of certain aspects of the biological immune system metaphor.

[5]We are certainly not the first to suggest firewalls as a protective technique or as a central element of a protective strategy. See [16]–[18].