# The Cyber Battlefield -

# Is This The Setting for the

# Ultimate World War?

# IEEE International Symposium on Technology and Society 1997

Sam Nitzberg, Information Security Engineer

Telos Information Protection Services

Telos Corporation

656 Shrewsbury Avenue

Shrewsbury, NJ 07702 USA

Abstract-It is clear that all of the elements normally associated with conventional war exist on the cyber battlefield; these elements just have different names. Additionally, the motivations for war are different in the cyber environment. The focus is not one of territorial acquisition, but one of information piracy and information system vandalism. The one exception to this notion is that there are no equivalents to the Conventional Forces Europe Treaty of the United Nations, nor is there international computer crime legislation to reconcile international cyber incidents. Couple this with the fact that, because our networked society is relatively new and evolving, many do not understand information security issues and are not able (or do not understand the need) to protect information and information systems. This creates an opportunity for cyber guerrillas to wreak havoc. What is worse is that even if you can determine who committed the act (not an easy task), there is no recognized mechanism or process for legal retribution.

## I. Introduction

On the cyber battlefield...

*replace snipers with hackers,*

*replace bullets with data packets,*

*replace chemical warfare with computer viruses,*

*replace anti aircraft guns with firewalls,*

*replace sentries with intrusion detection systems,*

*replace military intelligence with auditing tools,*

*replace physical battlefields with cyber equivalents that potentially extend conflicts to every point on the planet, and*

*replace international treaties, policies, and organizations with NOTHING*

This scenario is not far fetched and depicts a war unlike any we have fought in the past. At risk is a wide range of information and information systems that, if tampered with, potentially impact our standard of living and national security.

A recently reported incident concerns a group of Dutch hackers who were able to gain valuable intelligence relating to the Coalition Forces' waging of the Persian Gulf War and offered it to the Iraqi government for a price[1]. Iraq was not interested in the material so offered. As described, the information was too valuable, and was considered to have been a ruse. As the global information age has begun, so has the age of global information warfare. What matters above all else in today's military, and today's financial world, is information. And today, the methods available to covertly obtain information from either the military/government or commercial sectors is virtually indistinguishable.

Critical information that affects our national security is not strictly limited to military information, but includes valuable efforts and resources such as high tech research and development data. Additionally, with the rapid advancement of computer networking, there is a network continuum evolving that connects networks of all types- computer networks, telephone networks, air traffic control systems, and power grids. It is clear that with this network continuum, the potential to cause harm is great.

We need to recognize that a war is brewing, a high-tech war for information. Technology has caused the implements of war and the battle environment to change, but the concepts are the same and the threats are just as real. Part of managing the peace offensive is addressing the issue of information warfare. The global nature of the issue, made possible by the Internet, creates the potential for this to be a worldwide conflict. Is this the setting for the ultimate world war?

There are a number of definitions of information warfare floating about, and one may select the one that most closely reflects a given situation. What is of importance is that computers are essential to accomplishing organizational functions and imperatives, and that without an appropriately disciplined approach to their defense at all levels, these computers will be at the mercy of any wishing to cause harm, and not at the proper command of their masters.

One popular categorization divides Information Warfare into three categories[2]:

- Personal Information Warfare
- Corporate Information Warfare
- Global Information Warfare

In this vision of the battlespace, the victims are either individuals, corporate entities, or governments, respectively.

Another method of viewing Information Warfare is to consider the threats from two vantage points by identifying the internal and external threats to valuable computing assets. Internal threats are those originating from personnel working for the organizations hosting the (hopefully) secured systems. External threats originate from individuals or organizations without a legitimate interest in the internal operations of the organizations or computing systems in question. These internal and external threats are present whether yours is a banking concern, a major corporation, or a military or governmental organization. We would maintain that either the targets or aggressors in the cyberspace battlespace may be either private or governmental concerns. In the battles which ensue, we are all targets.

A properly equipped and determined individual or corporation may very well use methods similar to those at the disposal of governments. By dividing the security problem into internal and external elements early in a security analysis, security projects may be divided into manageable, logically cohesive chunks.

There are many issues that must be addressed to bring this escalating potential for cyber conflict under control. Some of the significant issues that need to be addressed include the:

ï Development of information system security policies, required to govern how information systems may be legitimately operated

ï Implementation of information security measures, needed to implement the security polices

ï Institution of computer crime laws, necessary to define socially acceptable computer behavior

ï Institution of international computer crime cooperation--demanded to pursue cyber vandals across international boundaries

Each of these important issues are discussed in additional detail in the course of this paper.

## II. THE CYBER BATTLEFIELD

The cyber battlefield includes all systems on the Internet, corporate and governmental intranets, systems used in electronic commerce, and systems used to provide services to society as a whole. Efforts may be waged to target and compromise any of these systems in order for an in individual or group to attain notoriety, seek financial gain, or to obtain services through their theft.

The cyber battlefield is also the place where the defensive and offensive actions occur which compromise computing environments, data (in both electronic and print form), and transmission/reception facilities and mechanisms. Points of attack and defense include all individual systems, servers, firewalls, anti-virus, access control applications, databases, and hardware essential to proper systems operations. Less glamorous, but just as real, are the mundane spaces in this battleground. These spaces include yellow sticky notes carrying passwords, sloppily maintained desks covered with sensitive materials, office trash containing sensitive documents, and any other material which may be readily accessible to people who could then use it to jeopardize computing systems and data.

If one reviews the current literature on the exploits of hackers, it is easy to get an uneven view of the source of current threats. Most books and tales of hacker prowess are related to stories and events which often date back to the 1980's. These stories often focus on individuals or groups of individuals (often adolescents), who would replicate copy protected software and make free phone calls. On occasion, they might even be capable of directly controlling various aspects of the telephone system's switching apparatus. A valuable frame of reference to describe some more recent hacker activity follows in Table 1:

Table I

Breaking and Entering[3]

| | |
|---|---|
| **GOVERNMENT:** | |
| Estimated number of hacker attacks on DOD 1995:<br>in 1996: | 250,000<br>500,000 |
| Estimated percentage that are successful: | 65% |
| Estimated percentage detected by the DOD: | Less than 1 |
| **RESEARCH:** | |
| Average number of potentially damaging hacker attempts on Bell Labs networks in 1992, per week | 6 per week |
| Average number of less threatening attacks, per week | 40 |
| Average rate of attacks in 1996 | No longer tracked. |
| **COMMERCE:** | |
| Percentage of banks in recent survey that report plans to offer Internet banking services in 1997: | 36% |
| Percentage of existing bank web sites found to have potentially significant security holes: | 68% |
| Percentage of Web sites selected at random with such holes: | 33% |

Today's hackers and commercial high-technology espionage agents have some very sophisticated tools to work with which include portscanners to identify services which are supported by a target system, password cracking tools to assist in obtaining users' passwords, and network scanners to remotely identify vulnerabilities in a host of well-known operating systems. Examples of tools in each of these classes are freely available on the internet. Ironically, these tools may also be used to improve the security of an organization's computing systems. With the proliferation of these tools and internationally and freely accessible hacker computing sites, it is safe to assume that any vulnerability on any system on the web could be exploited at will.

Risks posed to any organization with an investment in computer resources include the outright theft of their intellectual material including product and strategic plans, pricing data, internal reports, database contents, and proprietary source and executable code (programs). In addition to the outright theft of valuable corporate data, organizations face attacks which could cripple their information infrastructure, or prevent them from offering their automated services. Organizations also face the immediate risk of being the victims of vandalism or misinformation campaigns waged from their own sanctioned systems. An example of this is provided by the home pages of the United States Department of Justice and the United States Central Intelligence Agency. Their home pages were modified by hackers: the resulting Department of Justice home page sported a flag with a swastika, while the CIA's home page had, among other modifications, a link to images of "naked women" [4]. The effects of hackers or activists modifying a company's web pages to give the false appearance of the company's admitting guilt to dirty deeds, or otherwise manipulating data to be distributed to the public via their systems, could have profound negative consequences for the organization. In November 1996, Kriegsman Furs & Outerwear was the victim of precisely such an attack. Their commercial web page was changed into a scathing animal-rights home page, which included a request for viewers of the newly modified home page to harass Kriegsman Furs. A collection of before and after images of hacked home pages appears on the home page of the Hacker Quarterly, 2600 magazine's home page[5].

The nature and design of the world wide web brings risk with its rewards. While the web is global, and bandwidth may seem cheap, there are some serious consequences for industry to understand. Without proper security measures in place, data traffic between your systems and any user may be monitored by virtually anyone on the Internet. Certainly, any system connected to the Internet is subject to attempted attacks from any system virtually anywhere in the world. An analogy referring to software pirates replicating and distributing software after breaking the protection schemes applies, "Imagine an army of robbers, all attacking the same bank at the same time. And in the comfort of their own homes[6]." The present degree of global network connectivity renders this citation most apt.

One very humbling fact in addressing security problems is that none of the exotic measures at one's disposal will be effective if the fundamentals are overlooked or disregarded. Examples of lost corporate secrets from hackers, business competitors, and national agents obtaining corporate secrets by stealing "trash" left outside for pick-up abound. In one famous case, an individual working for Intel was unable to download data he wished to peddle on his own via the telecommunications link he used for work. His solution to this obstacle was to record all the desired data on videotape. By the time he was apprehended, the individual had passed the data, which had an estimated value of between $10 million to $20 million American dollars to Iran, North Korea, Cuba, and a competitor [7].

According to the GAO (United States General Accounting Office) Report on Pentagon Computer Security,

"... The Department of Energy and NSA [United States National Security Agency] estimate that more than 120 countries have established computer attack capabilities. In addition, most countries are believed to be planning some degree of information warfare as part of their overall security strategy.

At the request of the Office of the Secretary of Defense for Command, Control, Communications and Intelligence, the Rand Corporation conducted exercises known as 'The Day After . . . ' between January and June 1995 to simulate an information warfare attack. Senior members of the national security community and representatives from national security-related telecommunications and information systems industries participated in evaluating and responding to a hypothetical conflict between an adversary and the United States and its allies in the year 2000.

In the scenario, an adversary attacks computer systems throughout the Unites States and allied countries, causing accidents, crashing systems, blocking communications, and inciting panic. For example, in the scenario, automatic tellers at two of Georgia's largest banks are attacked. The attacks create confusion and panic when the automatic tellers wrongfully add and debit thousands of dollars from customers' accounts. A freight train is misrouted when a logic bomb is inserted into a railroad computer system, causing a major accident involving a high speed passenger train in Maryland. Meanwhile, telephone service is sabotaged in Washington, a major airplane crash is caused in Great Britain; and Cairo, Egypt loses all power service. An all-out attack is launched on computers at most military installations, slowing down, disconnecting, or crashing the systems. Weapons systems designed to pinpoint enemy tanks and troop formations begin to malfunction due to electronic infections.

The exercises were designed to assess the plausibility of information warfare scenarios and help define key issues to be addressed in this area. The exercises highlighted some defining features of information warfare, including the fact that attack mechanisms and techniques can be acquired with relatively modest investment. The exercises also revealed that no adequate tactical warning system exists for distinguishing between information warfare attacks and accidents. Perhaps most importantly, the study demonstrated that because the U.S. economy, society, and military rely increasingly on a high performance networked information infrastructure, this infrastructure presents a set of attractive strategic targets for opponents who possess information warfare capabilities. [8]"

An information warfare attack on a nation includes an attack on its computing corporate infrastructure. There will continue to be great interest by various governments in how to undermine the computing security of not only other governments, but of corporate and corporate run systems. This potential menace may not be seen in a full-scale assault between nations, but may also be used in limited warfare. This significantly raises the stakes in the "Hacker War."

The misconception that Information Warfare is merely computer security with additional monetary funding must be put to rest. Information Warfare is, however, computer security implemented (waged) and conducted with the knowledge that the cyber environments which exist today are very dangerous, are becoming even more so, and that the only way to effectively mitigate the implicit risks and to reap the rewards is to maintain a thorough, comprehensive computer and information security plan to address all security-related aspects of what you wish to be your secure computing environment. This environment must be regularly monitored, tested, and reviewed for any newly emerging vulnerabilities.

## III. Information security policies

A security policy is a high-level management document which officially mandates measures designed to safeguard corporate systems, data, plans, and services offered through its computing systems and environments. Security policies serve to protect the organization's valuable information from disclosure, unauthorized modification, and "denial of service attacks," where corporate systems are effectively taken off-line by a provocateur. These policies define acceptable information handling behavior, and define the mechanisms to be used towards defending the information from the assaults it may come under. Internally based threats must also be specifically addressed, and must include the judicious use of employee training to recognize what information is valuable to the organization, how to securely dispose of that information when the time comes, and to identify new threats as they arise.

Information Security Policies must not be developed in a vacuum, as they require significant input from information security engineers familiar with the practical aspects of the effectiveness of current security measures, and who will understand the architecture of the computer systems and their associated data and services. If security engineers are left "out of the loop," it is very possible that policies will be mandated which are not realizable on the given computing base, or that will so stifle productivity, that these edicts will be ignored.

Attention will be required from the corporation's legal department to assure that the rights of employees and customers are maintained under current law, especially with regard to privacy issues that are sure to arise - especially regarding the use and protection of both electronic mail and computerized personnel files. A not insignificant role of the security policy document is to mitigate corporate civil liability. By mandating that due care be utilized in electronic data processing and the providing of services, should any improper disclosures of personal information occur, the corporation has defenses against claims which may be lodged.

One paramount and difficult issue is that of employee privacy rights. The origin of this difficulty is that the law may be inconsistent or even contradictory within a single country. Examples of this sort of problem stem from court decisions likening computing systems and records to bulletin boards, telephone conversations, or other, more dated modes of communication [9]. For these issues to be resolved in a unified and meaningful fashion, the judiciary must consider computerized records in their own context. In the meantime, any issues which have not been specifically addressed by the courts must be considered as open issues, and their ultimate resolution as unpredictable.

The various service providers, employers included, must be assured of their rights. Businesses must be capable of accessing their own computer records and analyzing their own systems to ensure proper operation. The laws for electronic mail are not clear or unified, and are largely being decided following lawsuits. Companies need to access their own records, and yet, electronic mail (even in the corporate environment) is often considered to consist of personal speech. There is no sign that a unified body of law will emerge on this issue.

Of paramount importance to service providers is their fundamental right to exist. A service, an anonymous remailer, was being operated in Finland to allow individuals to anonymously communicate with each other about personal matters through the internet. In this case, the Church of Scientology wanted the identity of one of the individuals who had used the remailer service. Rather than comply with the Finnish judge's ruling that electronic mail does not enjoy the same protection as postal mail or telephone calls, the operator of this anonymous remailer decided to take it off-line [10]. After attempting to restrict incoming electronic "junk-mail," an internet service provider in New York, Panix (Public Access Networks Corporation), fell under an internet-launched attack, which rendered Panix unable to provide its internet services. The attack involved the use of difficult-to-trace packets which were fired at Panix with fraudulent return addresses. Had the attack continued, Panix would have been unable to resume its business operations. Instructions on how to launch such attacks have been published in both 2600 and Phrack, two publications widely read by hackers.

Executive management will have to understand the impact of the security policy on how operations are conducted and on the resources which they will consume. Executive management will further have to ensure that the policies have teeth, that there will be consequences if their organizations or individuals expose the organization to risk by not following policies.

Once an organization has considered the risks it is exposed to and has developed its formal policies, work can begin in earnest towards implementing the solutions to the identified security problems. Without a formal security policy, there will be no broad decree indicating management's intentions and determination. Above all, the policy document identifies issues to be resolved and is used to implement the defined information security policies; for without this, any groups could perform virtually any functions (or virtually no functions) in the name of security, and claim to be fulfilling the corporate security imperatives. Most often, however, if actual goals and responsibilities and deadlines are not established, no advances are made.

Implementing the necessary security measures will not be a simple matter of purchasing software to close any present security holes. A combination of technology, manual procedures, training, and awareness programs must be used in concert to achieve the appropriate defensive security posture. The Telos Information Protection Services Model (see Fig. 1) may be used to address these issues and identifies work to be accomplished in each of its steps. There will be a need for ongoing, regular practices to address training of employees in standard methods for defining day-to-day operations, including proper and acceptable user behavior on corporate computers, defending against social engineering attacks, and ways of reporting any suspicious activity. These training sessions must be used together with the prescribed technological measures to attain an appropriate level of security.

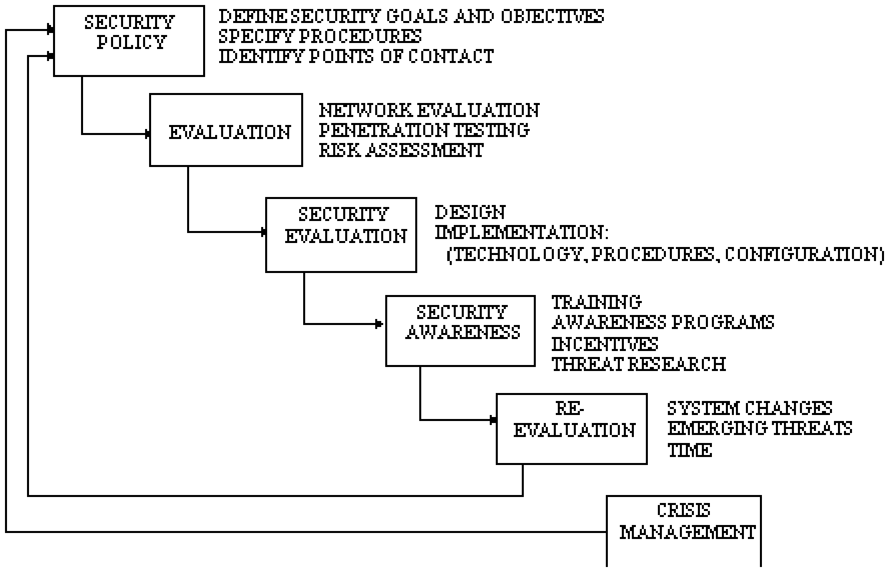

Fig. 1 TIPS INFOSEC MODEL

Due to matters related to employee turnover, as well as "technological turnover," prompting the inevitable closure of old security holes, and the introduction of new ones which will emerge with technological advances, both the employee training and the technological security studies must be performed at regular intervals as a part of standard corporate operations. To maintain a secure environment, all active security measures taken will have to be implemented as part of a continuous process towards the practice of enforcing the security policies.

A balance must be struck between the cost to safeguard corporate computing assets, the actual threats they are under, and the value they represent to the corporation It is possible to spend very large sums of money on security assessments and measures, and it is critical to ensure that this money is spent in a cost-effective manner.

It is very tempting for most organizations to conduct their own security audits and implement their own security solutions. Unless your organization has an enclave with significant expertise in computing security and espionage (corporate or international), a professional, dedicated group should be called in to conduct the security audit and assist in establishing its follow-through. All too often, organizations rely on their own administrators to ensure secure operations of their systems. The consequence of this is that these administrators tend to overlook the original errors in systems practices, architecture, and configurations, which created the original security vulnerabilities to begin with.

If your organization will be performing its own security countermeasures and solutions, they should be evaluated by an outside organization with the expertise described above. The single most important factor will be timeliness in your security engineering effort. If you wait until your company has suffered losses and incurred potential legal liability due to an information warfare plot waged against it, it will be too late to put the data back where it belongs, or to restore your services and protect your professional image.

## IV. COMPUTER CRIME LAWS,

## INTERNATIONAL POLICIES,

## AND COOPERATION

Presently, there is a great void in both legislation and enforcement relating to information warfare incidents. Historically, in most countries, while the law may be capable of handling routine criminal and civil matters, it has been unable to anticipate or react quickly to the emerging issues in computer and information warfare. Who has ever heard of an individual facing either criminal or civil penalties for unleashing a computer virus?

Glaring shortcomings exist in nations' laws regarding the very notion of what constitutes a computer crime. These differences range from the illegality of the production of computer viruses, to their dissemination, whether or not it is intentional, to using international communications lines to breach the security of computer systems.

Another interesting issue demonstrating the lag in the law involves the remote accessing of computing systems. Some laws interpret a welcome message without a warning as just that - a welcome for anyone and everyone to login to the given system. Generally, it is illegal to login to a system with specific warnings prohibiting unauthorized use. It is not illegal, however, to use software tools to generate large numbers of automated requests to remote computing systems to determine and record their vulnerabilities.

Even where an effort is made to form laws to address information security issues, the results can appear schizophrenic. One example of such law involves the American International Traffic in Arms Regulations (ITAR), which, while upholding the notion of information as both a weapon and an asset, has restricted the flow of security technology, while leaving huge gray areas in the law. The ITAR and associated legal decisions have created an environment where a large number of actions are neither clearly legal or illegal, and has generated legal decisions, some of which either may make sense or not, without clear distinction. Laws which draw the line between exportable and non-exportable software depending on whether the software is in print or electronic form reveal a fundamental failure of the lawmakers to understand the underlying technical issues. Similar problems are present in determining who may or may not be taught cryptography in American universities. Even the U.S. state department seems to have difficulty in distinguishing between the legal and illegal dissemination of cryptologic information under these provisions. [11]

One potentially tragic example of the kind of mismatch between developing computer law and technological reality seems to be emerging in United States Law. The Decency Act, intended to protect the young from indecency on the Internet, was found to be unconstitutional based on its loose notion of decency. In a global communications environment, internationally accepted laws must be adopted. Otherwise, any nation may effectively attempt to impose its law on the world at large. If another, perhaps more conservative, nation would impose a similar law, and attempt to enforce it, any corporation and its representatives in any country could be held liable for any infraction. Such an infraction might involve a woman in an advertisement shown without her hair being covered. Perhaps the sentence for this crime would be death or prolonged imprisonment for representatives of the advertising agency or internet service providers. At the very least, these representatives would be exposed to prolonged harassment through civil and criminal proceedings.

If restrictions were in place regarding the nature of business information permitted to flow into and out of countries, any corporation supplying such information (such as stock valuations), could potentially be required to keep track of the laws in dozens (or hundreds) of countries. To make matters worse, the laws of different countries could be in direct conflict with each other, such that there would be no manner in which legitimate trade or security of transactions could be legally ensured.

The only way to effectively organize any proper mode of conduct or body of laws for the internet must be done on a sweeping, international basis. There are too many ways for information to flow into and out of countries through the networks in place to even pretend to be able to control information on an ad-hoc or case-by-case basis. Any jurisdictional issues are, at best, hopelessly confused and unresolved.

What makes this international cooperation so crucial is that the Internet and Web effectively make any corporation an international corporation. These corporations must be able to securely establish communications amongst themselves, and immediately address any breaches regardless of their sources. In an example of decency in law, a similar, but perhaps more pertinent example would be that of a law restricting the information flow into and out of given countries.

Mechanisms must be established by which any organization may securely perform their business functions and initiate investigations of suspected intrusions upon their systems by way of the internet, telephonic networks, or satellite-based communications systems. The traditional philosophy has been that it is easier for terrorists to blow something up than to use computers. With the increasing availability of easy-to-use hacking tools, detailed description of system exploitations, and ease of contact with systems through present-day global networks, this is no longer accurate.

## V. SUMMARY

Conventional laws may be of some value in traditional cases of employees walking out with intelligence information. In this age of information and information warfare, governments have fallen behind in their roles to provide safe passage of information from the highwaymen of the Internet and Web. Here, governments have been abandoning their opportunities for leadership and effectiveness in creating a safe environment for business to be conducted. As governments are called upon more and more to defend enterprise, they will increase their capabilities to do so. Presently, their information warfare capabilities have remained more offensive than defensive in nature.

Part of the peacekeeping effort is to actively manage the security of information and information systems. First and foremost in this effort, organizations must form their own information intelligence groups. These will study the computing systems, both planned and in-place, identify the salient security issues, and take formal steps to resolve them. Then, measures will be taken and updated to maintain the security infrastructure of the organization. To build on this, corporations with like-minded infrastructures can exchange information within coalitions or bodies to disseminate information towards assisting in preserving the integrity of their secure infrastructures.

By actively implementing measures to address both internal and external security threats, the majority of information warfare incidents can be mitigated. The conventional wisdom is that most hackers and perpetrators will move on to easier targets if they are unable to defeat the security features of the one most closely at hand. Make your information infrastructure secure and give them that incentive to go poking around elsewhere!

## VI. References

[1] Associated Press (London), "Experts: Hackers Stole War Data," March 24, 10:18 PM EST.

[2] W. Schwartau, *Information Warfare: Chaos on the Electronic Superhighway.*, First Trade paperback edition, Thunder's Mouth Press, 1995, pp. 17-19.

[3] W. Wayt Gibbs, "Profile:Dan Farmer From Satan to Zen," *Scientific American*, April 1997 pp. 32-34.

[4] No author, "Hacked Pages," *2600*, Autumn 1996, pp. 54-55.

[5] http://www.2600.com/hacked_pages/

[6] David McCandless, "Warez Wars," *Wired*, April 1997, p. 180.

[7] Bill Romano, "Tech spy pleads guilty to theft: Engineer admits giving Intel 486, Pentium plans to AMD," *San Jose Mercury News*, March 19, 1996, p. 1E.

[8] General Accounting Office, "Report to Congressional Requesters: Information Security - Computer Attacks at Department of Defense Pose Increasing Risks," GAO/AIMD-96-84, May 1996.

http://www.epic.org/computer_crime/gao_dod_security.html

[9] Ellen Alderman and Caroline Kennedy, *The Right to Privacy*. New York: Alfred A. Knopf, 1995, pp. 310-317.

[10] Peter H. Lewis, "Behind an Internet Message Service's Close: Pressure From Church of Scientology Is Blamed for the Shutdown," The New York Times, September 6, 1996, p. D2.

[11] Paul Wallich, "Cyber View: Cracking the U.S. Code," *Scientific American*, April 1997, p. 42.

**Sam Nitzberg** was born in and lives in Long Branch, New Jersey, USA. He graduated from Monmouth University with a Bachelors degree in Computer Science, and a Masters degree in Software Engineering. His Masters thesis concerned the performance benchmarking of Unix audit trail systems. He is presently studying for his Ph.D. in Computer Science at Stevens Institute of Technology in Hoboken, New Jersey, USA. Mr. Nitzberg has been working for Telos for the last five years, specializing in software engineering and computing security.