Unclassified

Next Previous Contents

Are We Our Own Worst Enemy?

Safeguarding Information Operations

Stephen W. Magnan

> *The reality is that the vulnerability of the Department of Defense--and of the nation--to offensive information warfare attack is largely a self-created problem. Program by program, economic sector by economic sector, we have based critical functions on inadequately protected telecomputing services. In the aggregate, we have created a target-rich environment, and US industry has sold globally much of the generic technology that can be used to strike these targets.*
>
> -- Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D), November 1996

Most articles about the US information superhighway have concentrated on the need for better physical security, while at the same time identifying many of its cyber-related vulnerabilities. Few address what possibly is the most vulnerable element--the human operators--and the inability of those operators from the policy level down to practice good operations security (OPSEC).

In a 4 June 1998 *Guardian Online* article by Duncan Campbell, entitled "Hiding from the Spies in the Skies," he states, "The Internet has made tracking and evading spy satellites child's play.... Data and programs downloaded from the Net enable anyone to track the satellites and work out when the spies in the sky are overhead." Campbell also provides instructions on how to visually acquire satellites with the naked eye and even lists six Internet Uniform Resource Locator addresses where one can find programs and information on the location of the "spies in the skies." He refers to several Internet sites in his article that offer the capabilities to track the locations, routes, and times certain satellites will pass over specific locations.

India's Nuclear Tests

In May 1998, India conducted a series of underground nuclear tests that, according to the press, the Clinton Administration learned about when India publicly announced the tests. This prompted widespread speculation about how multibillion-dollar US surveillance and reconnaissance assets could have missed the critical clues that revealed the impending tests. India readily admitted that it knew how to deceive the United States. It referenced information the United States had shown it in the past and also downloaded tools freely available from the Internet. In an Associated Press article of 15 May 1998, Indian nuclear researcher G. Balachandran stated, "It's not a failure of the CIA. It's a matter of their intelligence being good, our deception being better."

An action that further assisted the Indians in their deception campaign was the "sharing" of intelligence and overhead imagery by the United States. In an effort to thwart a nuclear test in December 1995 and January 1996, the United States had shared this information with the Indians to convey the message that "We know what you are doing and do not approve." Demonstrating the US capability to track India's actions, *and* the fact that the United States *was* tracking their actions, directly informed the Indians that they needed to develop a superb OPSEC and deception campaign.

The commission that was formed to evaluate why the intelligence community (IC) failed to predict the Indian nuclear tests concluded that the IC needs a good overhaul. It directed little attention, however, to India's successful deception effort or to development of an information operation (IO) perception management campaign. Instead, it recommended reviews of policies, changes in leadership and

management philosophies, and organizational structures. The commission's recommendations address, in a generic manner, the symptoms of the problems, not the causes:

> *The organization needs to be scrubbed, and I am talking about the IC organization, not necessarily the CIA, to improve the clarity of the structure, to fix responsibilities, to resource the staff with appropriate tools, and to inform the organization once that review has taken place.*

No mention was made of improving education or training, increasing manpower, or dedicating more assets to those who need it most--the workers. Therefore, the imagery analysts will continue to work under a new and improved management and supervisory staff, who will tell or show the analysts how to do a better job with the available resources.

OPSEC requires the same elements as the imagery analysts do: improved education and training and increased billet authorizations. OPSEC requires as much senior-level support as do the other elements. Furthermore, all elements of IO can no longer be common-sense based--they are not integrally linked to each other.

Beating the System

Katie Hafner and John Markoff, in their book *Cyperpunk: Outlaws and Hackers on the Computer Frontier*, give an instructive example of how easy it can be to access a computer system:

> *While in Washington, Susan got the chance to demonstrate her "social engineering skills." As Susan later told the story, a team of...colonels and generals from three service branches sat at a long conference table with a computer terminal, a modem, and a telephone. When Susan entered the room, they handed her a sealed envelope containing the name of a computer system and told her to use any abilities or resources that she had to get into that system. Without missing a beat, she logged on to an easily accessible military computer directory to find out where the computer system was. Once she found the system in the directory, she could see what*

operating system it ran and the name of the officer in charge of that machine. Next, she called the base and put her knowledge of military terminology to work to find out who the commanding officer was at the SCIF, a secret compartmentalized information facility. "Oh, yes, Major Hastings." Casually, she told the person she was talking to that she couldn't think of Major Hastings's secretary's name. "Oh," came the reply. "You mean Specialist Buchanan." With that, she called the data center and, switching from nonchalant to authoritative, said, "This is Specialist Buchanan calling on behalf of Major Hastings. He's been trying to access his account on this system and hasn't been able to get through, and he'd like to know why." When the data center operator balked and started reciting from the procedures manual, her temper flared and her voice dropped in pitch. "Okay, look, I'm not going to screw around here. What is your name, rank, and serial number?" Within 20 minutes, she had what she later claimed was classified data on the screen of the computer on the table. A colonel rose from his seat, said, "That will be enough, thank you very much," and pulled the plug.

This story may or may not be based on a true incident, but similar such incidents occur on a daily basis around the world. In 1997, the JCS mandated the conduct of the first-ever No-Notice Interagency Exercise (NIEX) based on an IO scenario as part of the ELIGIBLE RECEIVER exercise series. Several other Unified Command commanders have also ordered that similar IO-based exercises be conducted within the confines of their command.

These IO-based scenarios are designed to test the Blue Team's ability to overcome an unknown adversary who will be attacking from an unknown location and time against a large variety of potential targets. The goals of these exercises are to prepare the United States for any type of IO attack, to get US personnel "thinking outside the box," and to test the US ability to thwart such an attack. Thus far, the Red Teams for these IO-related exercises have achieved unprecedented victories over the Blue Teams.

ELIGIBLE RECEIVER 97-1, as well as several other IO-based exercises, disclosed several human vulnerabilities in the cyber world, including the ease with which Red Team personnel "socially engineered" Department of Defense (DoD) personnel and the vast amount of valuable information the Red Team was able to

collect from the Internet on a daily basis. When participants were asked who was addressing the recommendations and conclusions from after-action reports for past IO-based exercises, the answer was always, "That's a good question."

Approaches to the Problem

The DoD has more than 2.1 million computers, more than 10,000 Local Area Networks (LANs), and more than 100 long-distance networks. More than 95 percent of this system is commercial, commercial based, or leased from commercial sources (phone lines, computer hardware and software, and service contracts).

The DoD is taking some actions to prevent similar exploitation of the US critical infrastructures, but, once again, these actions are mostly cyber- and computer-related. Is the popularity of IO-related exercises merely a result of the "newest fad," available funding, or survival techniques? By repeating Red Team victories from one Unified Command or agency to another without trying to fix the problem(s) creates a "self-licking ice cream cone" for the IO community, that is, an ensured mission and fund site for the foreseeable future.

One major obstacle some DoD agencies have overcome, however, is the propensity to create a "loophole" so the Blue Team always wins. This fact alone demonstrates some have taken a paradigm shift and a step in the right direction. But one more paradigm shift is required. DoD has to realize that the human element, not the computer, remains the true cornerstone of information warfare. OPSEC is not a dead program! It is also not a function of the IC but of the Operations (J-3) Community.

Presidential Commission

The President's Commission on Critical Infrastructure Protection (PCCIP), established in 1997 to evaluate the vulnerable components of US critical infrastructures, published its findings in an unclassified report titled *Critical Foundations: Protecting America's Infrastructures*. It identified eight critical components: telecommunications, transportation, banking/finance, electrical power, oil and gas production and storage, water supply, emergency services, and

government services. The report detailed how reliant the United States is on those systems and how vulnerable the systems are to disruption or destruction. The report does not identify the exact location of critical nodes, but it emphasizes the vulnerabilities associated with the identified infrastructures. It further implies that schematics, which outline the specific locations and breakdowns of these critical nodes, are available either for free or for a small fee. The entire PCCIP report, as well as subsequent updates, is available on the World Wide Web.

The publication of the PCCIP report is a two-edged sword. It offers a wake-up call to the United States about many of the possible threats it faces on a daily basis and actions that need to be taken to avoid such threats. On the other hand, it offers an excellent targeting resource launching pad: if someone with aggressive intent, either for war planning or terrorist purposes, were to read, study, and analyze this document, a great deal would be learned about a potential US Achilles' heel.

The PCCIP consolidated all the information, statistics, and even vulnerabilities for anyone who wants to read about them. The best counter-argument would be: if a bullet has your name on it, it is going to get you...but you do not stick your head out of the foxhole to see if you can read the *names* on the incoming bullets! The same holds true with the PCCIP. Even though this information is *unclassified* and available in open-source documentation, one need not search far--the PCCIP has packaged it all in one neat, organized, and searchable document.

Overpublication

Numerous articles, studies, and think-pieces have been published detailing the need to protect the infrastructure from "attack." By devoting considerable attention to these vulnerabilities, US authorities have inadvertently revealed their overreliance on the information superhighway and the tremendous impact any degradation would have. The rush to publish such articles, along with the publication of the PCCIP, are a boon to potential US adversaries who are beginning to realize the significance and ease of executing an Information Warfare (IW) campaign. Both China and Russia offer schools whose sole concentration of study is IW.

The tendency to fall into the publish-or-perish mode is not the exclusive preserve of the academic community. It appears to be just as relevant to the DoD, contractor, and other DoD-related industries. With this in mind, the United States needs to

rethink and readdress what constitutes publication and what truly *needs* to be proliferated on the World Wide Web. The Web already contains sensitive information about US military personnel, units, capabilities, and functions, which can be accessed anonymously from anywhere in the world. From the PCCIP to Joint Doctrine, the United States itself is peeling back its layers of protection of the US critical infrastructures.

OPSEC in the Corporate World: Ellery Systems

With the arrival of the information age, the civilian sector has become vulnerable in new ways to economic and corporate espionage. The computer allows more data to be "stolen," and the digitization of data also allows this data to be in more than one place at the same time. Individuals can steal information, and the victim will not know about the theft until it is too late. Consequently, OPSEC is becoming more of a priority in the private sector.

The experience of Ellery Systems, Inc., provides a good vulnerability case study. Ellery Systems was a leading information systems/software products/engineering services company based in Boulder, Colorado. Leading corporations, government agencies, and universities worldwide used its software and services to provide practical information systems solutions for scientific, educational, medical, manufacturing, aerospace, defense, and financial applications. In a case spanning 1989-1995, Ellery lost everything with a few keystrokes.

Ellery's principal customer was the National Aeronautics and Space Administration (NASA), for which Ellery was developing a system to transfer Astrophysics Data Systems over the Internet. At the time, it was the largest data system ever to be deployed across the Internet, and Ellery owned rights and source code for the program that allowed the compression of data and its transmission.

Ellery devoted years of research, some of which was financed by the DoD, and millions of dollars to develop a communications software program. Ellery was also contributing advanced software technology and applications, runtime licenses, systems engineering, quality assurance and management, and operations support to the National Information Infrastructure Testbed (NIIT), an industry-led consortium

formed to help stimulate business and enhance American competitiveness by turning the vision of a national information highway into reality. NIIT provided a nationwide, high-performance testbed environment for implementing a series of real-world applications. The members wanted to evaluate both the everyday and technical issues associated with the maintenance and operation of a national information infrastructure.

Ellery shared membership in NIIT with some well-known and well-established institutions, including AT&T; the College of Oceanic and Atmospheric Sciences; Oregon State University; Department of Energy/Sandia National Laboratories; Digital Equipment Corporation; the EUV Center for Astrophysics; University of California-Berkeley; Essential Communications; Hewlett-Packard; Institute for the Study of the Earth, Oceans, and Space, University of New Hampshire; Network Systems Corporation; Novell, Inc.; Ohio State University; Smithsonian Astrophysical Observatory; Sprint; Sun Micro Systems; and Syn Optics Communications.

Chinese Connections

In the spring of 1989, Andrew Wang and Jing Cui legally entered the United States from China to work for a corporation known as Unidata, in Denver, Colorado. In December 1990, Ellery Systems hired Wang. For the next year and a half, Wang worked long hours and performed in a superior manner. Most important, he gained the trust, admiration, and friendship of the other employees. He fit right in.

During this time, a Chinese business official showed up at Ellery interested in its technological advances. The Chinese official explained he wanted to improve China's ability to teach its children in foster homes, daycare centers, and schools. Ellery Systems personnel were attracted by the charitable nature of the inquiry, and they were excited to meet a foreigner who spoke their jargon. They told and showed the Chinese official anything he wanted.

In the summer of 1993, Wang obtained a printout of the Ellery source Data/Code. He approached Cui, who still worked for Unidata, and proposed that they start up a new computer company together, DC Nology. To help them get off to a good start, Wang explained the technological advances Ellery had made and was developing.

In late 1993, Wang contacted Fu Xiangqun, a trade official in China, and explained the opportunity available for them at Ellery's expense. Fu Xiangqun found a party interested in the opportunity and contacted Wang immediately. Wang approached the company's president, and he explained that his mother was sick in China and that he would like to visit her. The president, who later admitted to his ignorance and naiveté in the whole matter, said Ellery almost paid for Wang's plane ticket.

In January 1994, Wang flew to China and moved around trying to sell his wares to the highest bidder. He signed a $550,000 business deal with Beijing Machinery Import and Export, a company run by the Ministry of Defense.

On 31 January 1994, Wang returned to Ellery and gave notice he was going to leave the company within two weeks. On 1 February 1994, Wang electronically transferred 122 computer files from Ellery Systems to Unidata in Denver. These files contained 2.5 megabytes of Ellery's source-coded files. Ellery did not discover the missing files until 10 February. At that time, the firm's president immediately contacted the FBI and Colorado's Attorney General to investigate the "theft." After explaining to the president that virtually no laws pertained to the case, both the FBI and the state's Attorney General worked to help Ellery successfully prosecute this case. Realizing the precedent this case was setting and that they were entering new legal territory, they pushed hard on the case to help all the other small businesses that might also be victimized.

Enter the FBI

As FBI officials began their investigation, they briefed Ellery's president on the facts as they discovered them, including how this "attack" fit the profile of Chinese intelligence operations. They then informed him of Wang's travels around China and the contents of the letter Wang wrote to the Chairman of Beijing Machinery, in which he described advanced computing technology. In this letter, Wang stated: "The common practices of the Americans should be used to defeat them in their own competition." The president elected to pursue the case in court and break precedent with other companies that had not, until this point, even tried to prove their products had been "electronically" stolen.

Most companies that are victims of this sort of theft never tell anyone because they do not want to lose customers. Yet at that time, 25 percent of the US GNP came

from information technology companies, an industry in which Ellery was rapidly growing.

The FBI arrested Wang on 24 February 1994 and searched Unidata. They had no problem finding Ellery's files on the Unidata computer, and, on 5 April 1994, both Wang and Cui were indicted on charges of wire and computer fraud. The FBI had nothing else to charge them with at the time. The wire-fraud charges were based on a law enacted in the early 1900s which dealt with criminal acts over telegraph and telephone lines. Because the Internet was experiencing problems and re-routed Wang's transmission of the Data/Code signal through three other states, the FBI and State Attorney General's office saw this as their best chance to prosecute. Lawyers for both Wang and Cui entered innocent pleas.

On 15 April 1994, a US judge, citing national security concerns, blocked the $550,000 business deal between Wang and Beijing Machinery. He also ruled that Wang had to remain under house arrest until the trial. On 6 December 1995, however, the criminal charges against Wang and Cui were dropped due to insufficient evidence.

A Painful Lesson

Ellery's key mistake was to trust completely all new employees it hired. Since this case, the enactment of the Economic Espionage Act of 1996 has helped protect US trade secrets. Ellery downsized, declared bankruptcy, and eventually evolved into a new organization--Global Commerce Systems, Inc.--with Ellery's former president in charge. He openly discusses the lessons that he and his fellow owners learned from this incident, and he continues to work closely with the OPSEC community and the National Counterintelligence Center.

Testing Security

The computer security threat has gained the most attention of late with Red Teams as well as security consultants such as Ira Winkler for hire, Corporations, both large and small, hire Winkler and his staff to infiltrate their organization and steal whatever they can to test the corporation's security procedures and practices. Many of his success stories are documented in his book *Corporate Espionage*, and he also

speaks of several others when giving presentations. Today, the aspect of "Red Teaming a corporation" which is most widely written about is computer hacking. Many articles have been written about the different corporations and small businesses that make a hefty profit by hiring out their hacking services to test organizations. Winkler, however, stresses that the hacking part of his probes is only one small element.

OPSEC

In the armed services, initial OPSEC training at most units is lumped into the first month or so after the individuals have arrived on station, if the training is offered at all. It is either conducted during a long, drawn-out mass briefing process that only occurs once a quarter or once a year, depending on how many people rotate in and out of the unit, or it is contained in a binder the individual has to read on his own. The second alternative is more prevalent, because it is easier to circulate a binder than conduct a briefing. Given the current attitudes toward OPSEC, most people just sign documentation that they received initial or periodic required OPSEC training. In this fashion, they have satisfied the OPSEC representative's requirement to pass the next Inspector General inspection. This approach, unfortunately, leaves much to be desired in the training department, and it is reflected on a daily basis by poor OPSEC practices.

The level of interest personnel have in the OPSEC program is directly proportional to the attitude of not only the OPSEC representative, but also the content and style of his training program. Furthermore, the chain of command has to support enthusiastically and openly both the training program and the continued practice of sound OPSEC measures. A motivated and dedicated OPSEC representative, together with public support from the chain of command, can organize a dynamic and interactive training program that will entertain and educate.

Several different organizations, both civilian and DoD associated, offer a vast amount of information to assist any unit's OPSEC representative. These organizations offer free training programs, both hardcopy and computer-based training, and daily, monthly, quarterly, or annual newsletters, conference reports, and other OPSEC-related educational material. Getting the word out to those who need it most and the de-institutionalizing of the OPSEC community as a whole seem to be among the problems facing the DoD today.

The Interagency OPSEC Support Staff (IOSS) is charged by the National Security Decision Directive on OPSEC 298 (NSDD 298) to:

> *...provide or facilitate OPSEC training, and act as a consultancy to Executive Departments and Agencies required to have formal OPSEC programs. The IOSS offers expertise in different disciplines and skills through its diverse membership which currently consists of representatives from the DoE, CIA, NSA, GSA, FBI, and DoD.*

IOSS celebrated its 10-year anniversary in 1998, yet word of its existence and services has still not spread to the community as required.

Continuing Importance

A successful OPSEC program parallels a successful intelligence organization in that one never hears about the success stories, only the failures. Kudos should go to several commands within DoD that have begun filtering the information they post. Unfortunately, once something is inadvertently posted it should be considered compromised. The Scott O'Grady rescue e-mail is a perfect example of how, once something is exposed to the Internet, it takes on a life of its own. Many people have tried unsuccessfully to eradicate the e-mail from the Web.

As the Federal Government continues to publish articles and direct unprecedented attention to cyber threats while seemingly ignoring traditional human-related vulnerabilities, it is setting itself up for a potential future catastrophe. Even though our official world becomes more and more information-based with each passing day, it cannot and should not leave traditional programs such as OPSEC to each individual's common sense. The threat of individuals stealing critical information via computers remains real. On a daily basis, however, personnel in DoD and in the rest of the IC freely, and, more than likely, inadvertently, give more information away via the computer (e-mail and web pages), phone, fax, garbage, or any other number of methods.

The value of this information, freely and innocently published, distributed, and discarded remains underestimated and addressed primarily by OPSEC and OPSEC-related professionals. To help offset these human-related vulnerabilities, senior-

level support and funding need to be made available to help move OPSEC into the role of everyday applicability. This funding and support should go toward the training, education, and practices of the other elements of IO, particularly OPSEC, besides just those dealing with the cyber-threat.

Stephen W. Magnan is a captain in the US Air Force.

Unclassified