Are We Our Own Worst Enemy?

Safeguarding Information Operations

Stephen W. Magnan

> **"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."**

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

> *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," Campbell 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 the US multi-billion-dollar 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." By 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, and, ultimately, to 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 commission that was formed to evaluate why the Intelligence Community failed to predict the Indian nuclear tests concluded that the IC needs a good overhaul."

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 *Cyberpunk: 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

Approved for Release: 2014/09/10 C00935281