The Center for Security Policy

OCCASIONAL PAPERS SERIES

October 2007 No. 28

Information Warfare: An Emerging and Preferred Tool of the People's Republic of China

by Dr. William G. Perry

Center for Security Policy
1901 Pennsylvania Avenue, NW, Suite 201, Washington, DC 20006
http://www.centerforsecuritypolicy.org

Information Warfare:
An Emerging and Preferred Tool of the People's Republic of China

by Dr. William G. Perry*

In 1991, the U.S. devastated the armed forces of Saddam Hussein with a joint air, land, and sea assault that was unprecedented in ferocity and effectiveness. This victory, coming as it did on the heels of the Soviet defeat in Afghanistan, was a powerful statement to the world about American military supremacy. U.S. aircraft, aided by commandos on the ground, disabled Saddam's vaunted air-defense systems and destroyed his communications infrastructure, thereby severing the command-and-control links to his forces on the ground, which were then destroyed piecemeal. The result was one of the most rapid and decisive military victories in modern history.

The consequences of this triumph were widely felt, perhaps nowhere more keenly than in Beijing. Since the end of the Cold War, PRC strategists have been contemplating how best to challenge U.S. predominance in Asia, a region that China considers its own. Thinkers in the People's Liberation Army, having observed the Desert Storm campaign, realized that it was not feasible for them to directly challenge the U.S. military – to do so would be to invite certain defeat. However, America's reliance on satellite and information technology to mount its joint assaults presented them with an opportunity for an asymmetric advantage – if the U.S. networks could be corrupted, damaged, or destroyed, then the PLA would stand a fighting chance of winning a so-called "local war under high-tech conditions." This paradigm of exploiting a powerful adversary's weaknesses to counteract his strengths comports perfectly with a long military tradition in China of "defeating the superior with the inferior."

This paper purposes to analyze the evolving doctrine and practice of Chinese information warfare (IW) – the tool that Beijing is seeking to use to circumvent the U.S.'s conventional military might. First, a suitable definition of information warfare in the Chinese context shall be set forth. Second, we will discuss how China is amassing an IW infrastructure with the intention of infiltrating and debilitating U.S. military information networks. Third, it shall be demonstrated that these technical and human resources are directed both at American forces in the Pacific, and even more worryingly, at U.S. domestic IT infrastructure. We will conclude by offering concrete policy recommendations on how the U.S. can deter and defeat Chinese information warfare.

Before moving on, it should be noted that this paper will not address the related but distinct issue of electronic espionage. Even though the implements and ends are the same, it is a separate concept that deserves its own treatment.

---

* *Dr. Perry is a professor of computer information systems and teaches computer networking and information security at Western Carolina University. He has experience in counterintelligence and threat assessment and has made presentations on the protection of the nation's critical infrastructure.*

Chinese information warfare: background

To enable a detailed discussion about information warfare, it is useful to set forth both a context that will allow for an appropriate understanding of the subject at hand. First, a word about the modern information environment. The increasing digitization of military operations, economic and financial infrastructure, as well as all modern communication networks carries with it a great risk. According to a private industry report, "a combination of global connectivity, employee mobility and rapid technological change [exposes] the [information] infrastructure to a myriad of risks in the form of fraud, theft, pirating, industrial espionage and business disruption."[1] This statement deals only with civilian affairs, but given the internetted nature of Pentagon C^4ISR, such systems are obviously at high risk if they are not adequately defended.

Second, it is worth addressing the fundamentals of Chinese thinking on the subject. In the relevant literature, there are a great variety of definitions and descriptions of information warfare, some broad, some more narrow, and varying by author. The most apt is that set forth by Toshi Yoshihara, who claims in his *Chinese Information Warfare: Phantom Menace or Emerging Threat*? that Chinese IW "seeks to disrupt the enemy's decision-making process by interfering with the adversary's ability to obtain, process, transmit, and use information."[2] This strategy closely mirrors that pursued by the U.S. in the already-mentioned Desert Storm campaign, when Iraqi leaders were deprived of the information and communications systems crucial to effective warfighting. Thus, information warfare in the Chinese context is a non-conventional weapon designed to impede an adversary's decision-making with the aim delaying or even deterring conflict. If the use of force is unavoidable, the Chinese would use IW to "shape the battlespace" in a manner that increases their chances of victory.

China's information warfare capabilities and practice

To transform its information warfare thinking into practice, China is actively developing a body of intellectual and physical capital that it hopes will place it among the worlds leaders in IW. According to the Pentagon's 2006 *Report on the Military Power of the People's Republic of China,* the PRC is working to ensure that "militia [and] reserve personnel would make civilian computer expertise and equipments available to support PLA training and operations."[1] It is seeking personnel from "academies, institutes, and information technology industries" so as to integrate them "into regular military operations."[2] These units are trained to "support active PLA forces" by mounting large-scale IW assaults on adversary networks.[3] This combination of civil/military efforts in war dates back to the Maoist doctrine of "People's War," and has great traction in modern China. It also comports with the famous dictum of Deng Xiaoping of "*jun min jie he,*" or "combine the civil and the military."

These integrated IW capabilities are directed primarily at the American military. In the field of computer network operations, the Pentagon notes that the PLA operates computer virus-creating units whose goal is to attack enemy computer systems and networks. One type of virus, called Myfip, is particularly well-suited to information warfare. It is usually well-disguised, and once

activated on poorly protected network systems, can wreak havoc on an organization's information infrastructure. In one attack, pilfered information was traced back to Tianjin City in the People's Republic of China. (Myfip Intellectual Property theft Worm Analysis, 2005) This sort of assault is capable of compromising an entire network information system and stealing any of the following file types:

- .pdf – Adobe Portable Document Format
- .doc – Microsoft Word Document
- .dwg – AutoCAD drawing
- .sch – CirCAD schematic
- .pcb – CirCAD circuit board layout
- .dwt – AutoCAD template
- .dwf – AutoCAD drawing
- .max – ORCAD layout
- .mdb – Microsoft database

Any network infected with Myfip would be subject to losing its organization's documents, plans, communications and database. Any or all of the critical information could be stolen. Even more insidious is the idea that without proper monitoring the target may have had all of its proprietary information stolen and be totally unaware.

In recent years, hackers and IW practitioners in China have been actively testing U.S. cyber defenses with a series of low-level assaults and incursions. The 2006 Report to Congress of the U.S.-China Economic and Security Review Commission states that these activities amount to a program of "cyber reconnaissance" in which China is "probing the computer networks of U.S. government agencies as well as private companies" with the aim of "identifying weak points in the networks, understanding how leaders in the U.S. think, discovering the communications patterns of American government and private companies, and attaining valuable information stored throughout the networks."[4]

There are several recent examples such "probes":

- In late 2006, computer banks at the U.S. National Defense University were shut down by a large-scale cyber assault.[5] NDU was in the middle of a large electronic war-simulation at the time of the attack. The attack was not publicized.
- Also late in 2006, the entire Naval War College computer network was shut down by a Chinese intrusion. One report hinted that the attack was aimed at NWC's Strategic Studies Group, which had been developing modern cyberwarfare concepts.[6]

- In the summer of 2006, computers at the Commerce Department's Bureau of Industry and Science were offline for more than a month after a cyberattack based in China. The stealthy assault was aimed at the office which controls high-tech exports to China.[7]
- Most recently, a June 2007 attack was able to shut down several email communication systems in the office of the Secretary of Defense. While many media outlets noted that the intrusion came from China, DoD official were more reticent about naming a source.[8]

One of China's preferred methods for perpetrating such an attack is through a so-called Distributed Denial of Service (DDS). Put simply, a DDS attack occurs when a target is overwhelmed by "botnets" that make a request for service from a single information resource. Botnets are extensive networks of computers enlisted by the attacker to overload the response capability of the targeted information system. These computer foot soldiers are known as "zombies" in industry parlance, and can often number more than 100,000 per attack. In the cyber attack on Estonia in May, some new outlets report that the network employed may have enlisted more than one million members.[9] In the case of China, the scholar Timothy Thomas reports that numerous techniques, such as marshalling botnets, have found a home in several units of China's 1.5 million-man military reserve forces.[10]

China's information warfare doctrine has evolved to contain a blend of American IW doctrine with unique Chinese cultural components such as the gold standard of fighting a "People's War", deceptively *killing with a borrowed sword* and attacking weakness rather than strength.

The Chinese seek to conduct a "local" or limited war under conditions of "informationalization". The modern Chinese view of information warfare has departed from one with an exclusive ideological base to that of being a process of on-going innovation that is worthy of continuous study and adaptation. The Chinese appear to have incorporated much of U.S. information warfare strategy. Two key IW doctrinal publications, JP 3-13.1 and FM-100-6, have been translated into the Chinese language.

According to a paper written by Austin Williams for Georgetown University China's information warfare strategy is now based upon viewing information as a weapon of war or combat and something that is sought after by the warring parties. That is a broad umbrella.

Yoshihara's paper quotes the father of Chinese Information Warfare as stating:

> *IW is combat operations in a high-tech battlefield environment in which both sides use information-technology means, equipment, or systems in a rivalry over the power to obtain, control and use information. IW is a combat aimed at seizing the battlefield initiative; with digitized units as its essential combat force; the seizure, the control, and use of information as its main substance, and all sorts of information weaponry [smart weapons] and systems as its major means.*[11]

China intends to conduct information warfare with non-attributable asymmetric techniques that focus upon information suppression, destruction and alteration. This doctrine fits well with exploiting the inherent vulnerabilities of information systems. Even Chairman Mao acknowledged the value of 'making the enemy blind and deaf by sealing his eyes and ears and to drive his commanders to distraction by creating confusion in their minds.'

China's IW doctrine is based upon maintaining technical parity with its enemies while still being able to overwhelm the enemy with huge numbers of its own civilian population who have been prepared to conduct IW operations. Highly trained civilian computer experts are expected to become the soldiers in an information war rather than committing human wave after human wave of PLA troops to overrun the enemy's position on a battlefield. Sun Tzu's teachings of winning the battle without engaging a fortified structure also dovetail quite well with seeking out and attacking the weak points of an information system rather than committing the army and navy.

Chinese Information Warfare doctrine is chillingly captured in Williams' paper by citing a quote attributed to a Chinese IW theorist, Wei Jincheng. The quote is best read within the context of China's long-term desire to re-claim Taiwan:

> *Information-based confrontations will aim at reaching tangible peace Through intangible war, maintaining the peace of hardware through software confrontations, and deterring and blackmailing the enemy with dominance in the possession of information.*[12]

China is transparently planning to conduct a limited war to regain Taiwan and to deter Western interests by attacking the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) as well as our economic system. If a third party (a terrorist state or organization?) can be enticed to detonate an electromagnetic pulse weapon above the U.S. task of taking Taiwan would be relatively easy.

What should be done?

Policy makers, government administrators, infrastructure owners and operators need to become more aggressive when protecting our country against the information warfare that is being conducted. The following policy recommendations are made:

1. All contractors, universities and outsourced agents who interface with the federal government's information infrastructure should be required to be ISO 17799 certified.

> ISO/IEC 17799 is a set of international information security practices and standards. They specify accepted security practices related to securing information assets. The ISO/IEC 17799 standards (to become ISO 27000 in the future) seek to serve as "a starting point for developing organization specific (information security) guidelines."[13]

The ISO standards cover the following twelve domains: risk assessment and treatment, security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management and business continuity management and compliance.

Security analysts responsible for protecting sensitive information can be relatively confident if an organization is ISO 17799 compliant. A high degree of information assurance (security) is likely to be a characteristic of the data set being used. The reverse may be true if the organization is out of compliance with ISO 17799.[14]

2. The Department of Homeland Security must promote, as a matter of policy, a sector-by-sector information security awareness training program.

A majority of the private and government organizations in this country are woefully unaware of the threats and vulnerabilities associated with the use of the information infrastructure (computer networks, the Internet, etc). The focus of a DHS information security awareness training program should go beyond posting a series of web pages and reports that are tucked away in the third or fourth levels of a web site.

A cadre of well-trained DHS employees should be sent into each state in the nation to train a sufficient number of state homeland security staff in the essentials of information security. An information security awareness-training program should be funded for each sector of the interlinked critical infrastructure. Employees in each sector should be aware of their responsibilities for information security.

3. All sensitive national research and development programs should be required to implement an information security plan that includes vigorous personnel screening practices, security training and monitoring practices.

Millions of dollars of critical research and development programs are spread across the nation. Most programs lack even the most basic components of a cohesive information security program……"People don't appreciate the true nature of what information has value. Without an understanding of value, businesses and people will not be able to adequately determine the risk that is faced and justify the countermeasures that need to be implemented."[15]

The methods and means used by unfriendly competitors or hostile nation states and the nature of modern day information processing technology dictate that we must be vigilant in protecting critical information assets and our national research infrastructure.

4. Access to the Internet by federal employees should be severely restricted and isolated.

Access to the Internet by federal employees should be severely limited or denied. Many individuals would consider restricting access to the Internet in the workplace to be bordering on heresy. A reality check, however, is necessary. The Internet and its services bring threat vectors to the desktop computing environment and ultimately internal networks. Employees in both the public and private sector are unaware. Threats are typically programmed to seek out vulnerabilities that exist in a system for the ultimate purpose of stealing or damaging the target's information infrastructure.

Only a limited number of employees need to have direct access to the Internet for browsing to perform basic job tasks. An individual who needs Internet access should have his or her workstation completely isolated from the internal network using a combination of customized telecommunications equipment and software to reinforce isolation from the internal production network.

Isolating workstations from the Internet can be accomplished by either blocking selected services such as the transfer of files or (FTP) and "instant messaging" or separating workstations that have Internet access from critical portions of the internal network.

5. Communications on all federal information systems should be encrypted.

All information that is created, maintained, transported or transmitted by the federal government should be encrypted. The news is replete with examples of serious information security failures. For example, the Washington Post recently reported that the Transportation Security Agency lost a hard drive in early May of 2007 that contained the names of employees and other confidential information.[16] Had the information been encrypted the loss would have been less serious.

Reportedly, "The FBI and the Secret Service have opened a criminal investigation into the apparent theft of a computer hard drive containing the personal, payroll and bank information of 100,000 current and former workers of the Transportation Security Administration, including airport security officers and federal air marshals."[17] The missing hard drive did require the use of biometric authentication (such as a finger print). But if the thief was an insider, little would prevent the thief from accessing and using information in any manner.

The need for encrypting ALL federal data becomes even more apparent when recalling an incident in which the Department of Veteran Affairs lost more than 26 million records on military personnel. The data was apparently recovered but determining whether the information had been copied is virtually impossible. The Washington Post sited the following "Since 2003, 19 federal agencies have reported 788 incidents of data theft or loss, affecting thousands of employees and the public"[18]

Properly encrypted information and data would be extremely difficult to decipher.

6. Any products, materials, integrated circuits, components, programs, processes or other goods that are deemed to be crucial to national security of the United States should be manufactured exclusively in the United States without the use of foreign suppliers or materials and further should be declared ineligible for export.

Information warfare, as outlined in this paper, involves the intersection of multiple threats that can be exercised against a host of vulnerabilities. The People's Republic of China has been shown to conduct a very broad range of information warfare operations against American interests. Requiring that components and products that are essential to U.S. National Security to be manufactured within the borders of the U.S. by American owned companies (with sufficiently robust information security) would help to limit the loss of high technology to our adversaries.

Countries known to be unfriendly to the United States, for example, should be kept at arm's length from critical advanced research and development, such as nanotechnology and photonics. The rush to take advantage of potentially lucrative foreign markets and to use cheap outsourced labor results in our exporting sensitive technology for production and seriously increases the vulnerabilities we face. Computers purchased for the U.S. State Department, for example, should only be manufactured in the United States (rather than purchased from a PRC manufacturer such as Lenovo) and then only under the strictest requirements.

Thousands of seemingly innocent relocations of technological processes and manufacturing gaffs have resulted in countless compromises of America's national security. Such losses could be curtailed.

7. Private owners of information networks that interface with any of the nation's critical infrastructure should be required to become ISO 17799 certified.

A majority of the critical information infrastructure is owned by the private sector in the United States. Requiring private networks that directly interface with any components of the critical infrastructure (i.e. defense, law enforcement, finance, energy, etc.) to be ISO 17799 would be a prudent and strong security measure and the least that could be done.

The critical infrastructure include….."s*ervices that are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States".*[19] Components of the interconnected critical infrastructure would be among the first targets of a full scale, simultaneous information warfare attacks. The PRC has already demonstrated the capability to coordinate such an effort in concert with its technical civilian militias that were concentrated to conduct information warfare activities.

A malicious software attack directed against the critical infrastructure is capable of causing damage, destruction, theft, and denial of access to critical information that is

needed to protect our people. Attacks against the privately owned portions of the nation's critical infrastructure do and will come from cyberspace.

8. The United States should do everything in its power to produce more domestic engineers and scientists.

A report cited by the Central Intelligence Agency listed "education" as the single most important determinant of success for nation states and individuals between now and the year 2015. Our nation has a need for qualified information technology professionals. The critical nature of the situation becomes quickly apparent. Do we believe that our country's formal information technology training programs promote the protection of our vital political and economic interests?

We are without a cohesive national plan to promote professional information technology training programs. The U.S. simply isn't growing the intellectual resources that are needed. Indeed, the information technology industry had to ask Congress for increases in the number of H1-B visas to hire skilled foreign workers. The problem is even worse.

Nearly 30% of the science and engineering faculty employed by universities and colleges in the United States are foreign born. More than forty percent of the Ph.D.'s awarded went to foreign citizens in science, engineering, and math. Our dependence upon foreign born scientists with divided loyalties needs to be abated.

The number of foreign born individuals (who are unlikely to be U.S. citizens) who have close proximity to our information infrastructure is staggering. More than 43% of the people who have entered America with H1B visas have gone to work in the information technology field. Indian citizens make up the largest number of foreign nationals with Chinese nationals having the second largest number.

Our nation should draft a National Information Technology Bill to address the problem. Business and industry could specify the curriculum. Universities could compete to be the designated information technology institute for each state (similar to India's plan to be an IT megapower). Matching funds could be provided. The information technology institutes could sponsor certification standards, meet continuing education requirements as well as manpower training needs. Such a plan would help to eliminate our dependency on foreign born information technology professionals.

[1] *Military Power of the People's Republic of China*, 2006, 35.
[2] Ibid.
[3] *Ibid.*
[4] 2006 Report to Congress of the U.S.-China Security and Economic Review Commission, as cited in Minnick, Wendell, "Computer Attacks from China leave many questions," *Defense News*, 13 August 2007, 14.
[5] Tkacik, John, "China's Quest for a Superpower Military," Heritage Foundation Backgrounder #2036, 17 May 2007.

[6] Bill Gertz, "Chinese Hackers Prompt Navy College Site Closure," *The Washington Times*, 30 November 2006, A11, as cited in Ibid.
[7] Sipress, Allen, "Computer System Under Attack: Commerce Department Targetted; Hackers Traced to China, *Washington Post*, 6 October 2006, A21.
[8] United Press International, "Defense Department Confirms Cyber Attack," 4 September 2007. Found at http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/09/04/defense_department_confirms_cyber_attack/7582/.
[9] Landler, Mark, and Markoff, John, "In Estonia, What May Be the First Cyberwar," *International Herald Tribune*, 28 May 2007. Found at http://www.iht.com/bin/print.php?id=5901141.
[10] Thomas, Timothy L., *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice* (Foreign Military Studies Office: Fort Leavenworth, KS, 2001).
[11] Toshi Yoshihara, "Chinese Information Warfare: A Phantom Menace or Emerging Threat?", Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, Pennsylvania, 2001.
12 Wei Jincheng, "Information War: A New Form of People's War," translated from the Military Forum column, Liberation Army Daily, 25 June 1996
[13] "Information technology - Security techniques – Code of practice for information security management," ISO/IEC, Second edition, 16 June 2005, Geneva, Switzerland.
[14] William G. Perry, "Enhanced data mining information assurance by using ISO 17799," Defense & Security Symposium Information: Assurance and Security, Data Mining, Intrusion Detection, Information Assurance and Data Networks Security, The International Society for Optical Engineering, 17 April 17, 2006.
[15] Ira Winkler, "Spies Among Us," Wiley Publishing, Inc., 2006, Indianapolis, Indiana.
[16] Spencer S. Hsu, "TSA Hard Drive With Employee Data Is Reported Stolen," Washingtonpost.com, 5 May 2007.
[17] Ibid.
[18] Ibid.
[19] William G. Perry, "The Science of Protecting the Nation's Critical Infrastructure," Voices of Discovery, Elon University, 7 March 2007.