Executive Summary
Backgrounder
Published by The Heritage Foundation
No. 2106
February 8, 2008

Trojan Dragon: China's Cyber Threat

John J. Tkacik, Jr.

America's counterintelligence czar, Dr. Joel F. Brenner, painted an alarming picture of economic espionage in 2006, albeit in the objective tones and neutral parlance of the intelligence community. He reported to Congress that "foreign collection efforts have hurt the United States in several ways":

- Foreign technology collection efforts have "eroded the US military advantage by enabling foreign militaries to acquire sophisticated capabilities that might otherwise have taken years to develop."
- "[M]assive" industrial espionage has "undercut the US economy by making it possible for foreign firms to gain a competitive economic edge over US companies."

Dr. Brenner characterizes China as "very aggressive" in acquiring U.S. advanced technology. "The technology bleed to China, among others, is a very serious problem," he said in March 2007, noting that "you can now, from the comfort of your own home or office, exfiltrate information electronically from somebody else's computer around the world without the expense and risk of trying to grow a spy."

On November 15, 2007, the bipartisan, congressionally chartered U.S.–China Economic and Security Review Commission (USCC) put a finer point on it: "Chinese espionage activities in the United States are so extensive that they comprise the *single greatest risk* to the security of American technologies." Cyberpenetration is by far China's most effective espionage tool, and it is one that China's spy agencies use against America's allies almost as much as against U.S. targets.

Targeting America. The U.S. military has been the primary target of Chinese cyberattacks, followed closely by the Departments of State, Commerce, and Homeland Security. Academic, industrial, defense, and financial databases are also vulnerable. Regrettably, American officials tend to be very sensitive to China's feelings and refrain from public allegations that the attacks are launched by Chinese agents, even though, as one U.S. cybersecurity expert points out, "the Chinese are in half of your agencies' systems" already.

In fact, Chinese cyberwarfare units have already penetrated the Pentagon's unclassified NIPRNet (Unclassified but Sensitive Internet Protocol Router Network) and have designed software to disable it in wartime. One general officer admitted that "China has downloaded 10 to 20 terabytes of data from the NIPRNet already" and added, "There is a nation-state threat by the Chinese."

This paper, in its entirety, can be found at:
www.heritage.org/research/AsiaandthePacific/bg2106.cfm

Produced by the Asian Studies Center

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Richard Lawless, then Deputy Under Secretary of Defense for Asia–Pacific affairs, told a congressional committee on June 13, 2007, that the Chinese are "leveraging information technology expertise available in China's booming economy to make significant strides in cyber-warfare." Lawless noted that the Chinese military's "determination to familiarize themselves and dominate to some degree the Internet capabilities…provide[s] them with a growing and very impressive capability that we are very mindful of and are spending a lot of time watching."

Chinese People's Liberation Army's cyberwarfare units now have the source codes for America's ubiquitous office software—provided to the Chinese government as a condition of doing business in China. This means that they essentially have a skeleton key to almost every networked government, military, business, or private computer in America that is accessible through the Internet.

What the Administration and Congress Should Do. Recent cyberattacks on the United States and its allies combined with warnings from the Defense Science Board and the U.S.–China Economic and Security Review Commission emphasize the seriousness of this growing threat to U.S. national security. To address this threat, the Administration and Congress should:

- **Identify China as an intelligence risk.** The Office of the National Counterintelligence Executive, the Department of Justice, and the FBI should follow the USCC's lead and identify China as the *top* spy threat. Congress should hold public hearings on the problem.
- **Address the legal impediments to criminal prosecution of cyberspies.** Current U.S. criminal laws are vague about assisting unknown foreign actors to penetrate secure networks for information-gathering purposes.
- **Closely examine Chinese commercial investments in cyber companies.** The Treasury Department's Committee on Foreign Investment in the United States should closely examine any attempt by Chinese military or intelligence to gain access to U.S. cybertechnology operations via commercial investments.
- **Require software companies to patch vulnerabilities quickly.** Software firms should be required to give first priority to the most critical vulnerabilities and should coordinate with U.S. government cybersecurity offices in identifying, assessing the risks from, and patching and/or mitigating vulnerabilities.
- **Require "trustworthiness" in critical information technology (IT) systems.** Components for defense-critical IT systems—from chips to storage devices—must come only from trusted and certified firms. Congress must address the disappearance of an industrial capacity to manufacture trusted IT equipment for defense needs over the long term.
- **Strengthen America's engineering and scientific competitiveness.** At a minimum, Congress should offer "national service" incentives, including scholarships and internships, to students in information science and technology fields. Congress should also urge the defense and intelligence agencies to leverage competition among the U.S. national laboratories to sustain peak innovation in IT research and development on highly classified systems.

Conclusion. America's vulnerability to cyberattacks is a critical threat to national security. If the Administration and Congress do not address these problems and implement the 2005 recommendations of the Defense Science Board, the fix will become prohibitively expensive and/or America's national security will be irreversibly compromised.

—John J. Tkacik, Jr., is Senior Research Fellow in China, Taiwan, and Mongolia Policy in the Asian Studies Center at The Heritage Foundation.

Backgrounder

Published by The Heritage Foundation

No. 2106
February 8, 2008

Trojan Dragon: China's Cyber Threat

John J. Tkacik, Jr.

America's counterintelligence czar, Dr. Joel F. Brenner, painted an alarming picture of economic espionage in 2006, albeit in the objective tones and neutral parlance of the intelligence community. He reported to Congress that "foreign collection efforts have hurt the United States in several ways":

- Foreign technology collection efforts have "eroded the US military advantage by enabling foreign militaries to acquire sophisticated capabilities that might otherwise have taken years to develop."
- "[M]assive" industrial espionage has "undercut the US economy by making it possible for foreign firms to gain a competitive economic edge over US companies."[1]

Dr. Brenner's report goes on to say that foreign intelligence efforts increasingly "rely[] on cybertools to collect sensitive US technology and economic information." Foreign intelligence agencies do this by "placing collectors in proximity to sensitive technologies or else establishing foreign research" by "forming ventures with US firms."[2] The report specifically identifies China and Russia as the leading culprits.[3]

Dr. Brenner characterized China as "very aggressive" in acquiring U.S. advanced technology. "The technology bleed to China, among others, is a very serious problem," he said in March 2007, noting that "you can now, from the comfort of your own home or office, exfiltrate information electronically from somebody else's computer around the world without the expense and risk of trying to grow a spy."[4]

Talking Points

- "Chinese espionage activities in the United States are so extensive that they comprise the single greatest risk to the security of American technologies," according to the U.S.–China Economic and Security Review Commission.
- In 2007, Chinese military hackers launched a series of very sophisticated cyberattacks against U.S. and European government targets. Government offices in Australia and New Zealand were also reportedly hit by Chinese hackers.
- People's Liberation Army cyberwarfare units now have the source codes for ubiquitous office software, which means that they essentially have a skeleton key to almost every networked government, military, business, or private computer in America on the Internet.
- The high threat of Chinese cyberpenetrations into U.S. defense networks will be magnified as the Pentagon increasingly loses domestic sources of "trusted and classified" microchips.
- The U.S. government should publicly acknowledge that China is the *top* spy threat to the United States.

This paper, in its entirety, can be found at:
www.heritage.org/research/AsiaandthePacific/bg2106.cfm

Produced by the Asian Studies Center

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

The Heritage Foundation
LEADERSHIP FOR AMERICA

On November 15, 2007, the bipartisan, congressionally chartered U.S.–China Economic and Security Review Commission (USCC) put a finer point on it: "Chinese espionage activities in the United States are so extensive that they comprise the *single greatest risk* to the security of American technologies."[5] Cyberpenetration is by far China's most effective espionage tool, and it is one that China's spy agencies use against America's allies almost as much as against U.S. targets.

Genesis of China's Cyberwarfare

In the 1990s, China's Ministry of Public Security (MPS), which manages the country's police services, pioneered the art of state control of cyberspace by partnering with foreign network systems firms to monitor information flows via the Internet.[6] By 1998, according to an insider's account of China's Internet development, the MPS and its subordinate bureaus found that their resources for monitoring the Internet had been overwhelmed by the sheer volume of Internet traffic—which by 1998 had not yet reached 1 million users in China.[7] Several U.S. firms reportedly aided the Chinese security services in constructing a new Internet architecture and training a vast army of cyberpolice to monitor Internet sites in real time and identify both site owners and visitors.[8] In August 1998, the cyberpolice announced their first arrest of a Chinese hacker via online monitoring.[9]

China's MPS has been successful beyond its wildest dreams. Using widely available sophisticated telecommunications equipment and services and using its own software tailored to China's requirements, China can effectively monitor all domestic Internet and wireless traffic of its netizen population of 137 million.[10]

The People's Liberation Army (PLA) organized its first cyberwarfare units (zixunhua budui) in early 2003.[11] They have since become a highly active element in China's ground force organization, no doubt building on the expertise developed in the late 1990s by China's police and state security services, which are well trained and equipped in using the Internet and cell phone networks to monitor, identify, locate, and censor cyberdissidents. China's 2006

1. Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2005*, August 2006, at *www.ncix.gov/publications/reports/fecie_all/FECIE_2005.pdf* (January 28, 2008).
2. *Ibid.*, p. 8.
3. *Ibid.*, p. 2.
4. Bill Gertz, "China's Spies 'Very Aggressive' Threat to U.S.," *The Washington Times*, March 6, 2007, p. A3.
5. U.S.–China Economic and Security Review Commission, *2007 Report to Congress*, November 2007, p. 7, at *www.uscc.gov/annual_report/2007/07_annual_report.php* (January 28, 2008) (emphasis added).
6. For a comprehensive account, see Ethan Gutmann, *Losing the New China: A Story of American Commerce, Desire and Betrayal* (San Francisco: Encounter Books, 2004), pp. 127–173.
7. China's first national survey on the Internet showed 820,000 Internet subscribers by the end of March 1998. "Survey Reveals Information on China's Internet Users," Xinhua News Agency (Beijing), May 27, 1998.
8. Gutmann, *Losing the New China*, p. 130.
9. "Hacker Tracked," *South China Morning Post* (Hong Kong), August 7, 1998.
10. Wang Mingyi, "Dalu zhixing 'Jin Dun Gongcheng,' Jiankong Quanmin; Chengshi mi bu dianzi shiqi" (Mainland implements Golden Shield Project to monitor entire population; cities deploy secret visual surveillance equipment), *Zhongguo Shibao* (Taipei), August 17, 2007, at *http://news.chinatimes.com/2007Cti/2007Cti-News/2007Cti-News-Print/0,4634,110505x112007081700097,00.html* (January 28, 2008); "Xuni Jingcha wangshang zhan gang" (Virtual cyberpolice take up posts on Internet), *Shijie Ribao* (New York), May 6, 2007, at *www.worldjournal.com/wj-ch-news.php?nt_seq_id=1527632* (January 28, 2008); and Reuters, "China Netizen Population Leaps to 137 mln-govt ctr," *The Washington Post*, January 23, 2007, at *www.washingtonpost.com/wp-dyn/content/article/2007/01/23/AR2007012300199.html* (January 28, 2008). Recently, at the World Economic Forum, Wang Jianzhou, chief executive officer of China MobileCom, said, "We know who you are, but also where you are." Agence France-Presse, "China Mobile Stuns Davos Forum with Private Data Claims," *Taipei Times*, January 28, 2008, p. 10, at *www.taipeitimes.com/News/worldbiz/archives/2008/01/28/2003399233* (February 1, 2008).
11. Zhou Ye, "Jiefangjun Zixunhua budui jinnian chengjun" (PLA cyberwarfare units deployed this year), *Zhongguo Shibao*, March 15, 2003.

defense white paper states the PLA's intention to "basically reach the strategic goal of building informationized armed forces and being capable of winning informationized wars by the mid-21st century."[12]

PLA cyberwarfare units are both active and highly sophisticated. They are apparently the only PLA units that regularly target enemy military assets in the course of their duties. New PLA doctrine sees computer network operations as a force multiplier in any confrontation[13] with the United States and other potential adversaries, including Taiwan, Japan, and South Korea as well as Canada, France, Germany, and the United Kingdom.[14]

No Ordinary Hackers

The first public indication that PLA cyberwarriors had achieved initial operational capability came on November 1, 2004, Beijing time. As *Time* magazine melodramatically set the scene, on that day, PLA cyberwarfare troops "sat down at computers in southern China and set off once again on their daily hunt for U.S. secrets."[15] Pentagon computer security investigators had monitored their operations since 2003, when the unit began their attacks on U.S. government networks as part of an information operation that U.S. investigators have codenamed Titan Rain.

Using a simple but elegantly modified "scanner program," the PLA's Titan Rain cyberwarriors identified network vulnerabilities in scores of Pentagon systems, including the critically important computers at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona; Defense Information Systems Agency in Arlington, Virginia; Naval Ocean Systems Center in San Diego, California; and Army Space and Strategic Defense Command in Huntsville, Alabama. The attacks were traced to a network in China's Guangdong Province, and the software and hacking techniques, according to one expert, identified it as a professional military operation. The hackers "were in and out with no keystroke errors and left no fingerprints, and created a backdoor in less than 30 minutes. How can this be done by anyone other than a military organization?"[16]

Are the Titan Rain attacks military operations run by the PLA or purely espionage collection efforts by the Ministry of State Security, China's civilian spy agency? One need only ask who benefits from penetrating the vast range of U.S. military targets. Chinese military doctrine discusses the importance of penetrating an adversary's military logistics and personnel networks. Furthermore, the multiple intrusions into what nuisance and criminal hackers would regard as boring, mundane networks—networks that do not offer the treasure trove of credit card numbers, bank accounts, and identity data that criminal hackers typically seek—suggest a military purpose.[17] The attacks yielded a

12. People's Republic of China, *China's National Defense in 2006*, Sect. II, at *www.china.org.cn/english/features/book/194485.htm* (January 28, 2008).
13. For an overview of China's cyberwar strategies, see James C. Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency," testimony before the U.S.–China Economic and Security Commission, September 15, 2005, at *www.uscc.gov/hearings/2005hearings/written_testimonies/05_09_15wrts/mulvenon_james.php* (January 28, 2008).
14. See Dow Jones Newswires, "Taiwan Military—China Cyber War More Likely Than Invasion," December 14, 2004; "Chinese Hacker May Be PLA," *Chosun Ilbo*, July 15, 2004; "NK Hands Suspected in Cyberattacks," *Korea Times*, July 15, 2004; Nautilus Institute, "ROK Cyberattacks," July 15, 2004, at *www.nautilus.org/napsnet/dr/0407/JUL1504.html#item13* (January 28, 2008). See also Andrew Ward, "China Blamed for Cyber Sabotage in S Korea," *Financial Times*, May 3, 2005, at *http://news.ft.com/cms/s/d7ac166e-bc0a-11d9-817e-00000e2511c8.html* (January 28, 2008), and CNET News, "Flaw in Microsoft Word Used in Computer Attack," *The New York Times*, May 20, 2006, at *www.nytimes.com/2006/05/20/technology/20zero.html* (January 28, 2008).
15. Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, August 25, 2005, at *www.time.com/time/nation/printout/0,8816,1098371,00.html* (January 28, 2008).
16. Allan Paller, Research Director, SANS Institute, quoted in Bill Brenner, "Titan Rain Shows Need for Better Training," SearchSecurity.com, December 13, 2005, at *http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1151715,00.html* (January 28, 2008), and Bradley Graham, "Hackers Attack Via Chinese Web Sites; U.S. Agencies' Networks Are Among Targets," *The Washington Post*, August 25, 2005, p. A1, at *www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html* (January 28, 2008).

"substantial amount of reconnaissance" that would help the attackers to "map out" U.S. military telecommunications networks and "to understand who is talking to whom, and what means [we] are using to communicate."[18]

However, this does not mean that the PLA is the only Chinese organization that is engaged in widespread cyberpenetrations of U.S. and global networks. General James E. Cartwright, commander of U.S. Strategic Command, testified before the USCC that "China is actively engaging in cyber reconnaissance by probing the computer networks of U.S. government agencies as well as private companies."[19]

> When you do that type of activity, the opportunity to start to understand where the intellectual capital of a nation is and what it has put together to give you the chance to potentially skip generations in your R&D efforts—this is not just military—this goes across the commercial sectors, et cetera is usually availed.
>
> For us, we generally think about things in terms of—and I'm talking about military—as a threshold is the law of armed conflict. As long as you're willing to stay below that, you are probing around, you are looking for opportunity, you may stumble across opportunity, probably some of it [is] serendipity when you're talking information operations. In fact, probably a large part of it is, but the idea is to get an understanding of the neighborhood.
>
> The better you understand it, the more likely you are to be able to use that to your advantage should there be a conflict between us.[20]

General Cartwright's words are a reminder that the tools of cyberspace are both weapons of war and channels of intelligence gathering and industrial espionage.

Software Skeleton Keys

People's Liberation Army cyberwarfare units now have the source codes for America's ubiquitous office software, which Microsoft provided to the Chinese government as a condition of doing business in China. This means that they essentially have a skeleton key to almost every networked government, military, business, and private computer in America. But Chinese government hackers do not restrict their operations to U.S. targets.

United Kingdom. Throughout December 2005, British Parliament offices were surreptitiously penetrated, also from computers using the Guangdong network. Britain's National Infrastructure Security Coordination Center investigators told reporters, "These were not normal hackers.… The degree of sophistication was extremely high. They were very clever programmers." Some of the attacks targeted files in British government offices that deal with human rights issues—"a very odd target," noted one U.K. security official,[21] unless the hackers had been tasked by the Chinese government.

The hackers used highly sophisticated software and had authorization to develop Web sites in China. The hackers sent Trojan horse[22] e-mails

17. I am indebted to Dr. James Mulvenon for these insights. He made these points at a Heritage Foundation panel discussion on October 15, 2007. The Heritage Foundation, "Evaluating the National Security Risk of Chinese Investment," panel discussion, October 15, 2007, at *http://multimedia.heritage.org/mp3/Lehrman-101507b.mp3* (January 28, 2008). See also Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency."
18. See General James E. Cartwright, in hearing, *China's Military Modernization and Its Impact on the United States and the Asia–Pacific*, U.S.–China Economic and Security Review Commission, 110th Cong, 1st Sess., March 29–30, 2007, p. 90, at *www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf* (January 28, 2008).
19. *Ibid.*, p. 7.
20. *Ibid.* p. 91.
21. Peter Warren, "Smash and Grab, the Hi-Tech Way," *The Guardian* (London), January 19, 2006, at *http://technology.guardian.co.uk/weekly/story/0,,1689093,00.html* (January 28, 2008).
22. Trojan horse programs, or "Trojans," are "seemingly benign programs that attack computer systems from within." McAfee, Inc., "A Brief History of Malware: An Educational Note for Service Providers," *White Paper*, October 2005, p. 5, at *www.mcafee.com/us/local_content/white_papers/partners/ds_wp_telconote.pdf* (January 29, 2008).

directing the recipients to the Web sites, which then corrupted the recipients' browsers. As one British network security expert observed, "Whoever is doing this is well-funded…. [I]t costs money to be able to mount an operation of this complexity."[23]

The Trojan e-mail attacks targeted specific victims. "One email was targeted at one company in aviation. It was a Word document that had a Math/cad component. If you did not have math/cad on your computer it would not open," said one expert. "The point was to find documents that had been written in that particular program and then send them back."[24] PLA cyberpenetrations of Japanese organizations used Microsoft "zero-day" vulnerabilities.[25]

The PLA cyberwarfare units undoubtedly discovered many of these vulnerabilities in key global operating systems and business programs after they reportedly gained full access to Microsoft source codes via the Chinese State Planning Commission.[26] The commission had alleged that Microsoft's Windows operating systems were a "secret tool of the U.S. government" and obliged Microsoft to instruct Chinese software engineers on inserting their own software into Window's applications.[27]

Taiwan. According to an official of Taiwan's Ministry of National Defense, in 2006, Taiwan detected 13 PLA zero-day attacks launched within Microsoft applications and experienced a total of 178 days of vulnerability between notifying Microsoft of the attacks and receiving the appropriate patches. One PowerPoint-based attack was so sophisticated that it took Microsoft engineers over two months to construct a patch.[28] In spring 2006, a certain foreign "coast guard agency" discovered a covert program imbedded in its network that systematically searched for shipping schedules and then forwarded them to an e-mail address in China.[29]

United States. After the Titan Rain attacks, the Pentagon shored up its cyberdefenses somewhat, but other U.S. government agencies remained lackadaisical.[30] In 2006, Chinese intelligence agencies covertly attacked at least four separate U.S. government computer networks.

Sometime in the spring of 2006, State Department computers were shut down after software "backdoors" were discovered in the department's unclassified networks. Chinese hackers were using the backdoors to siphon off sensitive data dealing with China and North Korea.[31] It was later reported that hackers had penetrated the State Department by exploiting a zero-day flaw in Microsoft software.[32] In connection with this discovery, congressional pressure obliged the State Department to discontinue purchasing computers from Lenovo,

23. *Ibid.*
24. *Ibid.*
25. A zero-day vulnerability is a generally known vulnerability for which a patch does not yet exist.
26. Lian Junwei, "Weiruan chengnuo yu Zhonggong xiang yuanshima" (Microsoft commits to giving source codes to PRC), *Gongshang Shibao* (Taipei), July 18, 2002.
27. David Kirkpatrick, "How Microsoft Conquered China," CNNMoney, July 23, 2007, at *http://money.cnn.com/magazines/fortune/fortune_archive/2007/07/23/100134488* (January 28, 2008).
28. Major General Huei-Jane Tschai, "Information Assurance Challenge and Readiness," presentation at the U.S.–Taiwan Defense Industry Conference, Annapolis, Md., September 11, 2007, p. 14.
29. John Markoff, "Attack of the Zombie Computers Is Growing Threat, Experts Say," *The New York Times*, January 7, 2007, at *www.nytimes.com/2007/01/07/technology/07net.html* (January 28, 2008).
30. See Gregory C. Wilshusen and Keith A. Rhodes, "Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program," GAO–07–1003T, testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, U.S. House of Representatives, June 20, 2007, at *www.gao.gov/new.items/d071003t.pdf* (January 28, 2008); U.S. Government Accountability Office, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO–07–837, July 27, 2007, at *www.gao.gov/new.items/d07837.pdf* (January 28, 2008); Dawn S. Onley and Patience Wait, "Red Storm Rising," *Government Computer News*, August 21, 2006, at *www.gcn.com/print/25_25/41716-1.html* (January 28, 2008).
31. Ted Bridis, "State Dept. Suffers Computer Break-Ins," Associated Press, July 11, 2006.
32. Ted Bridis, "State Department Got Mail—and Hackers," Associated Press, April 18, 2007.

the Chinese firm that acquired IBM's personal computer division in 2005.[33]

In July 2006, overseas hackers operating from Chinese Internet servers penetrated computers in the Department of Commerce's Bureau of Industry and Security (BIS), which manages export licensing of military-use products and information. "Through established security procedures, BIS discovered a targeted effort to gain access to BIS user accounts," according to a Commerce Department spokesman, and Commerce officials admitted privately that Chinese hackers had implanted covert "rootkit" programs to mask their presence and enable them to gain privileged access to the computer system. When the damage was assessed, said one unnamed official, the agency's information security officers determined that the workstations could not be salvaged and instead spent several million dollars to build an entirely new system with "clean hardware and clean software."[34]

In mid-November, computer security officials determined that Chinese military hackers had penetrated the unclassified computer network at the Naval War College in Rhode Island. Retired Air Force Major General Richard Goetze, a Naval War College professor, said the Chinese "took down" the entire Naval War College computer network—an operation that prompted the U.S. Strategic Command to raise the security alert level for the Pentagon's 12,000 computer networks and 5 million computers.[35]

At about the same time, in November–December 2006, computers at the National Defense University (NDU) in Washington, D.C., were also attacked. The NDU attack was unpublicized, although it was common knowledge in academic circles that NDU e-mail accounts had been shut down for weeks while the penetrated systems were replaced.[36]

2007: A Banner Year for Chinese Cyber-Espionage

In 2007, a new spate of media reports of very sophisticated cyberattacks against U.S. and European government targets sparked renewed interest in China's military cyberwarfare capacity. In June, 150 computers in the $1.75 billion computer network at the Department of Homeland Security (DHS)—guardian of the nation's critical cyberinfrastructure—were quietly penetrated with programs that sent an unknown quantity of information to a Chinese-language Web site. Unisys Corporation, the manager of the DHS computers, allegedly covered up the penetration for three months.[37]

In June 2007, Chinese military hackers circumvented the Defense Department's Titan Rain patches, again hitting a Pentagon network in the "most successful cyber attack against the US defense department," according to the Financial Times. The newspaper cited a source who said that there was a "very high level of confidence…*trending towards total certainty*" that the Chinese army was behind the attack.[38]

In July, the State Department's unclassified computer system suffered "large-scale network breakins affecting operations worldwide,"[39] which were also attributed to the Chinese military.[40]

33. Agence France-Presse, "U.S. Pulls Lenovo PCs from State Department," May 19, 2006, and Associated Press, "U.S. to Restrict Use of Computers from Lenovo," *The New York Times*, May 20, 2006, at *www.nytimes.com/2006/05/20/business/20computer.html* (January 28, 2008).
34. Alan Sipress, "Computer System Under Attack," *The Washington Post*, October 6, 2006, p. A21, at *www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501781.html* (January 28, 2008).
35. Bill Gertz, "Chinese Hackers Prompt Navy College Site Closure," *The Washington Times*, November 30, 2006, p. A11.
36. Private conversations with students and instructors at the National Defense University.
37. Ellen Nakashima and Brian Krebs, "Contractor Blamed in DHS Data Breaches," *The Washington Post*, September 24, 2007, p. A1, at *www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html* (January 28, 2008). See also Bill Gertz and Rowan Scarborough, "NDU Hacked," *The Washington Times*, January 12, 2007, p. A11, at *www.gertzfile.com/gertzfile/ring011207.html* (January 28, 2008).
38. Demetri Sevastopulo and Richard McGregor, "China 'Hacked' into Pentagon Defence System," *Financial Times*, September 4, 2007, p. 1, at *www.ft.com/cms/s/0/4f25940e-5a7e-11dc-9bcd-0000779fd2ac.html* (January 28, 2008) (emphasis added).
39. Anita Chang, "China Denies Hacking Pentagon Computers," Associated Press, September 4, 2007.
40. Sevastopulo and McGregor, "China 'Hacked' into Pentagon Defence System."

The *Financial Times* also noted that "the White House had created a team of experts to consider whether the administration needed to restrict the use of Blackberrys because of concerns about cyber espionage."[41] The vulnerability of networked PDAs is not theoretical. In October 2007, Dr. Brenner commented to a group of intelligence professionals, "This week I learned of another smart guy who, after taking his PDA to a *foreign country well known for cyber intrusions*, synched it up to his agency's networks." Brenner calculated flatly that "the risk that he has infected his agency's servers with a 'phone home' vulnerability approaches 100%."[42]

In May 2007, Canada's intelligence chief told the Canadian Senate that "China is at the top of our list of counter-intelligence targets and accounts for close to 50 percent of our counter-intelligence program."[43]

In August 2007, *Der Spiegel* reported that German security agencies had discovered that computers in Chancellor Angela Merkel's *Bundeskanzleramt* and three ministries had been infected with Trojans, which had been inserted by hackers associated with the Chinese espionage programs.[44] Two days later, a poker-faced Chinese Premier Wen Jiabao promised to help track down the perpetrators when Chancellor Merkel confronted him with the matter.[45]

A few days later, Chinese cyberattacks hit computers at Britain's Parliament and Foreign Office.[46] On September 8, 2007, French Secretary-General for National Defense Francis Delon confirmed that "our information systems were the object of attacks, like in the other countries." Delon wryly noted, "We have proof there is involvement with China" but declined to say who in China was actually involved.[47] Government offices in Australia and New Zealand were also reportedly hit by Chinese hackers in September.[48] Chinese cyberspies apparently leave very few countries untouched.

Beware Chinese Bearing Gifts

No one should be comforted by the fact that some Chinese cyberattacks have been identified. While PLA cyberwarfare units devoutly wish to avoid detection, they also seek to give a false sense of security that all network penetrations can be detected.

One expert told a conference of federal information managers last year that "the Chinese are in half of your agencies' systems."[49] U.S. Defense Department sources say privately that the level of Chinese cyberattacks obliges them to avoid Chinese-origin hardware and software in all classified systems and as many unclassified systems as fiscally possible. The high threat of Chinese cyberpenetrations into U.S. defense networks will be magnified as the Pentagon increasingly loses domestic sources of "trusted and classified" microchips.

41. *Ibid.*
42. Joel F. Brenner, "Strategic Counterintelligence: Protecting America in the 21st Century," remarks at NRO/National Military Intelligence Association Counterintelligence Symposium, Washington, D.C., October 24, 2007, at *www.ncix.gov/publications/speeches/NRO-NMIA-CI-Symposium-24-Oct-07.pdf* (January 28, 2008) (emphasis added).
43. FOCUS News Agency, "China Is Biggest Espionage Threat to Canada: Spy Chief," May 1, 2007, at w*ww.focus-fen.net/index.php?id=n111309* (January 28, 2008).
44. "Chinesische Trojaner auf PCs im Kanzleramt" (Chinese Trojans in Chancellor Office PCs), *Der Spiegel*, August 25, 2007, at *www.spiegel.de/netzwelt/tech/0,1518,501954,00.html* (January 28, 2008).
45. John Blau, "German Gov't PCs Hacked, China Offers to Investigate," *The Washington Post*, August 27, 2007, at *www.washingtonpost.com/wp-dyn/content/article/2007/08/27/AR2007082700595.html* (January 28, 2008). See also Christopher Bodeen, "Merkel; China Must Respect 'Game Rules,'" *The Washington Post*, August 27, 2007, at *www.washingtonpost.com/wp-dyn/content/article/2007/08/27/AR2007082700790.html* (January 28, 2008).
46. Chang, "China Denies Hacking Pentagon Computers."
47. Agence France-Presse, "Now France Comes Under Attack from PRC Hackers," *Taipei Times*, September 9, 2007, p. 1, at *www.taipeitimes.com/News/front/archives/2007/09/09/2003377917* (January 28, 2008).
48. Asia Pacific News.Net, "ANI—Chinese Tried to Hack Australian Government PCs Too," September 12, 2007, at *www.asiapacificnews.net/story/281493* (January 28, 2008).
49. Mark A. Kellner, "China a 'Latent Threat, Potential Enemy': Expert," *Defense News*, December 4, 2006, at *www.defensenews.com/story.php?F=2389588* (January 28, 2008).

In a February 2005 report, the Defense Science Board warned that "a significant migration of critical microelectronics manufacturing from the United States to other foreign countries has [occurred] and will continue to occur." The strategic significance of this phenomenon cannot be overstated, because this technology is the foundation of America's ability to maintain its technological advantages in the military, government, commercial, and industrial sectors. Indeed, microelectronics supplies for defense, national infrastructure, and intelligence applications are now in peril.[50]

This is a critical national security issue because America's defense-critical electronics demand "trusted and classified" microchips. The "confidence that classified or mission critical information contained in chip designs is not compromised, reliability is not degraded, or untended design elements inserted in chips as a result of design or fabrication in conditions open to adversary agents" simply does not exist in commercial off-the-shelf (COTS) microchips from overseas foundries. Furthermore, as the February 2005 report explained, "Trust cannot be added to integrated circuits after fabrication; electrical testing and reverse engineering cannot be relied upon to detect undesired alterations in military integrated circuits."[51]

Increasingly, China is the source of COTS microchips, and Chinese foundries and design shops have had direct network access to foundries in other countries, particularly Taiwan—a fact that has become a source of alarm to Taiwan's intelligence agencies.[52] Chinese microchip output increased an average of 37 percent annually between 2000 and 2007, giving China a 6 percent share of the world semiconductor market,[53] and China's semiconductor production capacity grew about 45 percent annually for 2006 and 2007,[54] which suggests that China will surpass the United States in output in five years.

Intel Corporation is reportedly building a $2.5 billion semiconductor wafer fabrication plant in Dalian, China.[55] At the same time, however:

> Manufacturing costs in China are [only] 10 percent lower than in the United States while manufacturing cost in Taiwan are 7 percent lower.
>
> Almost all of the manufacturing cost difference…is accounted for by labor costs….
>
> The composite cost data…does not support the hypothesis that…the current migration to China is due to lower construction and operating costs. Other factors, primarily the [Chinese] *government policies…are driving this*.[56]

The United States simply "no longer [has] a diverse base of U.S. integrated circuit fabricators capable of meeting trusted and classified chip needs."[57] The Defense Department's Trusted Foundry Program is a good start toward addressing

50. U.S. Department of Defense, Defense Science Board, *High Performance Microchip Supply*, February 2005, p. 1, at *www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf* (January 4, 2007).
51. *Ibid.*, p. 17 (emphasis removed).
52. Jimmy Chuang, "Ex-TSMC Employee Suspected of Selling Secrets to Shanghai," *Taipei Times*, March 7, 2002, p. 1, at *www.taipeitimes.com/news/2002/03/07/story/0000126662* (January 28, 2008). See also Stephanie Low, "Government Drafts Law to Fight High-Tech Espionage," *Taipei Times*, March 31, 2002, p. 1, at *www.taipeitimes.com/news/2002/03/31/story/0000129898* (January 28, 2008), and Dan Nystedt, "Top Secret Report Sets Off Alarms in the Tech Sector," *Taipei Times*, July 4, 2001, p. 17, at *www.taipeitimes.com/News/biz/archives/2001/07/04/92739* (January 28, 2008).
53. Jia Yuankun, "Zhuanjia: Zhongguo bandaoti xinpian channeng zengsu ju quanqiu zhishou" (Expert: China's semiconductor wafer production capacity growth leads the globe), Xinhua News Agency, November 25, 2007, at *http://news.sd.cninfo.net/jrgz/319328.shtml* (January 28, 2008). In 2007, Taiwan accounted for 18 percent of global microchip production, second only to Japan with 24 percent. South Korea and the United States were tied at 17 percent. "Taiwan to Overtake US As No. 2 Maker of Semiconductors," *Taipei Times*, October 29, 2007, p. 1, at *www.taipeitimes.com/News/front/archives/2007/10/29/2003385241* (January 28, 2008).
54. For a survey of global semiconductor trends, see Christian Gregor Dieseldorff, "Fab Spending Tapers in 2008," *Semiconductor International*, January 1, 2008, at *www.semiconductor.net/article/CA6515396.html* (January 31, 2008).
55. Jason Dean and Don Clark, "China Clears Intel Chip Plant, Marking a Potential Milestone," *The Wall Street Journal*, March 14, 2007, p. A4, at *http://online.wsj.com/article/SB117377461012135302.html* (January 28, 2008), and Joe McDonald, "Rising Tech Power: Dalian, China," Associated Press, November 23, 2007.

near-term needs, but it does not address the long-term threat posed by a diminishing domestic capacity to supply critical systems for classified needs.

The 3Com–Huawei–H3C Nexus

Huawei Shenzhen Technology Company—China's top networking services, equipment, and supply corporation—is a prototypical PLA protégé firm. It was founded in 1988 by Ren Zhengfei, a former director of the PLA General Staff Department's Information Engineering Academy, which is responsible for telecommunications research in the Chinese military. According to a RAND Corporation study, "Huawei maintains deep ties with the Chinese military, which serves as a multi-faceted role as an important customer, as well as Huawei's political patron and research and development partner."[58]

Huawei's Dubious Reputation. The extremely close links between Huawei and the PLA mean that the People's Liberation Army has direct access to Huawei's training and technology infrastructure. The cyberwar units trained in this environment are now among the world's experts in the military applications of network communications and coding.

In 2003, Huawei was charged with stealing corporate secrets from U.S. counterpart Cisco Systems and wholesale pirating of Cisco's software—"even the software 'bugs,' or glitches, and misspellings matched."[59] With such a dubious reputation, one might think that Huawei would be persona non grata among American telecommunications firms, yet a few months later, 3Com established a joint venture with Huawei to manufacture and distribute routers in Asia.

The Problem. If a PLA protégé firm acquired an American firm that provided computer network equipment, software, and services to the U.S. government, the possibilities for cyber-espionage would be virtually unlimited. On September 28, 2007, Huawei Technology announced its intention to participate in a Bain Capital Partners' corporate buyout of 3Com, one of Huawei's top U.S. counterparts.[60]

This is a problem. 3Com is an important vendor of computer security software, routers, and servers to the U.S. government,[61] and several U.S. Senators say that the company is apparently a vendor to the U.S. Department of Defense.[62] How 3Com got into this predicament is complicated.

3Com, like many other U.S. high-tech firms, suffered losses during the U.S. stock market technology slump that began in 2001, and it looked for export opportunities in China. In 2003, in an attempt to penetrate the China market, 3Com sought out a top Chinese information technology firm with close ties to the government to help it break through government restrictions on telecoms and IT investments. Fatefully, 3Com partnered with Huawei Technology, a company that was being sued by Cisco Systems, one of 3Com's major competitors in the United States.[63]

In May 2003, faced with a ban on doing business in the United States because of vast intellectual property theft from Cisco, Huawei voluntarily with-

56. Thomas R. Howell, Brent L. Bartlett, William A. Noellert, and Rachel Howe, *China's Emerging Semiconductor Industry*, Semiconductor Industry Association, October 2003, Appendix 2, p. 3, at *www.sia-online.org/downloads/SIA_China_Study_2003.pdf* (January 29, 2008) (emphasis added). See also U.S. Department of Defense, *High Performance Microchip Supply*, p. 30.
57. U.S. Department of Defense, *High Performance Microchip Supply*, p. 36.
58. See also Evan S. Medeiros, Roger Cliff, Keith Crane, and James C. Mulvenon, *A New Direction for China's Defense Industry*, RAND Corporation, 2005, p. 218, at *www.rand.org/pubs/monographs/2005/RAND_MG334.pdf* (April 11, 2006).
59. Scott Thurm, "Cisco Ran Sting Operation to Nab a Copycat in China," *The Wall Street Journal*, April 4, 2003.
60. Press release, "3Com Announces Agreement to Be Acquired by Bain Capital Partners for $5.30 Per Share in Cash," 3Com, September 28, 2007, at *www.3com.com/corpinfo/en_US/pressbox/press_release.jsp?INFO_ID=267061*(January 28, 2008).
61. See 3Com, "Federal Government Solutions," Web page, at *www.3com.com/solutions/en_US/government/index.html* (January 28, 2008).
62. "3Com is one of the few manufacturers of computer networking hardware but is also involved in numerous U.S. government technology contracts." Senator Jon Kyl (R–AZ) *et al.*, letter to Robert Kimmit, Deputy Secretary of the Treasury, October 19, 2007.
63. Scott Thurm, "China's Huawei, 3Com to Form Venture to Compete with Cisco," *The Wall Street Journal*, March 20, 2003.

drew from the U.S. market.[64] 3Com would have been well aware of highly publicized charges against its new Chinese partner because Huawei was being sued at the time for stealing corporate secrets.[65] However, 3Com formed H3C, a Chinese joint venture with Huawei, paying $160 million to Huawei to capitalize the joint venture in return for a 49 percent share. 3Com later paid Huawei $28 million for 2 percent of H3C's shares,[66] giving 3Com controlling interest in H3C. "Controlling," however, is an imprecise term. Aside from two non-Chinese executives in H3C, the joint venture remained a Chinese entity staffed entirely by Huawei employees.

On November 29, 2006, 3Com reportedly bought out Huawei's 49 percent interest in H3C for $882 million, making H3C a wholly owned 3Com subsidiary.[67] Altogether, 3Com paid Huawei $1.26 billion for H3C.

Yet details of the Huawei–3Com joint venture posted on China Computer World, a Chinese computer news Web site, indicate that every one of H3C's Chinese employees remains on Huawei's personnel rolls, even though Huawei no longer owns any H3C shares. "They retain Huawei personnel employment numbers, Huawei stock ownership, and their internal corporate contacts, job descriptions (*zhiwei*) and ranks."[68] Therefore, Huawei likely continues to maintain all security dossiers and to control "work certificates" (*gongzuo zheng*) for all of H3C's Chinese citizen employees.

The 3Com–Huawei joint venture naturally raised suspicions because the Chinese military regularly penetrates U.S. national security agencies' computer systems. Huawei is now moving to buy a significant share of 3Com, initially paying $363 million for a 16.5 percent share via a major U.S. mergers and acquisitions firm. It is reasonable to speculate that Huawei intends eventually to take full control of 3Com, primarily as a vehicle for introducing Huawei's products into the U.S. market and incidentally giving China's telecoms access to American communications networks.[69]

The irony is that 3Com paid Huawei $1.26 billion over the past four years for the privilege of having Huawei as partner in China. Now Huawei hopes to buy a slice of 3Com for $363 million.

India and Huawei. Unlike the United States, other countries are more leery of cooperation with China in the area of telecommunications. India has kept Huawei at arm's length despite Chinese President Hu Jintao's personal intercession with Indian Prime Minister Manmohan Singh to permit the Chinese telecoms firm to expand its marketing in India.[70]

Intelligence agency concerns about Chinese cyberespionage prompted India to shelve a planned $60 million Huawei investment in its telecom in 2005. Although using Chinese equipment would be substantially less expensive than using domestic systems, India's Defense Ministry has warned that inadequate safeguards would also make strategic networks vulnerable to Chinese infiltration and manipulation. The choice was "between cheap Chinese equipment and national security."[71] India's intelligence services also noted that Huawei "has been responsible for sweeping and debugging oper-

64. Scott Thurm, "Cisco Ran Sting Operation to Nab a Copycat in China," and "Court Papers Show Huawei Tried to Hire Cisco Engineers," *The Wall Street Journal*, March 17, 2003.

65. Thurm, "China's Huawei, 3Com to Form Venture to Compete with Cisco."

66. Qiu Huihui, "Zheng Shusheng: Huawei 3Com zuizhong yao zili menhu" (Zheng Shusheng: H3C will ultimately become an independent firm), *21 Shiji Jingji Baodao* (Guangzhou), November 14, 2005, at *www.nanfangdaily.com.cn/jj/20051114/it/200511140074.asp* (January 28, 2008).

67. See Yong Zhongwei, "Huawei 3Com Gu Dan Shang Lu" (Huawei and 3Com go their separate ways), *Zhongguo Shiji Wang*, December 11, 2006, at *www.ccw.com.cn/netprod/dp/htm2006/20061211_228831.shtml* (January 28, 2008).

68. *Ibid.*

69. For more on this, see The Heritage Foundation, "Evaluating the National Security Risk of Chinese Investment," and Wang Tao, "Huawei de 3COM miti; Beimei Sike yexu cai shi daan" (Huawei's ulterior 3COM motive; North America CISCO is probably the answer), *Tongxun Shijie Wang* (Beijing), October 1, 2007, at *www.cww.net.cn/TComment/html/2007/10/1/20071012111128909.htm* (January 28, 2008).

70. Saritha Rai, "India and China Work on Building Trust," *The New York Times*, November 22, 2006, at *www.nytimes.com/2006/11/22/business/worldbusiness/22asia.html* (January 28, 2008).

ations in the Chinese embassy. In view of China's focus on cyber warfare there is a risk of exposing our strategic telecom network to the Chinese."[72]

Lessons Not Yet Learned

While the U.S. government is very reticent about the vulnerabilities of its databases to Chinese penetration, the known penetrations in 2007 alone show how widespread Chinese cyberattacks have become. Chinese PLA cyberwarfare units have already penetrated the Pentagon's unclassified NIPRNet (Unclassified but Sensitive Internet Protocol Router Network) and have designed software to disable it in time of conflict or confrontation.[73] Indeed, Major General William Lord, Director of Information, Services and Integration in the Air Force's Office of Warfighting Integration admitted that "China has downloaded 10 to 20 terabytes of data from the NIPRNet already" and added, "There is a nation-state threat by the Chinese."[74]

Richard Lawless, then Deputy Under Secretary of Defense for Asia–Pacific affairs, told a congressional committee on June 13, 2007, that the Chinese are "leveraging information technology expertise available in China's booming economy to make significant strides in cyber-warfare." Lawless noted that the Chinese military's "determination to familiarize themselves with and dominate to some degree the Internet capabilities—not only of China and that region of the world—provide them with a growing and very impressive capability that we are very mindful of and are spending a lot of time watching."[75]

Lawless further testified that:

> [The Chinese] have developed a very sophisticated, broadly-based capability to degrade and—attack and degrade our computer systems and our Internet systems. I mean, the fact that computer access, warfare and the…disruptive things that that allows you to do to an opponent are well appreciated by the Chinese and they spend a lot of time figuring out how to disrupt our networks—how to both penetrate networks, in terms of gleaning or gaining information that is protected, as well as computer network attack programs which would allow them to shut down critical systems at times of contingency. So first of all, the capability is there. They're growing it; they see it as a major component of their asymmetric warfare capability.[76]

PLA cyberwarfare units' access to source codes for America's ubiquitous office software means that the PLA essentially has a skeleton key to every government, military, business, and private computer in America that is accessible through the Internet. General Cartwright has warned, "I think that we should start to consider that 'regret factors' associated with a cyber attack could, in fact, be in the magnitude of a weapon of mass destruction."[77]

A well-planned and well-executed Chinese cyberattack could do significant damage to the U.S. economy, telecommunications, electric power transmission, financial data, and other vital infrastructure—damage equal to or exceeding the effects of the 9/11 terrorist attacks, conceivably even causing significant loss of life. After such a cyberattack, even if no one was killed, "regret" would be an understatement.

What the Administration and Congress Should Do

Recent cyberattacks on the United States and its allies combined with warnings from the Defense Science Board and the U.S.–China Economic and Security Review Commission emphasize the seri-

71. Navika Kumar, "Chinese Firm Gets a RAW deal," *The Times of India*, August 16, 2005, at *http://timesofindia.indiatimes.com/articleshow/1201359.cms* (January 28, 2008).
72. *Ibid.*
73. Mulvenon, "Chinese Information Operations Strategies in a Taiwan Contingency."
74. Onley and Wait, "Red Storm Rising."
75. Richard P. Lawless, in hearing, *Recent Security Developments in China*, Committee on Armed Services, U.S. House of Representatives, 110th Cong., 1st Sess., June 13, 2007, transcript from Federal News Service.
76. *Ibid.*
77. General James E. Cartwright, in hearing, *China's Military Modernization and Its Impact on the United States and the Asia–Pacific*, p. 7.

ousness of this growing threat to U.S. national security. To address this threat, the Administration and Congress should:

- **Identify China as an intelligence risk.** The Administration has been too timid in highlighting the espionage challenge from China. This failure to say that "China is our biggest intelligence problem" leads U.S. businesses and academies to assume incorrectly that they face no greater risk from Chinese penetrations than they face from any other country. The Office of the National Counterintelligence Executive, the Department of Justice, and the FBI should follow the USCC's lead and identify China as the *top* spy threat. Congress should hold public hearings on the problem primarily to educate the public, but also to gather important data for legislation.
- **Address the legal impediments to criminal prosecution of cyberspies.** Current U.S. criminal laws are vague about assisting unknown foreign actors to penetrate secure networks for information-gathering purposes. They are insufficient to prosecute other penetrations in which the purposes behind embedded Trojan horse programs are unclear.
- **Closely examine Chinese commercial investments in cyber companies.** The Treasury Department's Committee on Foreign Investment in the United States should closely examine any attempt by Chinese military or intelligence agencies to gain access to U.S. cybertechnology operations via commercial investments.
- **Require software companies to patch vulnerabilities quickly.** Software companies frequently seem to consider cyberpenetrations that involve no disruption of service as tolerable nuisances, not as immediate crises. Software firms should be required to give first priority to the most critical vulnerabilities and should coordinate with U.S. government cybersecurity offices in identifying, assessing the risks from, and patching and/or mitigating vulnerabilities.
- **Require "trustworthiness" in critical IT systems.** Components for defense-critical IT systems—from chips to storage devices—must come only from trusted and certified firms. Congress must address the disappearance of an industrial capacity to manufacture trusted IT equipment for defense needs over the long term, both by mandating "trustworthiness" for U.S. information systems—i.e., that defense-critical microcircuits be 100 percent designed, fabricated, packaged, and tested in the United States under secure conditions—and by providing adequate funding, personnel, and resources for compliance and oversight.
- **Strengthen America's engineering and scientific competitiveness.** In February 2005, the Defense Science Board made a number of recommendations to address this crisis, including the expansion of America's electrical engineering and scientific talent pool. At a minimum, Congress should offer "national service" incentives, including scholarships and internships, to students in the information science and technology fields and should require an ROTC-type commitment to national service in the IT industry as a condition of the academic grants.[78]

Congress should also urge the defense and intelligence agencies to leverage competition among the U.S. national laboratories as an ideal way to sustain peak innovation in IT research and development on highly classified systems. Just as the national laboratories competed with each other on scientific and engineering breakthroughs in developing nuclear weapons and tested each other's weapon designs, their competitive culture should be equally successful in designing and fabricating secure and trustworthy microchips.

Conclusion

America's vulnerability to cyberattacks is a critical threat to national security. If the Administration and Congress do not address these problems and implement the 2005 recommendations of the Defense Science Board, the fix will become prohibitively expensive and/or America's national security will be irreversibly compromised.

—John J. Tkacik, Jr., is Senior Research Fellow in China, Taiwan, and Mongolia Policy in the Asian Studies Center at The Heritage Foundation.

78. *Ibid.*, p. 38, Figure 5.