WebMemo
Published by The Heritage Foundation
No. 3242
May 5, 2011

China and Cybersecurity: Trojan Chips and U.S.–Chinese Relations

Dean Cheng and Derek Scissors

One subject of the third round of the U.S.–China Strategic and Economic Dialogue will be cybersecurity. Part of Secretary of Defense Robert Gates's proposed Strategic Security Dialogue, it reflects the growing prominence of cybersecurity in Sino-American strategic relations.

The concerns include computer network exploitation and computer network attacks, but also tampering with the physical infrastructure of communications and computer networks. Vulnerabilities could be introduced in the course of manufacturing equipment or created through purchase of malignant or counterfeit goods. Recent experience highlights these problems.

Such possibilities have brought calls for trade barriers, ranging from random entry-point inspections of various types of goods and equipment (e.g., chips and routers) to prohibition of some imports (e.g., communications hardware), especially from a major manufacturer, the People's Republic of China (PRC).

The trade proposals tend to be vague because the cyber threat itself, while real, is vaguely presented. While an ill-defined threat certainly bears watching, it does not justify protectionism. Cybersecurity is largely classified, but trade is not, and trade policy cannot be held hostage to cybersecurity unless specific dangers are put forward.

What Is the Threat? A longstanding fear has been that cyber attacks against the U.S. might result in disruptions to power, banking, and communications systems at a critical moment. The cyber attacks on Estonia and Georgia, which disrupted commerce and communications, raise the specter that the U.S. might undergo the equivalent of a cyber Pearl Harbor. Efforts by the Defense Advanced Research Projects Agency (DARPA) to improve verification capabilities highlight the limitations of current computer engineering skills in, for example, diagnosing cyber intrusions. Initial studies on the Trusted Integrated Circuit program, seeking to create a secure supply chain, were requested in 2007. As of late 2010, DARPA was still seeking new research proposals for determining whether a given chip was reliable, and whether it had been maliciously modified, as part of the Integrity and Reliability of Integrated Circuits (IRIS) program.[1]

A more recent worry is vulnerabilities "hardwired" into the physical infrastructure of the Internet. In the last several years, the FBI has warned that counterfeit computer parts and systems may be widespread.

This can manifest itself in two ways: fake parts and systems, which may fail at dangerously higher rates, or contaminated systems that might incorporate hardwired backdoors and other security problems, allowing a foreign power to subvert a system.[2] Similar problems have been identified by Ameri-

This paper, in its entirety, can be found at:
http://report.heritage.org/wm3242

Produced by the Asian Studies Center

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

can allies; the U.K. has identified counterfeit parts entering into its military supply chain.

Much cyber-related attention has been focused on the PRC. China is reportedly the source of many of the hacking efforts directed at U.S. military and security computer networks. Chinese computer infiltration has reputedly obtained access to such sensitive programs as F-35 design information. Such efforts as Titan Rain, Ghostnet, and others have reportedly attacked U.S. and other nations' information systems systematically and have infiltrated email servers and networks around the world. One example is the "Shadow network," which affected "social networking websites, webmail providers, free hosting providers and services from some of the largest companies."[3] Many have been traced back to the PRC—but attribution to any specific Chinese entity is extremely difficult.

A growing concern is that China can exploit its position as one of the world's largest producers of computer chips, motherboards, and other physical parts of the Internet to affect American and allied infrastructure. China has apparently already demonstrated an ability to tamper with Domain Name System (DNS) servers based in China, "effectively poisoning all DNS servers on the route."[4]

The fear is that they could now affect foreign-based routers. In this regard, the issue of Chinese counterfeit parts is compounded by uncertainty about whether fake parts are being introduced as part of a concerted intelligence campaign or simply the result of profiteering by local contractors.

Public Information Is Lacking

The arcane nature of the threat enhances uncertainty. Understanding the workings of computer viruses, patches, and the vulnerabilities of routers or microchips is difficult. Comprehending the intricacies of global supply chains and tracing the ultimate source of sub-systems and components can be equally difficult. Former NSA and CIA Director General Michael Hayden writes that "Rarely has something been so important and so talked about with less clarity and less apparent understanding."[5]

Several studies highlight some of the myriad vulnerabilities.

- The 2005 Defense Science Board Task Force on High Performance Microchip Supply identified the growing security problem of microchips being manufactured (and more and more often designed) outside the United States.
- The 2007 Defense Science Board Task Force on Mission Impact of Foreign Influence on DOD Software noted that software frequently incorporates pieces of code from a variety of sources, any of which might be a point of vulnerability.
- The 2008 National Defense Industrial Association's handbook "Engineering for System Assurance" provides a comprehensive overview of system assurance, which in turn highlights how difficult it can be to achieve it.
- Over-classification is also a problem. General Hayden notes that much of the information on cyber threats is "overprotected." Greg Garcia, head of the Bush Administration's efforts on cybersecurity, has similarly noted that "there was too much classified…Too much was kept secret."[6]

Leave Trade Alone

The ambiguity on the security side actually clarifies the trade side. If the cyber threat is understood

1. "Integrity and Reliability of Integrated Circuits (IRIS)," Federal Business Opportunity solicitation, at *https://www.fbo.gov/index?s=opportunity&mode=form&id=342ac5ed191ae7b8b03357fead590c4e&tab=core&_cview=1* (May 4, 2011).
2. Tom Espiner, "FBI Fears Hardware Backdoors in US Military Kit," ZDNet UK, May 14, 2008, at *http://www.zdnet.co.uk/news/security-threats/2008/05/14/fbi-fears-hardware-backdoors-in-us-military-kit-39417171/* (May 4, 2011).
3. Information Warfare Monitor, Shadowserver Foundation, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," April 6, 2010, p. 13.
4. Graham Lowe, Patrick Winters, and Michael Marcus, "The Great DNS Wall of China," at *http://cs.nyu.edu/~pcw216/work/nds/final.pdf* (May 4, 2011).
5. Michael V. Hayden, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), p. 3.
6. Hayden, "The Future of Things 'Cyber,'" p. 5, and Jill R. Aitoro, "Bush's Cyber Chief Calls National Security Initiative Too Secret," Nextgov, February 11, 2009, at *http://www.nextgov.com/nextgov/ng_20090211_6858.php* (May 5, 2011).

only tenuously, testing imported goods for cyber threats will be inadequate to identify compromised equipment. With ineffective testing, banning some importers would not be worthwhile. In a global economy, equipment will simply be re-routed. The U.S. does not have the resources necessary to track the true source of goods when dangerous items cannot be easily discovered—and discovery may even be impossible.

If the threat was well understood but national security argued against the disclosure of vital information, this at least suggests that the danger from trade is secondary to other dangers. America retains the option, of course, of simply restricting trade on national security grounds without disclosing its reasons. This would be unwise.

One drawback of restricting trade would be the costs incurred by the U.S. in terms of spending on import inspections and the loss of availability of certain goods. The defense community is often not well-positioned to anticipate the extent of these economic costs. People will not relinquish scarce resources voluntarily when the gains from doing so are not spelled out.

The second drawback is the reaction of American trade partners. American exports already suffer from undocumented national security justifications for protectionism. Were the U.S. to introduce a new set of potentially sweeping restrictions based on hidden national security requirements, the global trade environment would immediately and sharply deteriorate. Costs would be far higher than indicated by looking at American actions alone.

Balancing Economic and Security Responsibilities.

- ***Security.*** For policymakers and the public to properly comprehend the magnitude of the problem, the Department of Defense must be as transparent as possible. Some material will be classified. But the trade-off between security classification and the ability to promptly and adequately respond to a threat should be weighted more heavily to the transparency side than it is at present.
- ***Trade.*** The Department of Commerce and United States Trade Representative should restrict trade only in accordance with what can be defended publicly and systematically. Introduction of ad hoc trade restrictions that claim a classified basis will harm the American economy.

For now, it is unreasonable to impose considerable economic costs for the sake of a serious but vaguely presented threat.

*—**Dean Cheng** is Research Fellow in Chinese Political and Security Affairs and **Derek Scissors, Ph.D.**, is Research Fellow in Asia Economic Policy in the Asian Studies Center at The Heritage Foundation.*