Confrontation or Collaboration?

Congress and the Intelligence Community

Cyber Security and the Intelligence Community

Eric Rosenbach and Aki J. Peritz

HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Belfer Center
for Science and International Affairs

Cyber Security and the Intelligence Community

The United States information infrastructure, ranging from telecommunications to computer networks, is the foundation for much of the business, military and civilian activity that occurs daily throughout the country. Over the years, these systems have become increasingly complex and interconnected, and the tools and methods to attack our core information architecture—including critical national security systems—have multiplied as well. Hence, U.S. policymakers ought to pay increased attention to protecting, defending and responding to attacks on information systems and networks.

This memo provides members new members of Congress with an overview of cyber security and the potential areas in which the Intelligence Community (IC) can support the nation's cyber security efforts.

The Cyber Threat

The significance and potential impact of cyber threats to the United States has grown quickly over the past decade. Cyber attacks can potentially undermine:

- Information systems and military responses.
- Civilian and military aviation systems.
- Critical first-response systems, especially during times of crisis.
- Financial markets and the free flow of financial data.
- Electric power grids.

The last several years have provided a number of examples for the potential damage that a coordinated cyber attack may wreak upon a nation's information infrastructure. These instances include:

- Russia-based hackers during the summer of 2008 assaulted the Republic of Georgia's government websites and commercial internet servers during the country's conflict with Russia.
- Russia-based hackers in May 2007 attempted with some success to undermine Estonia's Internet and banking systems through denial-of-service attacks during a politically tense period between the two countries. Russia has denied any official involvement in attacking Estonia.

The U.S. cyber infrastructure is susceptible to foreign and domestic attacks, and the breadth of our information architecture makes security breaches nearly inevitable. Unsurprisingly, the U.S. national

security system comes under special assault from malicious forces.

- The Department of Homeland Security (DHS) reported over 18,000 cyber-related incidents against federal agencies and more than 80,000 attacks on military computer systems in 2007.
- The Department of Defense (DoD) reported during a May 2008 House Intelligence Committee hearing that U.S. military systems are scanned or attacked more than 300 million times per day. Along these lines, China-based hackers probably penetrated U.S. military networks in 2007, according to DoD. Previously, some experts have alleged that China-based hackers allegedly penetrated unclassified military systems in 2001, nodes in the northeastern U.S. electric power systems in 2003 and computers in the U.S. Congress in 2008.

U.S. lawmakers are not immune from foreign cyber attacks on their personal and professional property.

- China-based hackers allegedly attacked computers in 2006 and 2007 used by a human rights subcommittee of the House Committee on Foreign Affairs, according to two Members of Congress. China's Foreign Ministry subsequently denied the charges.
- During a trip to Beijing in 2007, spyware programs were clandestinely placed on electronic devices used by the Secretary of Commerce and potentially other members of a top U.S. trade delegation.

Recent National Initiatives

In recent years, policymakers have recognized the importance of securing our information infrastructure and responded by increasing resources and focus on cyber security. These efforts have included:

- *The National Strategy to Secure Cyberspace of 2003*: Aimed at preventing cyber attacks against critical U.S. infrastructures, reducing national vulnerability, and minimizing the damage and recovery time from cyber attacks that do occur.
- *The "Einstein Program" of 2003-U.S. Computer Emergency Readiness Team (US-CERT)*: Created an automated process for gathering and sharing security information through DHS.
- *The Comprehensive National Cybersecurity Initiative of 2008 (CNCI)*: a classified "multi-agency, multi-year plan to secure the federal government's cyber networks."

The Intelligence Community: Bolstering U.S. Cyber Security

The IC takes a leading role in preventing cyber attacks and protecting the U.S. information infrastructure. According to press reports, various organizations within the IC could pursue some of the following tasks:

- *Office of the Director of National Intelligence (ODNI)*: Head a task force coordinating efforts to identify sources of future cyber attacks.
- *Department of Homeland Security (DHS)*: Lead for protecting government computer systems.
- *Department of Defense (DoD)*: Devise strategies for potential counterattack of cyber attackers.
- *National Security Agency (NSA)*: Monitor, detect, report and respond to cyber threats.
- *Federal Bureau of Investigation (FBI)*: Lead national efforts to investigate and prosecute cybercrimes.

Issues for the 111th Congress

The 111th Congress can support the IC by focusing on three particular aspects of preserving cyber security: organization, detection and deterrence.

National Organization: As the roles and responsibilities for the national cyber security effort evolve, Congress may consider whether the IC should play a leadership role on an issue that has significant policy and non-intelligence implications. For example, organizations such as the U.S. Strategic Command (STRATCOM), NSA and DHS could play an important role in managing overall cyber security efforts.

Early Detection and Warning: The IC should attempt to develop mechanisms of early detection in order to prevent attacks against our information infrastructure. The IC's leaders are aware of this threat—the Director of National Intelligence (DNI) in February 2008 stated that, "nations, including Russia and China, have the technical capabilities to target and disrupt elements of the U.S. information infrastructure…Terrorist groups—including al-Qaeda, Hamas and Hizballah—have expressed the desire to use cyber means to target the United States."

- The DHS Secretary in April 2008 announced that federal officials are trying to develop an early warning system that alerts authorities to incoming computer attacks targeting U.S. infrastructure.
- Any successful nationwide early warning system must be able to distinguish between small

cyber 'nuisances' and large-scale coordinated and targeted attacks that could significantly threaten the nation.

Deterrence: A comprehensive national deterrence strategy for cyber threats does not yet exist. Based on information gathered from previous attacks, the IC could begin to assess cyber threats through the lens of deterring future attacks.

- These assessments could provide policymakers with the foundation to craft a viable strategy to deter adversaries from attacking the nation's information architecture. A complete strategy will not only require awareness of possible threats, but also provides a credible response to attacks that would deter enemies from attacking in the first place.

Sources

Cyber Security and the Intelligence Community

"Annual Report to Congress: Military Power of the People's Republic of China 2008." Department of Defense. <http://www.defenselink.mil/pubs/pdfs/China_Military_Report_08.pdf>.

Bain, Ben. "Number of Reported Cyber Incidents Jumps." Federal Computer Week. 17 Feb 2009.

"China Denies Hacking U.S. Computers." AP, 12 June 2008.

Department of Homeland Security. "National Strategy to Secure Cyberspace." <http://www.dhs.gov/xprevprot/programs/editorial_0329.shtm>.

Department of Homeland Security. "US-CERT." <http://www.us-cert.gov>.

Director of National Intelligence. "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee." 27 February 2008.

"Estonia's Web Sites Crippled by Russian Hackers." FOX News. 18 May 2007.

Harris, Shane. "Chinese hackers pose serious danger to U.S. computer networks." National Journal. 29 May 2008.

Morozov, Evgeny. "The Kremlin's Virtual Army." Foreign Policy. August 2008.

Shachtman, Noah. "Russian Coder: I Hacked Georgia's Sites in Cyberwar." Wired. 23 October 2008.

Shalal-Esa, Andrea. "U.S. working to respond to growing cyber attacks." Reuters, 27 November 2007.

Somashekhar, Sandhya. "Wolf Warns of Foreign Attacks on Computers." Washington Post, 12 June 2008.