

Threat.com – Part Two: The Age of Cyber Defense

Your computer may be the next weapon of mass destruction. Or it could be a mobile phone somewhere in Asia. Is such a threat even possible? In February 2010 war game, former top-level national security officials, including Michael Chertoff and John Negroponte, were asked how to respond to a cyber attack where cell phones and computers were used to shut down the internet and create power outages across the East coast that hit amidst hurricanes and a heat wave. Participants pondered challenges like controlling cellular and energy networks, as well as government authority, in emergencies. Unlike the 1983 movie *War Games* where a high school student nearly starts World War III by hacking into a military computer to run a nuclear war simulation, thinking it to be a computer game, the once cinematic threat is now all too real. Although the U.S. is widely acknowledged to have the most robust cyber infrastructure in the world, the recent exercise showed that protecting it is still a work in progress.

Cyber security has increasingly become a national security priority over the past decade with various government organizations taking leading roles. The National Security Agency and the Departments of Defense and Homeland Security have been protecting both civilian and military networks. The National Institute of Standards and Technology (NIST) has been leading cyber security compliance guidance for federal agencies. Cyber security policy is also influenced by the Office of Management and Budget and Congress.

The pace of cyber security has picked up considerably over the past year. In early 2009, the White House initiated an assessment of cyber policies across the federal government. The 60-day review released in May called for increased organization and coordination within the Federal government, extensive public-private partnerships and international collaboration, increased federal support for research and development, and strengthening cyber security leadership and accountability. One specific recommendation, the creation of a Presidential cyber security policy official was fulfilled with the naming of information security veteran Howard Schmidt in December.

Other recommendations have also begun to take shape. In October 2009, the U.S. Cyber Command went live with the mission to coordinate computer-network defense and direct U.S. cyber-attack operations. Based in Fort Meade, MD, the subordinate unified command will have an estimated budget of \$139 million in FY2011. The Department of Homeland Security also plans to invest \$379 million in FY2011 to bolster its National Cyber Security Division for cyber attacks defense and prevention capabilities. The Cyber Security Enhancement Act of 2009 tasks the National Institute of Standards and Technology to represent the U.S. in international cyber security technical standards development, manage technical and security standards for government information systems, and develop a cyber security education program.

However, effective cyber security will require a multi-faceted approach. In cases where attacks are believed to originate from other governments, responses may range from formal protests to economic retaliation, engaging various diplomatic and financial agencies. Consideration is also being given to President-authorized pre-emptive cyberattacks as part of national security strategies.

A significant opportunity in cyber security will be public/private cooperation. With about 80-90% of the America's critical infrastructure owned and operated by the private sector, leading cyber security experts urge stronger collaboration. Through increased sharing of information, the government can alert the private sector on threats in return for increased innovation and technical support. The most recent example is a cyber security partnership being formalized between Google and the National Security Agency. This new partnership was created to investigate the January 2010 cyber attacks that Google believes originated in China.

Collaboration will also have to cross borders. While the U.S. has worked with countries, like the United Kingdom, to counter cyber attacks, “international cooperation is imperative for establishing the chain of events in an intrusion and quickly and decisively fighting back,” as one Department of Defense official noted. In 2004, the Council of Europe Convention on Cybercrime became the first binding international treaty to harmonize national laws on computer and Internet crimes, as well as provide a framework for further international cooperation. In response to attacks on Estonian government websites in 2007, NATO established joint defense operations for cyber attacks. However, legitimate global initiatives have yet to emerge, complicated by the fact that most countries have active cyber warfare programs. Among the most active countries are China, Russia, Israel, France, the United Kingdom, and the U.S.

While there has been progress, there are still many challenges in developing a comprehensive and collaborative cyber security framework. The first is the source of the threat. Since cyber attacks can originate from an individual hacker, organized crime gangs, terror groups, or even other nations, it is often difficult to ascertain the source or credibility of a threat. The lack of a physical enemy also hinders retaliation. Also unlike traditional warfare, the size of arsenal is not a deterrent in cyber warfare. Although the U.S. is considered to have the most powerful cyber capabilities, it has consistently been a leading cyber attack target.

As sophisticated as the U.S.’ cyber capabilities are, the Former Homeland Security Secretary Michael Chertoff noted some shortcomings of American cyber security. He observed that the U.S: 1) does not have “well-defined responsibilities for maintaining common situational awareness of emerging critical operational developments in cyber space;” 2) “lacks an effective decision-making framework below the cabinet;” and 3) lacks a user friendly process to facilitate effective public/private collaboration to leverage expertise and coordinate during a cyber attack.

Public/private sector partnerships also raise other issues, such as privacy. There are concerns that collaboration may lead to continuous government monitoring of private communications. The Google-NSA alliance is reportedly designed so that NSA cannot view user accounts or searches, and Google will not share proprietary information with the NSA. Such concerns about individual liberties have also revealed that citizen awareness and participation have been an overlooked element in cyber security.

While both a national and global security priority, the role and form of cyber security is still evolving. Director of National Intelligence Dennis Blair noted that “new cybersecurity approaches must continually be developed, tested, and implemented to respond to new threat technologies and strategies.” The one certainty is that the age of cyber defense has arrived.

Sources

- James Blitz and Joseph Menn, “U.S. urges shared cybercrime defense,” *Financial Times*, January 26, 2010, <http://www.ft.com/cms/s/0/7a9a0c00-0ab2-11df-b35f-00144feabdc0.html>.
- Michael Chertoff Keynote Address, *Cyber Attacks: International Responses* Conference, February 17, 2010, <http://www.ewi.info/cyber-attacks-international-responses>.
- Mike Cronin, “World leaders to seek plan for cybersecurity,” *Pittsburgh Tribune-Review*, February 17, 2010, http://www.pittsburghlive.com/x/pittsburghtrib/news/s_667539.html.
- Cybersecurity Enhancement Act of 2009, http://science.house.gov/legislation/leg_highlights_detail.aspx?NewsID=2674.
- Bob Drogin, “In a doomsday cyber attack scenario, answers are unsettling,” *Los Angeles Times*, February 17, 2010, <http://www.latimes.com/news/nation-and-world/la-na-cyber-attack17-2010feb17,0,305928.story>.
- John J. Kruzal, Cybersecurity Seizes More Attention, Budget Dollars,” *American Forces Press Service*, February 4, 2010, <http://www.globalsecurity.org/security/library/news/2010/02/sec-100204-afps01.htm>.
- Elizabeth Montalbano, “Homeland Security Plans Cybersecurity, Data Center Investments,” *InformationWeek*, February 2, 2010, <http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=222600862>.
- “The New Civil Defense: Researchers Look at Public's Role in National Cybersecurity,” *ScienceDaily*, February 9, 2010, <http://www.sciencedaily.com/releases/2010/02/100201102020.htm>.
- “US intel chief warns of dire cybersecurity threats,” *Sydney Morning Herald*, February 3, 2010, <http://news.smh.com.au/breaking-news-technology/us-intel-chief-warns-of-dire-cybersecurity-threats-20100203-nbgz.html>.