GW CSPRI Newsletter

November 19, 2012

From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

Events

-Nov. 19, 1:00 p.m. - 2:00 p.m., **Implications of the Elections on the Tech Industry** - A webinar on the election and its potential policy impact on the technology industry. Speakers will include Kevin Richards, senior vice president of federal government affairs, and Trey Hodgkins, senior vice president of global public sector, Tech America. More information.

-Nov. 27, 7:30 a.m. - 9:30 a.m., **Leveraging Public-Private Partnerships to Protect Critical Infrastructure** - A discussion about the lessons learned by DOE, DHS and their private sector partners for collaborating effectively to enhance national security. Discussion topics include an enhanced perspective on the current national security vulnerabilities that can be alleviated by private-public partnerships, and how cyber information sharing between the public and private sector can work under existing authorities. Speakers include Matthew Light, program manager, Office of Electricity Delivery & Energy Reliability, U.S. Department of Energy; Samara N. Moore, national security staff, cybersecurity director for critical infrastructure, Executive Office of the President; Thad Odderstol, critical infrastructure protection cyber security program,

Department of Homeland Security; Mark Engels, enterprise technology security and compliance director, Dominion. National Press Club, 529 14th Street NW. More information.

-November 28, 10:00 a.m. - 12 noon, **Homeland Security: A Look Back, and Ahead** - The Homeland Security Policy Institute and the Center for Strategic and International Studies will collaborate on a discussion featuring Senator Joseph Lieberman, Chairman of the Senate Homeland Security and Governmental Affairs Committee. Senator Lieberman will look back and ahead, addressing key past events as well as homeland security challenges for the future. Other speakers include Dr. Steven Knapp, president, The George Washington University; Frank Cilluffo director, HSPI; and Rick "Ozzie" Nelson, director, Homeland Security and Counterterrorism Program, CSIS. The George Washington University, Jack Morton Auditorium, 805 21st St. NW. More information.

-Dec. 7-16, **SANS Cyber Defense Initiative 2012** - This event will feature more than 25 courses in IT security, security management, IT audit, software developer, and computer forensics. 1919 Connecticut Avenue, NW. More information.

Legislative Lowdown

-The Senate last week failed to garner enough votes to pass a cybersecurity bill that was brought to the floor for debate. Sen. Harry Reid (D-Nev.), the majority leader, last Wednesday night pronounced that the Cybersecurity Act of 2012 had run out of lives after it failed to gain 60 votes to end cloture, Federal News Radio writes. The Senate passed the motion to end cloture 51 to 47, but without three-fifths approval the bill cannot move forward to the debate and amendment portion of the process.

-The Senate cleared legislation on Wednesday that would reauthorize a six-year-old law that gave the Federal Trade Commission new authority to combat cross-border spam, spyware, and other types of online fraud, The National Journal reports. The Safe Web Act, which was first enacted in 2006 and expires next year, authorizes the Federal Trade Commission to share information with and provide investigatory assistance to foreign consumer-protection agencies about cross-border fraud, receive confidential information about fraud without having to disclose it publicly, pursue fraud cases that could involve foreign sources, and seek redress for foreign and U.S. consumers victimized by cross-border scams involving U.S. firms. The bill, which passed the House in September and now heads to the White House, would authorize the law until 2020.

-The Senate Judiciary Committee will hold a markup on Nov. 29 of legislation that would require police to obtain a warrant before reading people's emails, Facebook messages or other forms of electronic communication, The Hill reports. Committee Chairman Patrick Leahy (D-Vt.)

added the warrant requirement to H.R. 2471, a House bill that would loosen video privacy regulations.

Cyber Security Policy News

-President Obama has signed a secret directive that effectively enables the military to act more aggressively to thwart cyberattacks on the nation's web of government and private computer networks, The Washington Post reported last week. According to The Post, Presidential Policy Directive 20 establishes a broad and strict set of standards to guide the operations of federal agencies in confronting threats in cyberspace. The new directive is the most extensive White House effort to date to wrestle with what constitutes an "offensive" and a "defensive" action in the rapidly evolving world of cyberwar and cyberterrorism, where an attack can be launched in milliseconds by unknown assailants utilizing a circuitous route. For the first time, the directive explicitly makes a distinction between network defense and cyber-operations to guide officials charged with making often-rapid decisions when confronted with threats.

-Researchers in Norway have uncovered evidence of a vast Middle Eastern espionage network that for the past year has deployed malicious software to spy on Israeli and Palestinian targets, according to security blogger Brian Krebs. The discovery, by Oslo-based antivirus and security firm Norman ASA, is the latest in a series of revelations involving digital surveillance activity of unknown origin that appears designed to gather intelligence from specific targets in the Middle East.

-Brian Krebs also presents compelling evidence showing that an infamous Chinese hacker who made a name for himself leading a team that broke into U.S. Defense Department contractors in 2006 is now heading an upstart antivirus firm. CSPRI newsletter readers will find not only the story of interest, but Brian Kreb's digital sleuthing methods that led to the revelations detailed in the article!

-NASA is scrambling to implement full disk encryption on agency laptops after one containing unencrypted personal information on a "large" number of people was stolen recently. According to ComputerWorld, agency employees were told of the October 31 theft of the laptop and NASA documents from a locked car in an email message Tuesday from Richard Keegan Jr., associate deputy administrator at NASA. Keegan told employees that the stolen laptop contained sensitive "Personally Identifiable Information" (PII) about a large number of NASA employees, contractors and others.

-Federal Communications Commission Chairman Julius Genachowski has called for cybersecurity mandates to be kept out of an international telecommunications treaty that will be negotiated next month in Dubai. The Hill reports that Genachowski last week called the proposals to add cybersecurity regulations to the global treaty "misplaced and ultimately

counterproductive," according to his prepared remarks for a cybersecurity conference hosted by U.S. Central Command. Countries around the world will meet in Dubai next month to revise the International Telecommunications Regulations treaty, which will be updated for the first time since 1988. The treaty conference will be overseen by the United Nations's International Telecommunications Union and will put measures in place that affect how the flow of voice, video and data traffic will be managed across the world, according to the conference's website.

-Singapore's Ministry of Home Affairs (MHA) is proposing to amend its laws to give the government broader powers to curb cyberattacks before they are even initiated against its critical infrastructure, ZDNet reports. According to a statement issued by the MHA Monday, the Computer Misuse (Amendment) Bill seeks to change Section 15A to give the government powers to order an organization or individual to act against a cyberattack targeting national critical information infrastructure--even before the attack is carried out. For example, once the ministry receive specific, credible intelligence on a possible attack, the Minister may direct measures to be taken to "strengthen the resilience of the CII against the cyber threat", it noted. The Act currently endows the Minister the power to exercise such powers only when there is an outright attack on the CII such as a power station or water filtration plant, which could affect the economy and threaten national security.

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, http://www.cspri.seas.gwu.edu.