GW CSPRI Newsletter

September 18, 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

-Sept. 18-19, **Government Big Data Conference** - Two days worth of tracks dedicated to understanding federal agency strategy and plans, the status and forecast for key big data initiatives, and the latest tools and technologies being developed to exploit the massive amounts of information being collected at the federal level. Holiday Inn Rosslyn at Key Bridge 1900 North Fort Myer Drive, Arlington, VA. More information.

-Sept. 18, **Defense Systems Summit** - Tracks include talks on cloud computing, data center consolidation, smart phones and mobile devices, tactical communications, and data encryption technology. Hyatt Regency Crystal City, 2799 Jefferson Davis Highway, Arlington, Virginia. More information.

-Sept. 18, 12:00 noon - 1:15 p.m., **Locked Down: Keeping Confidential Information Confidential** - A teleconference panel of legal experts will share real-life horror stories and discuss how to avoid repeating costly data breach mistakes. Speakers include Sharon D. Nelson and John Simek of Sensei Enterprises. More information (PDF).

-Sept. 19, 9:00 a.m. - 11:30 a.m., **Long Term Challenges for Internet Governance** - The Center for Strategic and International Studies will include a keynote from Terry Kramer, U.S. ambassador to the World Conference on International Telecommunications. Panelists will include Bill Smith, Sally Wentworth and Veni Markovski. CSIS B1 Conference Center, 1800 K St. NW. More information.

-Sept. 19, 12:15 p.m. - 1:30 p.m., **Agency General Counsel Series: FBI General Counsel Andrew Weissman** - Andrew Weissman was appointed FBI General Counsel and Assistant Director in October 2011. At this brownbag lunchtime talk, he will discuss the work of the FBI GC's Office, including issues from financial fraud to cybersecurity, anti-terrorism to foreign corrupt practices. WilmerHale, 1875 Pennsylvania Avenue, N.W. More information.

-Sept. 20, 9:45 a.m. - 12:00 noon, **Plugging National Security Leaks While Preserving Free Speech** - The Constitution Project and Georgetown University School of Law will host a panel discussion. The speakers will be Lucy Dalglish, University of Maryland; Dana Priest, reporter, Washington Post; Harvey Rishikof and Kenneth Wainstein of Cadwalader Wickersham & Taft; and Laura Donohue, Georgetown University Law School. Gewirz Student Center, 12th Floor, 120 F St., NW.

-Sept. 21, 12:00 noon - 1:30 p.m., **Can Trade Agreements Facilitate the Free Flow of Information? The Trans-Pacific Partnership as a Case Study** - This brown-bag lunch event (RSVP requested) at GW examines two different views of a future Internet. The U.S. wants to protect intellectual property online, to encourage regulatory transparency for Internet governance, and to ensure open access to digital goods, applications, consumers, devices, networks, and information. Currently, although several non-profit US bodies oversee technical specifications and the domain name system, international multi-stakeholder groups collaborate to maintain the free flow of information on the web. However, Russia, China and several other nations want to use “the monitoring and supervisory capabilities of the International Telecommunication Union,” a U.N. agency, to regulate the Internet and allow national policymakers to restrict the free flow of information when such officials deem it appropriate. Representatives from the private sector, the Internet advocacy community, and the Senate Finance Committee will discuss the current U. S. proposal and present their views on the implications of these provisions for the future of the Internet. GW Elliott School, 1957 E Street, NW, 6th floor (Lindner Commons). More information.

-Sept. 24, 6:00 p.m. - 8:00 p.m., **Cybersecurity: Workforce Industry Building Learning Series Kickoff** - The Northern Virginia Community College's Workforce Industry Building Learning Series kickoff event about cybersecurity. Dr. Ronald Ross, one of the top 50

information technology decision-makers in government, will present about integrating cybersecurity requirements into mainstream organizational mission and business processes. The event is free to attend. All attendees will receive a complimentary dinner. Space is limited, so RSVP quickly. Ernst Cultural Center, Northern Virginia Community College, 8333 Little River Turnpike, Annandale, VA. To register, email camolinari@nvcc.edu or call 703-323-3281 or 703-323-3102.

-Sept. 27, **3rd Annual Billington Cybersecurity Summit** - A cross-section of over 25 confirmed federal, international and industry cyber experts will discuss late-breaking developments surrounding increasingly sophisticated threats to critical infrastructure. John Streufert, director, National Cybersecurity Division, DHS and Roberta Stempfley, deputy assistant secretary for cybersecurity, DHS, will be participating. National Press Club, 529 14th Street, NW. More information.

Legislative Lowdown

The House approved legislation last week that extends for five more years the government's authority to launch overseas surveillance operations on terrorists without first getting permission from a court, The Hill reports. The Foreign Intelligence Surveillance Act (FISA) Amendments Reauthorization Act, H.R. 5949, was approved 301-118 in a vote that split Democrats, just as it did in 2008, when the law was first approved. Under the bill, U.S. intelligence agencies could continue to surveil terrorists overseas without a court order. Supporters of the bill noted that both Presidents Bush and Obama have expressed support for this policy. Debate on the House floor was colored by this week's attack on the U.S. consulate in Libya, which some said shows the importance of continuing to collect information on terrorists as efficiently and quickly as possible.

The Hill also writes that Sen. Patrick Leahy (D-Vt.), the chair of the Senate Judiciary Committee, is pushing a bill that would require police to obtain a warrant before they seize emails, Facebook messages or other forms of digital communication. Under the Electronic Communications Privacy Act (ECPA) of 1986, police only need an administrative subpoena, issued without a judge's approval, to read emails more than 180 days old. Police simply swear an email is relevant to an investigation, and then obtain a subpoena to force an Internet company to turn it over.

Cyber Security Policy News

-The White House last week confirmed that the administration is considering issuing an executive order to secure the most privately-owned systems critical to the functioning of the United States economy and society, according to GovInfoSecurity. "Following congressional

inaction, the president is determined to use existing executive branch authorities to protect our nation against cyberthreats," President Obama's homeland security adviser John Brennan said in a letter to Jay Rockefeller, the chairman of the Senate Commerce, Science and Transportation Committee. The letter, dated Sept. 12, was released by Rockefeller's office on Sept. 14.

Meanwhile, Sen. Ron Wyden, a member of the select committee on intelligence, reminded the White House that any executive order addressing cybersecurity should only focus on those systems and networks critical to public safety, Federal News Radio reports. In a letter (PDF) to Michael Daniel, the White House cyber coordinator, Wyden detailed his views about what such a mandate should address. "I support efforts to create meaningful incentives for owners and operators of critical infrastructure to employ adequate security protocols," Wyden wrote. "In the case of interactive computer services, such as networks that facilitate commerce, provider search services or are platforms for social networking or speech, vulnerabilities are unlikely to constitute threats to our national security. It should be clear in any executive order related to cybersecurity that there is a fundamental difference between networks that manage infrastructure critical to public safety, like energy, water and transportation systems, and those that provide digital goods and services to the public." Wyden told Daniel that an order impacting the interactive computer services would be "a profound mistake" because it could stifle innovation, creativity and job growth.

-Two Chinese telecommunications companies last Thursday repeatedly denied accusations that they are using their software and equipment to spy on customers for the benefit of the Chinese government. Speaking to the House Permanent Select Committee on Intelligence, representatives from Huawei and ZTE told lawmakers that they answer exclusively to their shareholders and strive only to make profits, and rejected the notion they are accountable to the Communist Party in China. “Our customers throughout the world trust Huawei. We will never do anything that undermines that trust,” said Charles Ding, Huawei’s corporate senior vice president. “It would be immensely foolish for Huawei to risk involvement in national security or economic espionage.” Republican and Democratic legislators alike were skeptical of the companies’ claims of innocence, leading to several confrontational exchanges between the legislators and corporate representatives.

-In the hours before the testimony, Microsoft was breaking new ground in its efforts to combat botnets and malware threats to its user base: It convinced a U.S. judge to grant it authority over 3322.org, a dynamic DNS services provider in China that has been closely tied for years to targeted espionage attacks on Fortune 500 companies, KrebsOnSecurity.com writes. As part of a broad crackdown on software piracy, Microsoft convinced a U.S. federal court to grant it control over "Nitol," a botnet believed to be closely linked to counterfeit versions Windows that were sold in various computer stores across China. The court granted Microsoft temporary control over the name servers for that domain. While 3322.org is owned by a Chinese firm, the dot-org registry is controlled by the Public Interest Registry, a company based in Reston, Va.

-Over half of Android mobile devices are vulnerable to known security flaws that can be exploited by malicious applications to gain complete access to the operating system and the data

stored on it, according to a report from mobile security firm Duo Security. The slow deployment of security patches to Android devices is a problem that has been known of for years. Manufacturers stop issuing updates for some device models too quickly and even when they do issue updates, some carriers don't distribute them in a timely manner, the researchers found.

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.