GW CSPRI Newsletter

May 27, 2014

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

Announcements

Watch CSPRI Research Scientist, Dr. Allan Friedman comment on current cyber issues with different national and foreign media outlets. Click here for more.

Events

-May 29, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - An informal, all-ages, citysec-style meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank St., Baltimore, Md, 21231. More information.

-May 30, 12 noon, **NSA Surveillance Powers: How Effective Are They at Thwarting Terrorist Attacks?** - The advisory committee to the Congressional Internet Caucus will host a discussion about the effectiveness of the NSA's surveillance programs. Rayburn House Office Building (Room TBD). More information.

-June 2-3, **CyberSecureGov** - This conference will explore how government security personnel and managers are identifying opportunity in the midst of intense budgetary set-backs, what new technologies and policies are emerging to help agencies balance their IT investments and maintain support for a robust cyber defense capability, the status of key security initiatives such as CDM, FedRAMP, HSPD-12 and others, the government's investments in the areas of human capital, IT acquisition, guidance/policy and legislation that are impacting agency personnel and their contractors, and how collaboration between government, academia and industry is working to prepare the federal workforce of tomorrow. DoubleTree by Hilton Hotel, 300 Army Navy Dr., Arlington, VA 22202. More information.

-June 4, 1:00 p.m. - 3:00 p.m., **International Implications of the National Security Agency Leaks** - The Brookings Institution will host two panel discussions to explore the continued effects of Snowden's disclosures. The first panel will address the regional reactions to the NSA revelations and what, if any, repercussions they may have for American diplomacy, soft power and trust. The second panel discussion will focus on how the leaks have influenced Internet governance, trade and the intelligence community and what those consequences may mean for the future international order. Brookings Senior Fellow Peter W. Singer will moderate both sessions. This event also will be Webcast. Brookings Institution, Falk Auditorium, 1775 Massachusetts Avenue, N.W. More information.

-June 4-5, **The 4th International Summit on the Future of Health Privacy** - Engage with thought-provoking lectures, interactive panels, networking and discussion during the two-day Summit. Areas of discussion will include: patient ID, consumer education, mobile app privacy, international cybersecurity, data for research, ethics, and business models. Hart Auditorium, McDonough Hall, Georgetown Law Center, 600 New Jersey Ave NW. More information.

-June 5, 2:00 p.m. - 6:30 p.m., **AFCEA Presents: Insider Threat to Small Business** - One of the biggest myths is that "I'm too small for cyber attackers to care about me." This common misperception leads to tremendous vulnerabilities as companies do not understand implications for their intellectual property and/or their link to others as part of the larger supply chain. Bill Wright will brief on Symantec's recently released 2014 report on cyber attacks, including the devastating facts on attacks on small- and medium-sized businesses. Michael Theis, from the CERT Insider Threat Center at Carnegie Mellon University, will discuss the Center's current research aimed at establishing best practices to mitigate insider threats, including techniques for identifying insider threats and strategies for building a robust insider threat program. AFCEA International, 4400 Fair Lakes Court, Fairfax, VA 22033. More information.

-June 5, 8:55 a.m. - 5:00 p.m., **DC Metro Cyber Security Summit** - This conference series seeks to connect C-Level and senior executives responsible for protecting their companies' critical infrastructures with cutting-edge technology providers and renowned information

security experts. Sheraton Premiere, 8661 Leesburg Pike, Tysons Corner, VA 22182. More information.

-June 11, 8:30 a.m. - 6:00 p.m., **The 2014 Cloud Computing Policy Conference** - The 2014 Cloud Computing Policy Conference USA will bring together over 150 delegates from the digital industries, the public sector, civil society and policymaking communities to debate the priorities facing the US cloud computing sector. It will explore market developments in cloud computing and how businesses and government administrations can best exploit the opportunities offered by the technology. Central to the discussions will be a debate on how to frame and deliver the necessary measures to restore trust following the PRISM revelations, ensuring that at both and home and abroad, the US continues to lead the way in cloud innovation and services. W Washington DC Hotel, 515 15th St NW. More information.

Legislative Lowdown

-Last week, the House of Representatives passed the USA Freedom Act, despite objections from tech companies and privacy groups which charged that the bill leaves loopholes open for intelligence agencies to exploit. "Under the legislation, the government would no longer retain bulk collection of phone metadata—the numbers and timestamps of calls but not their actual contents," National Journal reports. "Instead, phone companies will keep those records and be required to hand them over to the NSA and other intelligence agencies only after the government receives approval for each data search from the Foreign Intelligence Surveillance Court, except in emergency cases. The measure also reduces from three to two the number of 'hops,' or degrees of separation, away from a suspected target the National Security Agency can jump when analyzing communications. The amended language, however, dropped a provision that would have allowed companies to disclose the level of surveillance orders received under Section 702 of the Foreign Intelligence Surveillance Act, and it codifies a two-year delay for making some surveillance orders public."

-The New York Times's editorial page panned the USA Freedom Act, saying it doesn't live up to its title. "Privacy advocates said the N.S.A. could use the changed language to demand records for an entire ZIP code, state or region. Administration officials say they don't intend to do that, but their record of exploiting legal loopholes doesn't provide much confidence," The Times argues. "The changes demanded by the White House would also weaken the provision allowing Internet companies to report how often the government made requests of their data. (Most of those companies now say they can no longer support the bill.) And the role of declassifying court decisions would go from the attorney general to the director of national intelligence, the last person who should do it."

-Meanwhile, civil libertarians upset that the House didn't go far enough with the USA Freedom Act are mounting a renewed effort in the Senate to shift the tide more in their favor, writes The Hill. "This is going to be the fight of the summer," The Hill quotes Gabe Rottman, legislative counsel with the American Civil Liberties Union. "If advocates are able to change the House bill's language to prohibit NSA agents from collecting large quantities of data, 'then that's a win,'

Rottman added. 'The bill still is not ideal even with those changes, but that would be an improvement.'"

-A bill designed to make it easier for cybersecurity employees at the Department of Homeland Security to have salaries that compete with the private sector is headed to the Senate floor, as NextGov writes, there is a shortage of skilled computer security employees at many civilian agencies with heavy cyber responsibilities, and this bill could help DHS compete with the private sector and the U.S. military for scarce talent. But some critics of the measure say it could be abused to boost infosec hiring that doesn't fill information security staff shortages. GovInofSecurity quotes a key senator quipping that the bill is primarily aimed to fill positions in the Washington area, rather than taking advantage of cheaper cybersecurity expertise that can be found elsewhere in the United States.

Senate lawmakers introduced a measure last week to go after employees and businesses that steal valuable economic secrets from American companies. The "Deter Cyber Theft Act" would authorize the President to direct the Treasury Department to freeze the assets of any foreign person or company, including a state owned enterprise, determined to have benefited from the theft of U.S. technology or proprietary information stolen in cyberspace, The Washington Post reports. "The bill also requires the director of national intelligence to publish an annual report of which foreign nations are contributing to commercial cyberspying against the United States -- be it by actively engaging in the practice themselves or by failing to prosecute it domestically. The report would include watch list of countries actively using the Internet for economic or industrial espionage and identify which U.S. technologies or trade secrets are being targeted by hackers among other things."

Cyber Security Policy News

-Just days after the United States Justice Department indicted five Chinese nationals for cyberspying, China has opted to suspend involvement in a cybersecurity working group with the U.S., Business Week writes. "The group was established last year when U.S. Secretary of State John Kerry visited Beijing and the two sides tried to patch up ties that have long been dogged by accusations of cyber espionage. It met in Washington in July, even after former U.S. National Security Agency whistle-blower Edward Snowden began making revelations about America's cyber-spying that included hacking into computers in China since 2009."

The fallout from those indictments is being felt elsewhere: China also reportedly ordered state enterprises to cut dealings with U.S. consulting firms, accusing them in turn of spying for the U.S. government, according a report in the Financial Times. The "instruction," as the paper called it, was handed down after U.S. Attorney General Eric Holder announced indictments against five Chinese military officers for "serious cybersecurity breaches," writes Gordon Chang, in an op-ed for Forbes, in which he quotes liberally from the FT story (which is behind a paywall). The letter apparently continued: "The top leadership has proposed setting up a team of Chinese domestic consultants who are particularly focused on information systems in order to seize back this power from the foreign companies," the paper quoted a 'senior policy adviser to

the Chinese leadership' as saying. "Right now the foreigners use their consulting companies to find out everything they want about our state companies."

In addition, China has begun imposing new inspection requirements for networking gear sold there. Citing the state-run Xinhua news agency, Ars Technica observes that, "Jiang Jun, a spokesman for the State Internet Information Office, told Xinhua that the move was to counter large-scale spying, saying that the networks of Chinese government agencies, universities, businesses and telecommunications providers have 'suffered extensive invasion and wiretapping,' the news service reported." According to Ars, the measure is intended to prevent technology providers from "taking advantage of their products to illegally control, disrupt, or shut down their clients' systems, or to gather, store, process, or use their client's information." Under the new policy, IT products that don't pass the government's vetting process will be banned in China.

-Gen. Keith Alexander, the former head of the National Security Agency, is planning to launch his own cybersecurity firm in Washington, D.C., Politico reports. "Less than two months since his retirement from the embattled agency at the center of the Edward Snowden leak storm, the retired four-star general is setting up a Washington-based operation that will try to attract clients based on his four decades of experience in the military and intelligence — and the continued levels of access to senior decision-makers that affords," wrote Darren Samuelson and Joseph Marks. "Alexander will lease office space from the global consulting firm Promontory Financial Group, which confirmed in a statement on Thursday that it plans to partner with him on cybersecurity matters."

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.