GW CSPRI Newsletter

May 6, 2013

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

-May 7, 1:00 p.m. - 2:30 p.m., **Cyber Threats and Network Security Countermeasures: Keeping Your Intellectual Property and Secrets Safe** - The American Bar Association will host a webcast and teleconferenced panel discussion. The speakers will be Zal Azmi, former CIO, Federal Bureau of Investigation, Senior Vice President, Cyber Solutions Group, CACI; Harlan Carvey, chief forensics officer, Applied Security; David Opderbeck, director, Gibbons Institute of Law, Science & Technology, Seton Hall University Law School; and David Manning, vice president, Applied Security. More information.

-May 7, 6:00 p.m. - 8:15 p.m., **International Privacy: Working in the Global Cloud and Preparing for the EU's New Privacy Approach** - The Federal Communications Bar Association will host an event. Covington & Burling, 11th floor, 1201 Pennsylvania Ave., NW. More information.

-May 8, 8:30 a.m. - 10:00 a.m., **Robotic and Remotely Piloted Aircraft Inside the United States: Applications, Safety, Perceptions, and Privacy Concerns** - RTI International will host a panel discussion. The speakers will include Sen. Mark Udall (D-Colo.); Tim Gabel, executive vice president, social, statistical, and environmental sciences RTI; David Schanzer, associate

professor of public policy, Duke University & co-director, Institute for Homeland Security Solutions; Peter Singer, director of the Center for 21st Century Security and Intelligence, Brookings Institution; John McGraw, founder and principal, John McGraw Aerospace Consulting, LLC; Kenneth Mortensen, former associate deputy attorney general and chief privacy & civil liberties officer, U.S. Department of Justice; and Darryl Jenkins, airline analyst, Aviation Consulting. National Press Club, 529 14th St. NW., Ballroom, 13th floor. More information.

-May 8, 9:00 a.m., **Cyber Threats: Law Enforcement and Private Sector Responses** - The Senate Judiciary Committee's Subcommittee on Crime and Terrorism will hold a hearing, which will also be Webcast and archived. Dirksen Senate Office Bldg., Room 226. More information.

-May 8, 1:00 p.m. - 2:00 p.m., **Cybersecurity -- Information Sharing, Privacy, Regulation, and Reason** - The International & National Security Law Practice Group will host a teleforum discussion of whether information sharing can improve security while protecting privacy, and whether regulatory measures help without imposing excessive burdens on business. Speakers will include Gus P. Coldebella, partner, Goodwin Procter LLP and former Acting General Counsel, Department of Homeland Security; Michelle Richardson, legislative counsel, American Civil Liberties Union; and Nathan A. Sales, George Mason University School of Law and former deputy assistant secretary for policy development, Department of Homeland Security. More information.

-May 8-10, **Cyber Security for Defense, Intelligence & Homeland Security** - This gathering will examine a broad range of defense and cybersecurity topics, including interagency information sharing, securing big data, and critical infrastructure protection. Holiday Inn Rosslyn at Key Bridge, 1900 North Fort Myer Drive, Arlington, Va., 22209. More information.

-May 9, 8:15 a.m. - 5:15 p.m., **Baltimore Tech-Security Conference** - This all-day conference features discussions on current tech-security issues such as email security, VoIP, LAN security, and wireless security. Hilton Baltimore, 401 West Pratt Street, Baltimore, Maryland, 21201. More information.

-May 14-15, **GovSec** - A security conference and expo, GovSec will feature discussions about cyberespionage, critical infrastructure protection, and why cybercrime has become the perfect crime. Walter E. Washington Convention Center, 999 9th Street NW. More information.

-May 14-16, **FOSE** - This three-day conference and expo will feature 10 separate tracks on cybersecurity, including talks from a variety of government technology and cybersecurity experts, including Joe Albaugh, chief information security officer, Federal Aviation Administration; Bob Brese, deputy CIO, Department of Energy; and Mischel Kwon, president, Mischel Kwon and Associates. Walter E. Washington Convention Center, 999 9th Street NW. More information.

Legislative Lowdown

-The White House last week shed more light on its decision to issue a veto threat against a cybersecurity bill that passed the House this month in a response published to a "We the People" petition, The Hill reports. The original petition opposed the Cyber Intelligence Sharing and Protection Act, or CISPA, citing privacy concerns with the bill. In its response, top White House officials said final changes made to the bill still didn't allay the administration's underlying concerns with the measure. The administration will keep advocating for cybersecurity legislation that includes privacy protections for people's personally identifiable information and also "closely monitor" developments in the Senate on legislation, White House Cybersecurity Coordinator Michael Daniel and White House Chief Technology Officer Todd Park write in the response.

-A government task force is preparing legislation that would pressure companies such as Face-book and Google to enable law enforcement officials to intercept online communications as they occur, according to The Washington Post. Driven by FBI concerns that it is unable to tap the Internet communications of terrorists and other criminals, the task force's proposal would penalize companies that failed to heed wiretap orders — court authorizations for the government to intercept suspects' communications. Rather than antagonizing companies whose cooperation they need, federal officials typically back off when a company is resistant, industry and former officials said. But law enforcement officials say the cloak drawn on suspects' online activities — what the FBI calls the "going dark" problem — means that critical evidence can be missed.

Cyber Security Policy News

-The United States is gravely concerned about the impact that Chinese theft of U.S. trade secrets is having on American companies and the economic security of the United States, the U.S. Trade Representative's office said last week. Reuters writes that the U.S. Trade Representative's office stopped short of designating China as a "priority foreign country" because of trade secret theft, as recently urged by two senior Democrats in the House of Representatives. Doing so would have initiated a process that could lead to sanctions on Chinese goods if U.S. concerns were not addressed.

That assessment came the same week Bloomberg News revealed that the company which acts as a top developer of new technologies for American spies had Chinese cyberspies stealing the firm's secrets for more than three years. QinetiQ North America is known for spy-world connections and an eye- popping product line. Its contributions to national security include secret satellites, drones, and software used by U.S. special forces in Afghanistan and the Middle East. Former CIA Director George Tenet was a director of the company from 2006 to 2008 and former Pentagon spy chief Stephen Cambone headed a major division. Its U.K. parent was created as a spinoff of a government weapons laboratory that inspired Q's lab in Ian Fleming's James Bond thrillers, a connection QinetiQ (pronounced kin-EH-tic) still touts. QinetiQ's espionage expertise didn't keep Chinese cyber- spies from outwitting the company. In a three-year operation, hackers linked to China's military infiltrated QinetiQ's computers and compromised most if not all of the company's research. At one point, they logged into the company's network by taking advantage of a security flaw identified months earlier and never fixed.

Meanwhile, North Korea is expected to mooch off other nations for cyber offensive tools because it is not plugged into the global Web, according to the Defense Department's first report to Congress on the regime's military might. NextGov reports that these are some of the spare details describing Pyongyang's network operations found amidst a larger discussion of the regime's antagonism with South Korea and pursuit of nuclear weapons. The unclassified 2012 assessment concludes the Democratic People's Republic of Korea "probably" has the capability to carry out military computer network operations. Since 2009, the nation has been linked to cyber espionage campaigns and distributed denial of service attacks that externally flood websites with paralyzing traffic, according to the Pentagon.

-The United States, concerned that Iran is behind a string of cyberattacks against U.S. banking sites, has considered delivering a formal warning through diplomatic channels but has not pursued the idea out of fears that doing so could escalate hostilities, The Washington Post writes. At the same time, the officials told The Post, the disruptive activity against the Web sites has not yet reached a level of harm that would justify a retaliatory strike. The internal discussion reflects the complex nature of deciding when and how the United States should respond to hostile cyber-actions from other countries. It also reflects the pressure the administration is under from banking industry officials, who want to know what amount of pain or damage will justify a government response.

-The Department of Homeland Security characterizes as a nuisance the threatened May 7 Operation USA attack against U.S. federal government and banking websites, contending some of the participants possess only rudimentary hacking skills. The campaign "likely will result in limited disruptions and mostly consist of nuisance-level attacks against publicly accessible webpages and possibly data exploitation," reads the DHS alert, a copy of which was printed by Krebsonsecurity.com. "Independent of the success of the attacks, the criminal hackers likely will leverage press coverage and social media to propagate an anti-US message." The DHS alert is in response to chest-thumping declarations from anonymous hackers in the Middle East who have promised to team up and launch a volley of online attacks against a range of U.S. targets beginning May 7. According to the DHS alert, 46 U.S. financial institutions have been targeted with distributed denial of service (DDoS) attacks since September 2012 — with various degrees of impact — in over 200 separate DDoS attacks.

-According to the 2012 Foreign Intelligence Surveillance Act (FISA) Report, the Department of Justice submitted 1,856 applications to the Foreign Intelligence Surveillance Court (FISC), a 6.4% increase over 2011. The Electronic Privacy Information Center has the lowdown on the applications for FISA warrants, which the government requests in order to conduct covert surveillance activities of foreign entities and individuals in the United States. Of the 1,856 search applications, 1,789 sought authority to conduct electronic surveillance. The FISC did not deny any of the applications, although one was withdrawn by the Government. However, the FISC did make modifications to 40 of the applications, including one from the 2011 reporting period. In addition to the FISA orders, the FBI sent 15,229 National Security Letter requests for information concerning 6,223 different U.S. persons. This is a modest decrease from the 16,511 requests sent in 2011. Almost no information is available about FISA surveillance beyond the figures contained in the annual FISA letter, sent to the Senate each year by the Department of Justice, Office of Legislative Affairs.

CSPRI Research Developments

-On April 23-25, Prof. Lance Hoffman, Director of CSPRI, ran an NSF-sponsored workshop in Orlando, Florida that brought together computer scientists, social scientists, and other stakeholders in an attempt to integrate social sciences into design of future cyber security mechanisms and systems. The workshop will allow the development of new models of and paradigms for cyber security and will lead to the development of communities of researchers who today do not interact, but whose cooperative work is necessary for the development of cyber security mechanisms and systems. Results from the workshop are being used to produce a research agenda in social sciences related to cyber security that addresses user, economic, and sociopolitical realities.

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.