THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
*Thoughtful Analysis of Cyber Security Issues*

# GW CSPRI Newsletter

June 20, 2011

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



# Upcoming Events

-June 20-23, **Gartner Security & Risk Management Summit** - Topics to be covered include governance risk compliance; cloud computing and recovery; security architecture; mobile applications and security; and security threats and vulnerabilities. Gaylord National, 201 Waterfront Street, National Harbor, MD. More information.

-June 21, 10:00 a.m. - 12 noon, **Cybersecurity and Data Protection in the Financial Sector** - The Senate Committee on Banking, Housing and Urban Affairs will hold a hearing. Witnesses will be **Kevin Streff**, associate Professor and director of the Center for Information Assurance, Dakota State University; Leigh Williams, BITS President, The Financial Services Roundtable; Marc Rotenberg, president, Electronic Privacy

Information Center. Additional witnesses may be announced. Room 538, Dirksen Senate Office Building. More information.

-June 21, 7:30 a.m. - 9:30 a.m., **Will 2011 be the Year of Cyber?** - Join a panel of federal cyber experts on June 21 to explore the changing federal landscape. What are the White House cyber bill's chances of passage? How are CIOs partnering with CISOs to lead federal cyber strategy? What new measures are being used to gauge the effectiveness of agencies' efforts? Speakers include **John Gilligan**, former chief information officer for the U.S. Air Force; and **Tommy Ross**, senior defense and intelligence adviser, Sen. Harry Reid (D-Nev.). Ronald Reagan Building ~ The Rotunda 8th Floor (North Tower) 1300 Pennsylvania Avenue, NW. More information.

-June 21, 8:30 a.m. - 11:00 a.m., **Controlling Cyber Conflict? Arms Control, International Norms, and Strategic Restraint** - This panel discussion brings together expert panelists to discuss and explore how cyber conflict can be mitigated. Is the cyberspace domain amenable to arms control solutions, and what would such solutions look like, or are the development of international norms more appropriate? On the other hand, given the unique nature of the cyber domain, is strategic restraint by individual actors, as well as the resilient character of the domain itself, enough to mitigate the worst excesses of any cyber conflict? National Press Club, 529 14th St. NW, 13th Floor. More information.

-June 21, 2:30 p.m., **Hearings to Examine Cybersecurity** - This meeting of the Senate Judiciary's Subcommittee on Crime and Terrorism will focus on evaluating the Obama administration's legislative proposals on cybersecurity. Witnesses to include **James A. Baker**, associate deputy attorney general, U.S. Department of Justice; **Greg Schaffer**, acting deputy undersecretary, National Protection and Programs Directorate, Department of Homeland Security; and **Ari Schwartz**, senior internet policy analyst, National Institute of Standards and Technology, U.S. Department of Commerce. Room 342, Dirksen Senate Office Building. More information.

-June 22, 10:00 a.m. - 11:00 a.m., **National Security Risks from Electromagnetic Threats** - This free Webinar, offered in association with the National Electric Security Cybersecurity Organization, focuses on the national and cybersecurity threat from electromagnetic disturbances and directed electromagnetic pulse (EMP) attacks. A look at new initiatives underway in Congress, the White House, FERC, DOE and DOD to begin taking a range of actions to protect critical U.S. infrastructures and assets from Severe Space Weather and EMP. More information.

-June 23, 7:45 a.m. - 9:30 a.m., **NERC: Cyber Status, Trends and the Future - Mark Weatherford**, vice president and chief security officer of the North American Electric Reliability Corporation’s (NERC), will discuss cybersecurity trends as they relate to the bulk power system, the current cyber threat landscape, the status of ongoing NERC efforts and recent initiatives, and legislative matters related to NERC's activities. ICF International, 1725 Eye St NW, Suite 1000. More information.

# Announcements

-There is a new monthly seminar series at the National Science Foundation: the Washington Area Trustworthy Computing Hour (WATCH). The series will meet at NSF at noon on the first Thursday of each month, starting June 2, 2011. These talks will be held in Stafford I, Room 110, (4201 Wilson Boulevard, Arlington, VA) and the public is invited; no badges required.

The inaugural speaker was **Prof. Fred B. Schneider** of Cornell, who spoke on "Cybersecurity Doctrine: Towards Public Cybersecurity." Abstract: With increasing dependence on networked computing systems comes increasing vulnerability. The vulnerabilities are mostly technical in origin, but their remediation is not. Only by coupling technical insights with public policy do we stand a good chance to create a safer and more secure cyberspace. This talk surveyed the landscape, discussed why past doctrines have failed, and proposed a new doctrine of Public Cybersecurity. This is joint work with **Deirdre Mulligan**, a professor of law at the UC Berkeley School of Information and a Faculty Director of the Berkeley Center for Law and Technology.

The next talk in the series will be held on July 7, 2011. Paul L. Harris of Harvard University Graduate School of Education will be speaking on “Selective Credulity.”

# Legislative Lowdown

-The chairwoman of the House Energy and Commerce Manufacturing subpanel issued a draft version of her SAFE Data Act, a measure drafted in response to a raft of data breach disclosures that has not been timely enough for many critics. The bill, to be offered by **Rep. Mary Bono Mack** (R-Calif.), would require firms to notify the Federal Trade Commission within 48 hours of securing and assessing the scope of a data breach, Politico reports. The FTC would be able to levy fines if companies wait before notifying customers. Non-profits and charities would also be subject to the bill's requirements.

**-Sens. Al Franken** (D-Minn.) and **Richard Blumenthal** (D-Conn.) introduced a bill Wednesday that would require firms including Apple and Google to obtain users' consent before collecting or sharing their mobile location data with third parties. The Location Privacy Protection Act (PDF) would close loopholes in existing law, such as the one that currently forces any firm that obtains location data from more than 5,000 mobile devices to take reasonable steps to protect and delete that data if requested by the customer, according to eWeek. The bill proposes fines of up to $2,500 per violation.

# Cyber Security Policy News

- The recent string of sensational hacker attacks is driving companies to seek "cyberinsurance" worth hundreds of millions of dollars, even though many policies can

still leave them exposed to claims, Reuters reports. Companies are having to enhance not just their information technology practices but also their human resources and employee training functions just to get adequate coverage against intrusion -- and in some cases, they are also accepting deductibles in the tens of millions of dollars.

-The National Security Agency is working with Internet service providers to deploy a new generation of tools to scan e-mail and other digital traffic with the goal of thwarting cyberattacks against defense firms by foreign adversaries, senior defense and industry officials say, The Washington Post writes. "The novel program, which began last month on a voluntary, trial basis, relies on sophisticated NSA data sets to identify malicious programs slipped into the vast stream of Internet data flowing to the nation's largest defense firms. Such attacks, including one last month against Bethesda-based Lockheed Martin, are nearly constant as rival nations and terrorist groups seek access to U.S. military secrets."

-China must boost its cyber-warfare strength to counter a Pentagon push, the country's top military newspaper said on Thursday after weeks of friction over accusations that Beijing may have launched a string of Internet hacking attacks, Reuters reports. "The accusations against China have centered on an intrusion into the security networks of Lockheed Martin Corp and other U.S. military contractors, and deceptions intended to gain access to the Google e-mail accounts of U.S. officials and Chinese human rights advocates," reporter Chris Buckley wrote. "But the official newspaper of the People's Liberation Army said it was Beijing that was vulnerable to attack, in a news report that surveyed the Pentagon's efforts in cyber security."

-European Union countries have agreed to tougher sentences against cyber attacks and created a cyber-crime unit to be attached to Europol, the continent-wide police agency, SiliconRepublic writes. Under the new rules, being part of an organized crime group involved in a cyber attack against a critical IT system or causing serious damage via a botnet carries a maximum prison term of at least five years. The penalties for creating a botnet for mounting cyber attacks are up to three years in prison. General cyber crime carries a prison term of at least two years.

-Spanish authorities said last week they had arrested three members of the hacking group Anonymous in connection with attacks against Sony's online Playstation network, among other sites. Police said the three, whose identities were not disclosed, carried out the attacks from a server based in one of the suspect's houses in northern Spain. Anonymous, a loose-knit collective of hacktivists, has denied involvement in the Sony hack, but has publicly taken credit for attacks against PayPal, Visa and others because those institutions declined to transmit donations to the whistleblower site, WikiLeaks.

-Comerica Bank is liable for more than a half a million dollars stolen in a 2009 cyber heist against a small business, a Michigan court ruled, KrebsOnSecurity.com writes. Experts say the decision is likely to spur additional lawsuits from other victims that have been closely watching the case. The ruling comes just a week after a Maine court presiding over a similar e-banking breach case ruled in favor of the bank.

*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.*