Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

In This Issue

Quick Links

[About CSPRI](#)

[Contact Us](#)

[Newsletter Archive](#)

[Blog: The CSPRI Byte](#)

Cyber Monday 2014 is Cybersecurity Monday in Washington. Followed immediately by Cybersecurity Tuesday.

Cyber Monday may be a term created by marketeers to encourage online shopping, but this year at least, it offers some wonderful opportunities to hear from leaders in cybersecurity and privacy and to make your own assessments about what the future will look like. There are at least two important events on Monday, December 1 and two more on Tuesday,

November 24, 2014

Seven (7) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.

Event Announcement

Cybersecurity Events Dec 1-2 at GW

Monday, December 1, 4:30pm-6pm, Towards a Trusted Internet: Backdoors to the Crypto Nirvana Promised Land. Panel Discussion moderated by Prof. Eric Burger, Georgetown University with panelists Russ Housley, Chair, Internet Architecture Board; Lance Hoffman, Director, GWCyber Security Policy and Research Institute; Quentin Liu, Senior Director of Engineering, Symantec; and Christopher Soghoian, Principal Technologist, American Civil Liberties Union.

Tuesday, December 2, 2:00pm-3:30pm, The U.S.-China Bilateral Relationship and Cybersecurity. Minister Lu Wei, head of the Cyberspace Administration of the People's Republic of China. (Opening remarks by Dr. Stephen Knapp, GW President; Q&A moderator is Philip J. Crowley, Institute for Public Diplomacy and Global Communication, GW SMPA and ESIA)

Registration links:
-Click **here** for registration for the December 1 event.
-Click **here** for the registration for the December 2 event.

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman: @allanfriedman

December 2 in Washington, so plan now to hit the ground running as you return from the Thanksgiving holiday weekend. Registration for one closes on November 25. Whether you're interested in the technology or policy, there is something for you. And if you are interested in both, prepare to run around a bit, as you can catch all of these!

Click here for all the events and details!

Legislative Lowdown

NSA reform bill fails in the Senate
-A legislative effort to curtail the National Security Agency's domestic surveillance activities failed in the Senate last week. The "USA Freedom Act" was supported by civil liberties groups, which considered tonight's vote the last-gasp chance for the bill to move forward before some of its staunchest supporters hand over seats lost in the November elections, according to Wired.com. "The bill would have put an end to the government's controversial bulk collection of phone records from U.S. telecoms-a program first uncovered by *USA Today* in 2006 but re-exposed in 2013 in leaks by NSA whistleblower Edward Snowden," writes Kim Zetter. "The bill would instead have kept records in the hands of telecoms and forced the NSA to obtain court orders from the Foreign Intelligence Surveillance Court to gain access to them. It would also have required the agency to use specific search terms to narrow its access to only relevant records."

Cyber Security Policy News

Grim predictions on cyber attacks
NSA Director Michael S. Rogers told US lawmakers last week that China and other foreign countries have broken into systems at organizations supporting US critical infrastructure, with the intention of stealing data that could be used to launch a destructive attack, The Washington Post reports. "In the past, U.S. intelligence officials warned that the Chinese had penetrated the electric grid. Now, NSA Director Adm. Michael Rogers has confirmed that "there's probably one or two others" that have also wormed their way in," Ellen Nakashima writes. "The Cyber Command head said he agreed with a recent Pew Research Center report that found a majority of cyberexperts predicted a catastrophic attack within the United States by 2025."

NSA objections, pre-Snowden
Years before Edward Snowden sparked a public outcry with the disclosure that the NSA had been secretly collecting American telephone records, some NSA executives voiced strong objections to the program,

according to interviews the Associated Press conducted with current and former intelligence officials say. "The program exceeded the agency's mandate to focus on foreign spying and would do little to stop terror plots, the executives argued," the AP wrote. "The 2009 dissent, led by a senior NSA official and embraced by others at the agency, prompted the Obama administration to consider, but ultimately abandon, a plan to stop gathering the records." Read more here.

Documents unsealed on cellphone tracking

A judge last week unsealed a trove of court documents that could shed light on a secret cellphone tracking program used by police nationwide, reports The Hill. "Included are 529 requests from local Charlotte-Mecklenburg police asking judges to approve the use of a technology known as StingRay, which allows cellphone surveillance," writes Cory Bennett. "Together, the requests give the most complete account yet of the U.S. law enforcement tactic, about which little is known."

Washington state: Sharper monitoring of use of StringRay technology

Meanwhile, Washington state is cracking down on police use of StingRay technology, according to The News Tribune. "Pierce County judges didn't know until recently that they'd been authorizing Tacoma police to use a device capable of tracking someone's cellphone," writes Adam Lynn. "Now they do, and they've demanded that police change the way they get permission to use their so-called cell site simulator. From 2009 to earlier this year, the county's Superior Court judges unwittingly signed more than 170 orders that Tacoma police and other local law enforcement agencies say authorized them to use a device that allows investigators to track a suspect's cellphone but also sweeps cellphone data from innocent people nearby."

US State Department hacked

The State Department last week joined a growing list of hacked federal agencies. As NBC reports, the agency put its unclassified email system out of commission after "activity of concern" was detected recently.

"It's the latest of several acknowledgments that sensitive government systems have been successfully targeted. The official said no classified systems were compromised," NBC observed. "The attack, which wasfirst reported by The Associated Press, affected unclassified email traffic and State Department access to public websites, and the systems were expected to be restored 'soon,' the official said."

About this Newsletter

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. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613. cspri@gwu.edu
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052