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

November 10, 2014

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

Speaker Announcement

Costis Toregas to speak on emerging cyber threats

Elliott School of International Affairs
1957 E Street, NW
Washington, DC 20052

Monday, Nov. 10 (today) - 6:30 p.m. - 7:45 p.m.

Room B12

CSPRI Associate Director Costis Toregas will discuss a recent agreement signed between US and German stakeholders that will organize a long term, sustained program of academic exchanges, seminars and collaborative research intended to build trust between the two nations.

For more information, click **here.**

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

Cyber Security Policy News

Silk Road 2.0 shut down
-Last week, U.S. federal agents shut down the online black market and drug bazaar Silk Road 2.0, and arrested a Houston man in San Francisco accused of administering the forum. "Agents with the FBI and the Department of Homeland Security arrested 26-year-old Blake Benthall, a.k.a. 'Defcon,' in San Francisco, charging him with drug trafficking, conspiracy to commit computer hacking, and money laundering, among other alleged crimes," writesBrian Krebs. "Benthall's LinkedIn profile says he is a native of Houston, Texas and was a programmer and "construction worker" at Codespike, a company he apparently founded using another company, Benthall Group, Inc. Benthall's LinkedIn and Facebook profiles both state that he was a software engineer at Space Exploration Technologies Corp. (SpaceX), although this could not be immediately confirmed. Benthall describes himself on Twitter as a 'rocket scientist' and a 'bitcoin dreamer.'"

The shutdown of Silk Road 2.0 and the arrest of its alleged administrator was one of dozens of such takedowns executed in tandem worldwide last week. As The New York Times reports, the series of raids and arrests in 16 countries, nicknamed Operation Onymous, "was aimed chiefly at sellers, and deactivated upward of 50 such websites, including Silk Road 2.0 and Blue Sky, as well as Mr. Quid's Forum and Cannabis Road Markets, according to Europol, the European Union's law enforcement agency," wrote Benjamin Weiser and Doreen Carvajal. "Across Europe and the United States, at least 17 sellers were arrested, and law enforcement authorities seized Bitcoins valued at $1 million, along with gold, cash and drugs."

Rule 41
Federal investigators are hoping to expand their authority to hack into and locate computers by changing an arcane federal rule governing how judges can approve search warrants, according to the National Journal. "The Justice Department has petitioned a judicial advisory committee to amend a rule that specifies under what conditions magistrate judges can grant the government search warrants," writes Dustin Volz. "The provision, known as Rule 41 of the federal rules of criminal procedure, typically allows judges to issue search warrants only within their judicial district. But the government has asked to alter this restriction to allow judges to approve electronic surveillance to find and search a computer's contents regardless of its physical location, even if the device is suspected of being abroad."

FBI facial recognition technology is flawed
In a separate National Journal piece, Volz writes about a futuristic FBI facial recognition database that is getting some more public scrutiny thanks to a court ruling that will let open-government advocates take a closer look at the program. "U.S. District Judge Tanya Chutkan said the bureau's Next Generation Identification program represents a 'significant public interest' due to concerns regarding its potential impact on privacy rights and should be subject to rigorous transparency oversight," Volz reports. "Her ruling validated a Freedom of Information Act lawsuit filed by the Electronic Privacy Information Center that last year made a 2010 government report on the database public and awarded the group nearly $20,000 in attorneys' fees. That government report revealed the FBI's facial-recognition technology could fail up to 20 percent of the time. Privacy groups believe that failure rate may be even higher, as a search can be considered successful if the correct suspect is listed within the top 50 candidates.

New cybersecurity tests coming for small banks and networks
-Small banks and the networks that serve the financial industry can expect tougher cybersecurity tests, a key regulator told an industry conference last week. "Regulators have been threatening to boost cybersecurity regulations as the financial sector moves to establish their own cyber threat info sharing programs," The Hill writes. "The government has encouraged the industry to adopt cyber information sharing programs."

In addition, federal banking regulators will soon scrutinize C-level executives and boards of directors at community banks and credit unions to gauge their cybersecurity awareness, according to GovInfoSecurity. "This news comes in the wake of the Federal Financial Institutions Examination Council's just-completed pilot program for cyber-risk assessments of community banks, which revealed a lack of understanding of emerging cyberthreats among many leading banking institution executives," writesTracey Kitten, on the upshot of an interview with Amy McHugh, an attorney and former FDIC IT examination analyst who now works as a banking consultant for CliftonLarsonAllen.

NIST publishes final version of report on cloud computing
-The National Institute of Standards and Technology (NIST) has published the final version of the US Government Cloud Computing Technology Roadmap, Volumes I and II. The roadmap focuses on strategic and tactical objectives to support the federal government's

accelerated adoption of cloud computing. This final document reflects the input from more than 200 comments on the initial draft received from around the world. The first volume, *High-Priority Requirements to Further USG Agency Cloud Computing Adoption*, describes the roadmap's purpose and scope. The draft focused on three priorities: security, interoperability (the ability for systems to work together) and portability (enabling data to be moved from one cloud system to another). Read more here.

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