the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

Cyber Maryland

October 29-30, 2014 Baltimore, MD

October 28

CyberMaryland opens in Baltimore tomorrow and continues through Thursday. Watch for CyberWire special issues and live tweets from the conference sessions. See the articles below for details on the conference, including speakers and sessions.

And, in observance of the National Cyber Security Hall of Fame's class of 2014 induction ceremonies this Thursday, the CyberWire will run an exclusive interview with one of the inductees, Richard A. Clarke.

October 29

CyberMaryland 2014 opened this morning. We'll be live tweeting from the conference — watch for the hashtag #CYBERMD2014.

Peter Bloom (Advisory Director, General Atlantic) opened the conference with a keynote on cyber situational awareness. Such situational awareness, he observed, is increasingly difficult to achieve given the rapid evolution (and arrival) of cyber threats and the challenges of recognizing the boundary conditions within which we operate.

He urged the conference to consider some "canaries in the mine" that indicate the near future of cyberspace. The first of these were the massive Russian cyber attacks on Estonia in 2007. 2012's "Night of Power" attacks on Saudi Aramco — which bricked some 30,000 endpoints — represent another canary, and one that Bloom believes has dangerously faded from memory. More recently, the subversion of SSL by hackers spoofing Dropbox was very disquieting, as are the currently circulating "probe and slurp" malware infesting the Android ecosystem. The increase in the exploitation of side-channel leakage in cyberspace should also place us on alert.

That said, Bloom noted some positive examples. Some come down to getting and staying inside an attacker's OODA loop. Estonia's excellent situational awareness (and ability and willingness to act upon it) enabled it to shut down an unprecedented nationwide DDOS attack, and remains an instructive standard for cyber defense. Real-time situational awareness is coming, arriving largely from the financial services sector. Other positive signs point to increasingly effective collaborative defense: the Novetta-led coalition that cleaned up Chinese-delivered malware is a very recent and heartening case of this. Technological advances, and their widespread adoption, also give reason for optimism. Tokenization and 2-factor authentication are essential technologies, available today. A less well-known measure is BitCoin's block chain, which, in the form of side chains, shows a way of enabling trustless transactions. The final positive trend Bloom discerns is the growth of cyber insurance. This is a rapidly maturing market, and it will bring greater rigor to cyber security.

We will continue our coverage of CyberMaryland 2014 tomorrow, with a conference wrap-up on Friday.

Tomorrow night, the National Cyber Security Hall of Fame will induct its class of 2014. The CyberWire will run an exclusive interview with one of the inductees, Richard A. Clarke, on Thursday morning. We'll also offer a recap of the ceremony in Friday's issue.

October 30

Yesterday's session included a "fireside chat" with Admiral Michael Rogers, NSA Director and Commander of Cybercom. He opened with a brief review of the NSA and Cybercom missions (not identical missions, he noted). He commented, with pleasure, on the commitment and seriousness of NSA personnel, and then turned to the challenges of developing a cyber labor force adequate to national needs. Industry plays an indispensible role in such development.

Rogers likes the NIST Framework, especially with respect to its growing influence on workforce development. The cyber workforce is a disparate one, even between Cybercom and NSA; the two organizations differ in their respective military and civilian balance (Cybercom tilting more toward uniformed personnel). Both recruit nationally.

When asked about technological innovation, Admiral Rogers stressed that partnerships with a wide range of entities are essential. The Department of Defense no longer drives technological advance. We look to the private sector for technology, and securing the benefits of innovation requires positive relationships with that sector. The challenge of innovation is creating an ethos that sees change as both essential and beneficial. An organization's large size can work against that ethos, and this must be compensated for.

One development that will demand innovative responses, Admiral Rogers argued, is the rise of the Internet-of-Things (IoT). The IoT represents fundamental change. We don't understand the effects of its connectivity or proliferation. We want the IoT's convenience, but it brings with it a tremendous vulnerability. What if, for example, we had an Ebola-like challenge in the Internet? How could it spread across the IoT? We need serious thought and research about these issues.

Turning to the policy challenges we confront in cyberspace, Admiral Rogers noted that in the US we have distinguished spheres proper to the private sector, civil government, and defense or security. But cyber, he said, blurs these lines. This means we need partnerships that address issues across these spheres. We need automated machine-to-machine threat information sharing. We've got to decide what information we need to share (and, he said, NSA and Cybercom don't want private information, shared or otherwise.) We'd like the private sector to get situational, predictive awareness from the government. We'd like the private sector to give the government feedback on what worked for them in defending their networks, and what didn't. We'd like the private sector to tell us what they're seeing in the way of malicious activity. We don't, he said, want to be in private networks. We do want to talk to and cooperate with them.

Admiral Rogers suggested that cyber awareness might best be built by working down from the largest, best-resourced enterprises. He's heard people at the US Chamber of Commerce say, in effect, that security is a collaborative, not a competitive, advantage.

The admiral concluded by posing some unanswered questions for discussion and debate. What, in a digital age, does privacy mean? What, in that age, does intellectual property mean? What about cyber war? We ask about the intent of an action to distinguish war from crime, but there are many gradations of appropriate response. Much discussion of these questions has, so far, has been incredibly simplistic. He praised the people who work at NSA for their ethos of adhering to the law, and he called for thoughtful, well-informed dialogue about how to achieve both freedom and security.

Yesterday's sessions concluded with announcement and recognition of the College and Professional team winners of the Maryland Cyber Challenge. The University of Maryland University College (UMUC) bore away both laurels: UMUC's Padawan Team 1 took the College Division, its Pro Team 2 the Professional. Winners of the High School Division will be announced late this afternoon.

Today's morning session began with a talk by Representative "Dutch" Ruppersberger (D-Maryland), who, after some pleasantries, asserted that the US faces severe challenges in

cyberspace. He sees these as representing an economic threat. Intelligence gathering is a legitimate government function — in any event, all governments collect — but China's current cyber operations are a different matter: they're engaged in the theft of intellectual property. Meeting the cyber challenge will require a well-trained, well-educated work force. He urged companies to boost the cyber work force by offering students internships that will get those students started on the process of gaining security clearances.

Representative Ruppersberger praised some pending cyber legislation. One of the more significant of these would enable easier sharing of cyber intelligence that might otherwise have been classified. He expressed his support for strong checks, balances, and oversight for the Intelligence Community. He praised legislation that supports privacy by restricting the bulk collection of telephonic data, and he closed with praise for the decency and professionalism of the Maryland-based NSA work force.

Representative Ruppersberger was succeeded at the podium by Maryland governor Martin O'Malley. After thanking the audience and praising trade's increase, the governor offered his take on taxation. Taxation, he argued, is something we collectively decide to do: specifically, it's an investment we make in common. Taxation properly invested can create a business ecosystem – as it is done, he asserted, in Maryland. He went on to suggest that those enamored by a low-tax society might consider the example of Yemen, which provides a look at life in a low-tax society. (He didn't directly describe Yemen as being in a Hobbesian state-of-nature, but that's the general tenor of the distinction he drew.)

After discussing the importance of cyber education (including the benefits of evolving common standards) to the future of the economy, Governor O'Malley concluded with a valediction to innovation in his home state and a call to continued investment.

Retired US Navy SEAL Lieutenant Jason Redman, who drew motivational lessons from his service, delivered the morning keynote. Severely wounded in Iraq, Lieutenant Redman analogized military problem solving under pressure to challenges faced in the cyber domain. He placed cyber conflict into the context of military history, describing the centrality of cyberspace to current and future warfare.

But Redman was most concerned to share lessons from his own experience of being wounded and brought back from the brink of death. The first of these is the importance of a determination to overcome adversity. He advised all to stay positive and lead, and to live life every day and not let fear deter you from doing so. Love deeply. Stay humble. And finally, live a life without regrets.

Tonight the National Cyber Security Hall of Fame inducts its class of 2014. The CyberWire has an exclusive interview with one of the inductees, Richard A. Clarke (CEO of Good Harbor Security), who offers a retrospective look at the work of the President's Review Group on Intelligence and Communications Technologies. Mr. Clarke served as one of the principals on that panel.

We'll wrap-up our coverage of CyberMaryland 2014 tomorrow with a final special edition.

October 30

CyberMaryland 2014 wrapped up yesterday with sessions devoted to technology transition, infrastructure security, business development and entrepreneurship, leadership roles for women and veterans in cyber security, cyber insurance and risk mitigation, cyber education and work force development, and, of course, perspectives on the cyber threat.

The conference closed with recognition of Maryland CyberChallenge's High School Division winners. Marshall Academy (Falls Church, Virginia) and Loyola Blakefield Blue Team (Baltimore, Maryland) shared the Perseverance Award. Each team member received, from the University of Maryland Baltimore County, either a complimentary security certification course (if they're 18 or older) or a complimentary summer development course (if they're under 18).

Second place was taken by Harford Technical High School (Bel Air, Maryland). Harford Tech's team members will each receive a $2000 education grant from NSA. This year's first-place winners were the students in Loyola Blakefield's Gold Team — they'll each receive a $5000 education grant from NSA. Congratulations, and well done to them all.

The National Cyber Security Hall of Fame inducted its class of 2014 yesterday evening. NSA and Cybercom chief Admiral Michael Rogers delivered a keynote in which he again called for new forms of partnership across worlds that ordinarily have little to do with one another, but that can share their passion and achieve a sense of common purpose. "You don't," he reminded the gathering, "have to wear a uniform to serve." Cyber, while a matter of paramount importance to national security, is paradoxically a domain that knows no boundaries, and this paradox should summon a new dialogue that moves beyond simplistic and ill-informed dog whistling about either liberty or security. He concluded with a call for mutual trust on the part of all cyber stakeholders, and reiterated his organizations' commitment to accountability, the rule of law, acknowledgement of mistakes, and a determination to never cut corners.

The five members of the class of 2014 all spoke briefly and gracefully.

Paul Kocher (designer of SSL 3) warned of three challenging trends: coding is faster, devices are proliferating rapidly, and data are assuming dramatically greater value. These give rise to exponentially larger problems, but to larger opportunities as well.

Vint Cerf (co-designer of TCP/IP, who spoke in absentia) — after confessing feelings of unworthiness of the award — counseled all to "think twice when we roam around the Web," and to always remember that our failures in cyberspace place others at risk.

Phillip Zimmermann (creator of PGP email encryption and developer of VOIP encryption protocols) noted that the law firm Venable was a sponsor of the evening's ceremonies, and recalled his own defense (pro bono) by a Venable attorney in the 1990s, when Zimmermann was under threat of indictment for his crypto work. When he asked the lawyer why he had taken his case, the lawyer answered: "I believe you should be able to whisper in someone's ear from a thousand miles away." Those words have stayed with him ever since. In the 1990s, Zimmermann reflected, you had to explain yourself if you were using strong crypto. Now, you have to explain yourself if you aren't – and that, he said, "is as it should be."

Steven Bellovin (professor of computer science at Columbia University and a major contributor to encryption and network security) described his realization that insecurity arose from increased system complexity, and that security must be understood and approached as a system problem.

Richard Clarke (former US National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, principally responsible for the first National Plan for Cyber Security) said he agreed with the current Chairman of the Joint Chiefs of Staff that the US needs a new strategy for cyberspace. He also urged those present to accept the invitation of Admiral Rogers to help explain the work of NSA, and to foster the dialogue that the Admiral called for.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.4.15