the cyberwire

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

SINET Innovation Summit

August 6-7, 2013 New York, New York

August 5

Solving the research transition problem: Dr. Douglas Maughan, Director of Cyber Security at the Department of Homeland Security's Science and Technology (S&T) Directorate, spoke with the CyberWire this morning about organizing research in ways that facilitate the transition to operational systems. He'll be moderating the Innovation Summit's panel on "Research Collaboration Models that Work" tomorrow afternoon.

Federal science and technology programs often find it difficult to move the results of research to the end users on whose behalf it's conducted. The challenge of transition is familiar to anyone involved with S&T, but Maughan believes the Department of Homeland Security (DHS) has found some workable models that overcome many of these problems.

In general, DHS S&T finds that involving prospective end-users in defining problems, setting requirements, and funding some of the research (and tests and evaluations) has greatly eased transition problems. Posing user-informed challenges to researchers and offering them early adopters for their products has done a great deal to channel research into eventual operational use. Maughan describes three successful public-private engagement models:

- **LOGIIC (Linking the Oil and Gas Industry to Improve Cyber Security).** In this program, companies in the oil and gas sector fund research and DHS S&T funds administration and management. The industry partners, via an agreement with the Automation Federation, pose cyber security challenges and then decide which research projects will receive support. This collaborative agreement is structured to avoid the anti-trust issues that often inhibit private-sector cooperation. LOGIIC is a unique public-private partnership that brings five major oil and gas competitors together to work with the government on the development and distribution of cybersecurity solutions for protecting the industry's critical infrastructure.
- **Industry-University Research Consortium**. A joint National Science Foundation and DHS S&T program, the consortium is housed in Ball State University's Security and Software Engineering Research Center. A dozen universities participate in addition to the private sector. Government agencies and private companies identify research challenges, universities propose research projects to address them, and the agencies and companies select the proposals to fund. The university performers tend to be highly capable institutions that are willing to focus on practical and hands-on operational solutions that they can deliver in the near term.
- **TCIPG (Trustworthy Cyber Infrastructure for the Power Grid)**. Hosted by the University of Illinois at Urbana-Champaign, this consortium brings together DHS, the Department of Energy, Dartmouth, Cornell, the University of California-Davis, and Washington State University. Funding is provided by the government and the universities themselves, but a key element of the program's success is its advisory board: some four hundred owners, operators, and vendors in the electrical power sector who collaborate with the university researchers. The advisory board's members set the research challenges and agree to act as early adopters of TCIPG technologies.

Maughan stresses the importance of a technology's ultimate users setting its research requirements, and notes the importance of intelligence in shaping those requirements. "We're not surprised by the claims made last week at Black Hat, or that critical infrastructure is of interest to attackers," he says. "We're interested in it from the defensive point of view, and we find that the technologies and techniques developed to defend control systems in the power sector have implications across critical infrastructures — some are using the same technologies — that can be of benefit to other infrastructure sectors. Tools developed to protect oil and gas infrastructure, for example, tend to be applicable to other infrastructures as well."

We'll be covering Dr. Maughan's panel tomorrow, along with the rest of the SINET Summit.

August 6

Frank Montoya, National Counterintelligence Executive, opened the conference this morning with a keynote address. Before placing counterintelligence into the context of cyber innovation, he lamented what he characterized as the current misrepresentation of Intelligence Community programs and activities—these are defensive, and not directed against US citizens. He was especially concerned to dispute claims of pervasive government surveillance of content, which he described as simply beyond any agency's human capacity.

He urged symposiasts to leave their preconceptions about counterintelligence behind. It's no longer trench coats and fedoras; the threat is not what it once was. Now, counterintelligence concerns itself with protecting supply chains, thwarting insider threats, and all other aspects of cyber security. Our lives are now online, and so the adversary is there as well. Cyber conflict is waged globally, and government depends upon industry for innovation. By law, the US government is committed to protecting American businesses from industrial espionage.

Finally, Montoya called for engagement—industry should bring its challenges and solutions to the government. Our law and our infrastructure must catch up with our technology. He concluded by drawing attention to the risk of neglecting STEM education in the United States.

The morning's first panel, "Federal Cybersecurity Opportunities for Small and Large Businesses," on which Deltek, NSA, Mocana Corporation, and DHS National Protection and Programs Directorate were represented, stressed the third phase of mobile technology as the coming need for the enterprise: security is the bottleneck to more widespread adoption.

John Mullen (Senior Operations Officer, CIA) spoke on the intersection of cyber security and human frailty. He began with three points: (1) Risk management strategies protect intellectual property. (2) Security programs aren't easy and don't generate revenue, but they will protect long-term viability and profits. (3) People represent the greatest cyber vulnerability any organization has – insiders facilitate 70-98% of information losses.

Mullen noted that tools used by foreign opposition to steal secrets include open source intelligence, an integrated (and state-sponsored or state-owned) approach, tradecraft, and organization. Their technology includes remote hacking, black-bag operations on mobile devices, and the supply chain itself.

Mullen observed that the traditional recruitment and compromise of people continues. Opposition intelligence services work hard to compromise insiders. And it's worth noting that people tend to be more open (with secrets, opinion, and secrets disguised as opinion) online than in person.

He advised companies to look at themselves and identify what's invaluable. What makes your organization unique? Who determines what is secret or what is proprietary in your company? Mullen concluded with a reminder that the opposition only needs to get it right once. Security and threat mitigation must be an integral part of every enterprise's regular operations.

The morning's final panel, on legislative action and executive orders affecting critical infrastructure protection, addressed emerging voluntary industry-driven standards and the forcing role regulation plays in material disclosure. European regulation differs from US regulation in that it's risk-based. In the US, regulation and legislation tend to issue in long lists of things that must be done. This fixation on compliance breeds compliance fatigue, over-lawyering, and concentration on doing the exact minimum. The US might look with profit at the European model.

We'll continue our coverage of SINET's Innovation Summit tomorrow. In the meantime, follow us on Twitter @thecyberwire for updates as the conference continues.

August 7

We continue our coverage of SINET's Innovation Summit, which concluded yesterday evening in New York. Here are some of the conference's highlights.

CIA Senior Operations Officer John Mullen took as his topic **the weakest link: the intersection of cyber and human frailty.** His talk emphasized cyber security's continuity with traditional intelligence and security tradecraft and dealt largely (and appropriately) with the threat to companies from foreign intelligence services. Protecting information is inconvenient but essential to an enterprise's long-term viability, and therefore organizations should anticipate and prepare for cyber attacks.

The tools used to steal secrets include open-source intelligence, integrated approaches to exploit diverse vulnerabilities, traditional tradecraft, and organizational compromise. One can expect the opposition to manipulate relationships under the direction of state agencies.

Expect the opposition to use remote hacking and black-bag operations on mobile devices. The supply chain is also an attack surface. Offensive intelligence operations are inherently dynamic; adaptive security is great, but it must be genuinely adaptive to a threat that responds, learns, and modifies its approach.

When you're abroad you're on the opposition's turf, and can expect that opposition to pursue and scrutinize you closely. The opposition aggressively targets people via, for example, blackmail, theft, and exploitation of their simple naiveté. Never lose physical control of devices abroad. Never accept files. Never use local services. Travelers' hotspots are typically active and aggressive sources of compromise.

Mullen emphasized that, in security, having one person make the decisions is always a bad thing. Get the right people around the table. Enunciating a theme other symposiasts would echo, he urged in effect a risk-based approach to security: identifying, before you engage foreign entities, exactly what you need to protect.

Finally, he reminded the conference that the CIA gives security briefings to US corporations upon request.

Bloomberg's Norman Pearlstine moderated a panel that discussed **how legislation and executive orders might improve the security of critical infrastructure**. Panelists pointed out that standards are evolved in a voluntary, industry-led process, and that the government serves more as a partner than a director in many such efforts.

In general, US regulatory approaches tend to be compliance-based, which some think tends to drive security toward a minimum set of requirements. Panelists suggested a look at the European approach, which tends to be risk-based. Keeping up with evolving legislation and regulation is difficult, but the consensus was that social media and open news outlets provided the best way of staying current. One warning that would resurface throughout the day was the risk to information sharing that over-classification posed.

Afternoon sessions began with Doug Maughan (DHS S&T cyber lead) and his panel on **successful models of public-private research collaboration**, which we covered in Monday's issue. The panelists agreed on the importance of having end-users set challenges and requirements. The three programs represented, S2ERC, TCIPG, and LOGIIC, noted that solutions that evolved in one economic sector often have ready applicability to others. They also noted the role of DHS in overcoming regulatory barriers to cooperation.

Columbia's Salvatore Stolfo opened a discussion of **transitioning federally funded university research to markets**. He began with an anecdote – microbiologists say that bacteria devote 30% of their resources to securing themselves; thus, germs are twice as committed to security as the Federal IT budget.

He and some of his colleagues described some of Columbia's work on "beaconizing" documents, placing them in locations where they can be exfiltrated, and then using the resultant beacons to gather attack telemetry. He characterized this approach as "data loss alerting": innocuous files flow out and then report back. This kind of technology fills a gap in adversary intelligence necessary for threat-based, as opposed to vulnerability-based, security. Other Columbia research has produced virtual containers to isolate attacks as well as software tools to identity vulnerabilities and malware embedded in hardware devices.

Stolfo's reflections on technology transition focused on impediments to commercialization imposed by an academic culture that devalues short-term impact and academic legal practices that emphasize licensing patents. Treating university patent offices as a revenue source is the beginning of a misalignment between academic and entrepreneurial cultures. And, finally, successful transition necessarily involves people: the wetware must be transitioned along with the hardware and software.

After the panels' addressing **security for the boardroom and hardware-enforced security for the "Internet of Everything"**, Dawn Meyerriecks, the CIA's Deputy Director for Science and Technology, delivered the closing keynote on **technological innovation for intelligence and security.** She began by noting technology's democratization, a long-term trend that places capabilities once limited to well-resourced nation-states into the hands of poorer states and non-state actors. It's easy to profile a target, and we face adversaries who are capable and determined.

The Intelligence Community is well served by two innovation engines, In-Q-Tel (the venture fund that wants technology, not IP) and IARPA (an analogue to DARPA that invests in analysis, secure operations, and smart collection). She outlined some particular programs, several of them involved with improving socio-cultural context for natural language processing and different modes of detecting and overcoming cognitive bias and groupthink.

Two points were striking: first, her characterization of large-scale data ingestion as "wildly impractical – it doesn't scale," and second, her interest in bringing automation to analysis, particularly in ways that would tend to reduce analytical errors. (And, finally, she lost no opportunity to point out how the Intelligence Community was delivering good value for taxpayer dollars.)

We'll conclude our coverage of SINET's innovation Summit in tomorrow's issue. In the meantime, please note that SINET's next event, SINET Showcase: THE SINET 16, will meet in Washington at the beginning of December. We mention it here because applications for recognition as one of the SINET 16 close next week, on August 15. Supported by the Department of Homeland Security, Science & Technology Directorate, the Showcase puts industry's most innovative global entrepreneurs in front of 350 sophisticated investors, buyers, and researchers from commercial and government markets.

August 8

We conclude our coverage of SINET's Innovation Summit with two interviews, one with Chertoff Group Principal Mark Weatherford, the other with Mach37's Managing Partner Rick Gordon.

Mark Weatherford on information-sharing and workforce development.

The CyberWire: *How would you rate the ongoing effort to improve public-private information sharing?*

Weatherford: *I think the "effort" to improve information sharing has been heartfelt, but "success" has been harder to substantiate. One reason is that there are so many organizations playing in the sandbox, the private sector oftentimes doesn't know who the right organization they should be sharing with. Thinking narrowly about cyber security threat information sharing, you have US-CERT at DHS, the US Secret Service, the FBI, DoD, state fusion centers, local law enforcement, sector-specific Information Sharing and Analysis Centers (ISACs), and even many private sector organizations. It can be very confusing. I think the government has made a lot of progress in the past year or so, mostly in response to some of the cyber-related activity focused on the United States, but it's still a challenge and there's still some wariness on the part of the private sector. The president's recent executive order, and specifically the recently announced "incentives" initiative, could have a very positive impact on public-private cyber security information sharing.*

The CyberWire: *What obstacles do you think remain, and what ongoing efforts would you like to make people aware of?*

Weatherford: *TRUST. Trust continues to be the biggest obstacle. I read a blog by retired General Stanley McChrystal the other day where he talked about trust. In it, he said to invest early and often in relationships, and trust will follow. That is a profound truism. The government needs to continue investing in relationships with the private sector, and not just from a "check the box, we talked to them" perspective but real, sincere relationships where the goal is to improve everyone's enterprise knowledge about cyber security risks. I think the ISACs are another area where the government could make some real, tangible improvements. The ISAC's were a result of Presidential Decision Directive 63 in 1998, which called for action within critical infrastructure companies. Unfortunately, there has never been much support from the government to create a consistent and repeatable model for what an ISAC looks like and how it operates. A privately operated non-profit ISAC organization funded (at least partially) by the government for each of the 16 critical infrastructure sectors would be hugely beneficial to the nation and could serve as an aggregation point for critical cyber security information sharing.*

The CyberWire: *Building a "cutting-edge" cyber workforce is generally recognized as a challenge. What measures would you recommend we take, as an industry, to meet it?*

Weatherford: *Make the development of cybersecurity talent a national priority. It gets great lip service but most government organizations and private companies do very little to actually invest in growing talent, finding it easier to poach people from each other. So while I think a certain amount of workforce transition is healthy, too much exacerbates the problem because it means we are losing valuable institutional knowledge. It's shortsighted and doesn't prepare us for the future, which will eventually have serious economic consequences for the nation. Companies should obviously be funding internal training for current staff, but more importantly they should be supporting external programs like the US Cyber Challenge, the Air Force Association's CyberPatriot Program, and others to help grow the next generation of cyber security professionals. I also think it makes sense to begin thinking about adding a cyber component to the national STEM program - the situation is becoming that dire. There are dozens of answers for how industry can help address this problem, but it requires a laser focus and the time is now.*

Rick Gordon with advice to early-stage cyber startups.

The CyberWire: *So, how would you describe a business accelerator?*

Gordon: *We focus on very early-stage cyber companies. Through the CIT GAP Fund, we offer an initial investment of $25k to help cover an entrepreneur's expenses during our three-month program. During those three months, we work with the company to answer three critical questions tech start-ups can tend to overlook: 1) What business problem are they solving, and is there an attractive market? 2) Is the problem being solved uniquely by them? and 3) Who would buy the product, and at what price? Once they get through the program, if certain milestones are met, the CIT GAP Fund will offer an additional $100k in additional investment.*

The CyberWire: *What do you try to get from a start-up's prospective customers?*

Gordon: *We look for unambiguous market validation – willingness to alpha test, beta test – and we also look for an interest in buying the product at a realistic price point. Taking market risk off the table for investors will be reflected in significantly increased valuations of our companies by the end of the program.*

The CyberWire: *Some incubators merely offer low rents or even free occupancy for surplus office space, and that kind of hoteling's clearly not what you're doing.*

Gordon: *Right. While we do provide them with operating space, our process is consultative, bespoke, and intensively focused on creating value for the entrepreneur.*

The CyberWire: *Will you take an equity stake in the companies in your portfolio?*

Gordon: *We will – a 7% stake is our model.*

The CyberWire: *What would you like prospective cyber entrepreneurs to know?*

Gordon: *Since we're meeting on a university campus, and have just heard from panelists who know something about the challenges of transitioning technology from universities to markets, I'd like to expand on some themes they've already sounded. Developing an enterprise security product takes more investment capital than most of them think. In particular, we often have discussions with academic researchers who can be a little naïve about what it takes to deliver to market a product that is reliable, easy to use, and easy to deploy and upgrade. In general, they assume that R&D-oriented funding (SBIR grants for example) is adequate. The best they can expect from those sources is a working prototype, but that's not the same as an enterprise-ready product.*

We see a variation of this with small consulting shops as well, where they see a need they think they can address with a product but then elect to invest cash flow from services instead of raising adequate capital. This greatly lengthens their development process, and, inevitably, they find they're not quick enough to market – someone's beaten them to it. Service-oriented businesses often fail to realize they are usually competing against time.

The CyberWire: *Is cyber different from other technology sectors?*

Gordon: *In some ways it is. The cyber entrepreneurs usually aren't twenty-somethings writing mobile apps. There are some twenty-somethings, but they're not typical. Typical cyber technologists are older with significant domain expertise. However, with that age and experience come added responsibilities – family, financial commitments, and so on – that stereotypical twenty-somethings do not have. We have found these responsibilities often make it difficult for cyber technologists to take the leap into entrepreneurship and we are focused on making that leap easier.*

The CyberWire: *As you work with entrepreneurs and the venture capital community, how would you like to see their opinions and ways of doing business evolve?*

Gordon: *I'd hope to see VCs realize that it's not necessary to get cyber security start-ups in our area to relocate elsewhere. We see this too often as a condition of investment where VC's, on the West Coast for example, expect a company to pull up stakes and head for Silicon Valley. It's unnecessary and counterproductive given the rich density of cyber security expertise that exists in the Virginia-Maryland-DC region. And, it's particularly difficult for entrepreneurs who are more mature and are already integrated into their communities.*

We also hope to collaborate more with our colleagues in Maryland and DC in this regard. While we are a part of the Virginia Center for Innovative Technology, I don't view similar efforts in Maryland and DC as competitive. Sometimes I see a misguided parochialism between Maryland and Virginia, but it's my belief that developing the cyber economy in either state is mutually beneficial.

I'm hoping, by the way, that the SINET 16 event helps foster some of these changes.

Final notes on SINET's Innovation Summit.

Our thanks to Mssrs. Weatherford and Gordon for their time and their thoughtful remarks. We'd be remiss if we didn't pick up on the occasion they've given us to mention two worthwhile upcoming events. Cyber Maryland's Cyber Challenge, which will provide the rising cyber generation a chance to show its stuff, meets in Baltimore on October 8 and 9. And applications for recognition as one of the cyber innovation-leading SINET 16 close next week, on August 15.

The CyberWire resumes its customary daily form with tomorrow's issue. Thanks to SINET for an interesting and productive program at the Innovation Summit.

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