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

6th Annual Billington Cybersecurity Summit

September 17, 2015 Washington, DC

Several clear themes emerged at this sixth annual Billington summit. The adversaries' tradecraft is getting better, but "better" isn't necessarily synonymous with "novel" or "innovative." Rather, we see familiar exploits used successfully against known vulnerabilities. The economics of cyber conflict don't favor the defender. Attackers in many parts of the world face negligable risks and very low barriers to entry as hacking tools become increasingly commodified. And individual hackers scale well, at small expense easily imposing great costs on their targets. Defenders should understand that cyber security is essentially an exercise in risk management, especially management of consequences, and that risk will never be driven down to zero. Finally, many of the presenters looked to the still immature cyber insurance market as the best and likeliest source of improved security and risk management across all sectors.

Cybersecurity Priorities of the Department of Defense CIO

Stuart McClure (Cylance CEO) introduced the opening keynote by US Department of Defense Chief Information Officer Terry Halvorsen. Halvorsen's key concerns with respect to cyber security are cultural and economic.

Cyberspace, he explained, is a warfare area, but a different one: it differs from the traditional domains of land, sea, air, and space in the speed with which operations take place there—obviously very fast. Those who would operate in cyberspace need a distinctive culture, and the domain's combination of familiarity and poor understanding (it's ubiquitous, and we spend time there every day for the most ordinary purposes) make development of the right culture especially problematic.

Halvorsen, then, isn't concerned about resources ("Budget turmoil isn't unusual: we'll spend a lot of money on cyber"). But he worries about getting cyber culture right. He sees cyber "discipline" as important for the nation as a whole: we should think about how to make a culture in which people are held accountable for cyber effects they bring about (deliberately or not). There are interesting analogies between cyber operations and the early days of military aviation. In both cases it takes time to stand up the right culture of safety, reliability, effectiveness, and so on.

Cyberspace is not just a warfare area, but a business area, and Halvorsen thinks we're currently "on the wrong side of the cyber economic curve." Adversaries can spend a little and cause us to spend a lot. "We need to raise barriers to attackers' entry," he argued, "making it more expensive to play. It will be tough to raise that barrier."

In response to a question about autonomy, Halvorsen acknowledged that learning systems capable of autonomy are needed to cope with the speed of the threat. They also have great potential for data analytics. "We do not lack for information. We lack actionable intelligence that would enable us to stop threats."

Halvorsen closed with responses to questions about cyber self-defense and arms control He thinks that working out the implications of a right to cyber self-defense is part of building cyber

culture. And instead of cyber arms control treaties, he thinks a more productive route would be development of international standards of conduct for cyberspace. "These are feasible, but they're not going to be achieved soon, or easily."

Cybersecurity Post-OPM: What Do We Do Now?

Cheri McGuire (Vice President, Global Government Affairs and Cybersecurity Policy, Symantec) moderated a panel composed of General (retired) Michael Hayden (former Director of Central Intelligence and the National Security Agency, now a Principal with the Chertoff Group), Jack Harrington (Vice President, Cybersecurity and Special Missions, Raytheon), Nir Peleg (Head, Research and Development Division, Israel National Cyber Bureau), Michael Daniel (Special Assistant to the President and Cybersecurity Coordinator, the White House), and Robert Bigman (former CISO, Central Intelligence Agency, now President, 2BSecure).

McGuire opened by painting a grim if familiar picture of a threat environment in which the attackers seem to enjoy all the advantages, and then turned to the panel with the wan hope of extracting some optimism. Daniel (who would later demur "I'm not exactly the bluebird of happiness at NSC meetings") offered more reinforcement of pessimism than he could optimism. He noted the rapid increase of threat surfaces, and the industrialization of hacking, which has also grown more destructive. And finally, he said, "We're witnessing the development of cyber as a tool for statecraft." Our cyber environment will only grow more contentious.

Hayden shared Daniel's dark view, but tempered it with optimism: he's "modestly hopeful" because "we're now seized of the issue." For example, the prospect of sanctions laid out in a recent Executive Order and the policy directions enunciated in Defense Secretary Carter's speech at Stanford are hopeful signs. But we cannot expect the government to lead in this domain. Social norms, technology, law, and policy are changing at very different speeds, and Hayden thinks the government will always be behind. "The center of cyber response will be in the private sector, with government relegated to doing that which only it can do."

The conference didn't hear much optimism from Peleg, either, who contrasted the defender's challenges (legacy systems, multiple supply chain dependencies, disparate network governance) with the attackers' limited risk and rapidly advancing tradecraft. That tradecraft can use commodity attacks against known vulnerabilities. As long as these still work, why not? "'APT' now means 'adequate persistent threat'."

Recognizing that we're at way, Raytheon's Harrington said, is the beginning of clarity. We're under attack by criminals, hacktivists, terrorists, and states, more than a hundred of whom are building a cyber capability. "The cyber arms race is on," he said, and noted that with international actors upping their game, we need tight relationships with our allies.

2BSecure's Bigman thinks things are worse than his fellow panelists believe. "We need to get serious," he said, and pointed out that OPM, pre-breach, was FISMA compliant. He called for industry to build secure operating systems, and for the Government to get "more granular" in its internal guidance.

After these gloomy (if realistic) estimates of the situation, McGuire again asked for reason to hope. Daniel did think we'll eventually get better, but cautioned that things will get worse, or at least seem to get worse, before that happens. This is to a significant extent due to a good thing: we're getting better at detecting and recognizing attacks.

Harrington, quoting an acquaintance in the FBI, pointed out that we haven't solved physical crime, and so what makes us think we'll solve cyber crime? But he does expect some good results from better training, improved cyber hygiene, and (especially) self-healing systems.

Observing that we've been talking about these problems for years, McGuire asked the panel how we could accelerate innovation for better security. Peleg thought that innovation came from necessity, and advised the conference to consider investment in developing the right ecosystem in which such innovation can occur. More organizations, he said, understand the need for innovation as they see how a compromised data center can destroy a business. One fruitful area for innovation is in developing the right techniques and training to cut through the glare of too much unanalyzed data.

Bigman thought the success of the trusted computing program offers both a model for innovation and an illustration of a positive role for government. Hackers fear secure firmware and operating systems, and much good could come from advances along these lines.

Daniel noted that the challenge isn't purely a technical one. Most intrusions rely on known, fixable vulnerabilities, which means we don't understand the incentives. Cyber insurance markets will clearly play a big role in driving improvements to security.

Government, said Hayden, does have an important role to play, "but government is a supporting command—the private sector is the supported command." More enabler than doer, government should conform its movements to the private sector. He likes the idea of government removing penalties for information sharing, but he thinks a strong government hand in enforcing compliance could prove self-defeating, especially given how slow the positive effects of compliance can be. "We need active defense, not compliance." He called for creation of a business model that would incentivize security, and joined Daniel in pointing to the insurance market.

Bigman cited the Underwriters Laboratory (UL) as a model. He thinks we need a "Manhattan-style project" to develop the UL-like standards he advocates. "We created this; we can fix it."

Hayden called on enterprises to become smarter consumers. "Take cloud migration—it's giving us a security mulligan. We should take advantage of it."

Taking up the question of government's role in fostering security innovation, Daniel observed that "we don't have a good process in government for thinking of IT as a capital investment, as opposed to a maintenance one."

A question about what Google might be doing right, and what it could do better, with respect to security, prompted Harrington to say he thought the company was doing much good work is on hard problems, and that they're properly investing a lot in cyber security. He noted the importance for industry as a whole in addressing cyber labor shortages. Hayden thought Google a good example of the important contributions private companies can make to setting policy. (And he pointed out a historical percent for this: British foreign policy in the 18th and 19th Centuries would have been unthinkable without the participation of the East India Company.)

Daniel cautioned that security cannot be bolted on, and that it's always essentially an exercise in risk management—we'll never drive risk to zero.

A question from the audience, directed at Hayden, asked whether proposed sanctions against Chinese hackers were a good idea. Hayden offered an enthusiastic and emphatic "Yes!" He thinks the Executive Order concerning sanction is brilliant, and that sanctions are "a natural." But Bigman was markedly less sanguine. He observed that most cyber crime comes, after all, from criminal elements, and that as long as criminals can continue to monetize hacking, it will continue, sanctions or no. And cyber crime now appears to be more lucrative than drug trafficking.

Asked about security incentives for business, and whether such incentives should be global, Daniel thought it a complex area. He's never seen a purely domestic issue raised at the National Security Council. He did note the importance of small entrepreneurs. "Out-googling

Google is a fool's errand," but huge entrepreneurial possibilities are open in cyber security. Hayden recommended building international norms from insider out, starting with the 5 Eyes, which he characterized as "like-minded, like-valued nations."

The panel wrapped up with a discussion of why (as the questioner put it) has the cyber insurance market failed to flourish? Daniel thought the basic cause was the continuing lack of actuarial data on risk and response. The NIST Framework will help the cyber insurance market, but we're still building the risk information base. Hayden expressed the view that governments should act as second insurers until the private sector market gets on its feet.

Speaking for the Victims, with a Look Back and a Look Ahead

Kevin Mandia (FireEye President) delivered the day's second keynote. He promised to speak for the victims of cyber attack—themselves too often misunderstood—reviewing the recent past and looking to the future.

The principal lesson he wanted to draw for the conference was one other presenters had and would continue to take up: "There are few risks or repercussions for the attackers." In part this is because there are simply too many safe havens for hackers. If you're in Iran, Syria, China, or Russia, you probably face no risk whatsover for hacking American targets. "The bad guys are in risk-free game time all the time. This makes their game better." This fundamental assymetry in cyberspace between offense and defense has created an imbalance of power.

Attackers exploit trust within organizations, and their operationalized spearphishing is highly targeted and tough to detect. There's no patch for exploitation of trust. And the state attackers we face have got the language skills to be convincing.

Looking at the economics of hacking, Mandia finds that individual hackers scale very well. Their cyber-crime tradecraft has improved drastically. Nation-states have been purging, as opposed to wiping, logs as they cover their tracks. Crooks now do so too, and "it's not good when cyber criminals do counter-forensics."

Disclosure has become more general, he thinks. But most organizations did not get to disclose on their own terms. Many of them still find out they've been breached from bloggers or the media, and so they're usually disclosing prematurely, before they've been able to understand what's hit them, and what the implications of the incident are. "We all need to figure out how to disclose during the fog of war, when everyone knows about it at the same time you do." Detection efficacy is weaker in the cyber kill chain's later stages. We've gotten good at exploit detection, but not at detecting lateral movement.

90% of the attacks FireEye works on are from Russia, China, or Iran. Cyber activities signal the intentions of nation states. When we, the US, failed to punish (as promised) chemical weapon use in Syria, SEA activity spiked. In Mandia's opinion, every zero-day discovered over the last two years was sprung by a nation state.

He offered some observation on what's working: creation of secure enclaves, credential management, dry runs of response plans, phishing prevention programs, requiring two-factor authentication, and permitting only authorized programs to run on servers. He also advised using newly available technology to block advanced malware, and urged enterprises to promote "a security culture."

2015 represents an inflection point. As a country we haven't figured out defense versus deterrence in cyberspace. Why should healthcare, entertainment, and media companies be expected to withstand a military cyber attack? He recommended a capability progression: first, defend government infrastructure, second, inform the the private sector, and third, explore deterrence, attribution and retaliation. Some of the retaliation may well be non-cyber

(presumably financial, legal, or even kinetic) but it should always be proportional to the initial attack. Attribution is a precondition for deterrence. Attribution also enables proportional response. Above all, accurate, timely attribution is critical for influencing opinion.

Beyond "Detection and Response" to Prevention: the New Cybersecurity Paradigm?

Moderated by Cylance CEO Stuart McClure, the panel included Curtis Dukes (Director, Information Assurance Directorate, US National Security Agency), Eric Sporro (Acting Deputy Assistant Director, Cyber Division, US Federal Bureau of Investigation), Suzanne Spaulding (Under Secretary, National Protection and Programs Directorate, US Department of Homeland Security), Dr. James Kilbride (Director of Technology, Cyber Systems, General Dynamics Mission Systems), and Tony Spinelli (Senior Vice President, CISO, Capital One Financial Corporation).

McClure set the discussion with a cautionary tale of one CISO who told him he didn't want prevention, just faster clean up. "This means we've created a broken industry." So, he asked the panel, is prevention really impossible?

We're not at the future crime enforcement we see in the movie "Minority Report," Spinelli said, That would indeed be a high bar to set, and in many ways an undesirable one. Prevention is about the data. Since this is the case, we need to think of the problem of prevention as a big data problem. And therefore we also need to think about faster processing, and about processing data on ingest. These may move us closer to prediction.

Dukes thought our goals should be to prevent, interdict, find, and evict. It's difficult to stop initial access, but you can limit the adversary's actions. Really, the adversary today doesn't have to use zero-days. It's just too easy to get to key information from initial access. 80% of our problems could be prevented through good patching, sound configuration, and knowing what's on your network.

"Prevention," in Kilbride's view, "should focus on preventing damage, not on preventing access." Preventing damage is "very doable." Spaulding agreed: "We're engaged in risk management, not risk elimination. Curtis [Dukes] is exactly right—good cyber hygiene could prevent 80-90% of the problems we face."

From a law enforcement perspective, Sporro thought that we should aspire to infiltrate cyber criminal organizations. Good HUMINT and sound counterintelligence help here.

McClure took up the panel's observations about the importance of cyber hygiene. "There's very little—no?—new tradecraft in hacking. Preventable hacks are more in the 99% than the 90% range. So why are we finding it so hard to apply basic hygiene?" Spinelli answered by returning to his earlier point about the importance of speed in defense. "Our security tradecraft should be at least as artful as the attackers'."

Kilbride stressed the overwhelming importance of human usability. Our security must be easy to use. It must be adapted to human behavior. Dukes agreed, and pointed out the natural tension between security and usability. "There is, for instance, no 'easy button' for patch management."

So, McClure, summed up, security needs to be as invisible to the user as possible. What about artificial intelligence? He asked the panelists where they've seen it applied, and how it could address usability. Kilbride saw AI's great potential in doing the heavy math that would enable humans to focus. He'd like to see the adaptation of techniques from, for example, computational biology, to the cyber space.

To the FBI's Sporro, McClure said, "You've been great, but how can you anonymize some of the more interesting information you have for sharing?" Sporro thought there were practical approaches to doing this that would protect sources, methods, and law enforcement equities.

But he thought that the best way to foster effective information sharing was for businesses to establish and maintain continuing partnership with FBI field offices. Spaulding believed the Government has made great strides in equity review, and in implementing appropriate privacy controls. Kilbride reminded the panel that attack data were also useful in risk management.

New Capabilities for a New Domain

Lieutenant General James "Kevin" McLaughlin, Deputy Commander, US Cyber Command, delivered the afternoon keynote.

Describing creation of a new capability in a new domain, he noted that Cyber Command is employing its new units even before they reach initial operating capability. "We're putting a force into the fight, but it's a young force." Cyber Command is also creating and maturing a construct for planning. Authorities have been shaped, and are in place.

In today's world, the threat is a constant, and our focus is necessarily on achieving resilience through layered defenses. McLaughlin has been gratified by the general absence he's seen of squabbling over roles and missions. "Job one is defending the DoD." After this, he said, "Our job is also to provide full-spectrum military effects to our combatant commanders. The same C2 structure, these young units, are being tasked by combatant commands. Our teams are out there right now."

The Command's third broad goal is to be prepared, when called upon, to defend the US from attack. From a policy and legal perspective, McLaughlin noted, this role is the least fleshed out of the three. It's a "be-ready" mission, and Cyber Command is learning, through exercises, how this may work out.

"Partnership in cyberspace isn't trite, and it isn't a throwaway line. Our interdependencies mean you can't be turf-oriented." Within the Department of Defense, Cyber Command's direct, everyday partner is the DoD CIO, and that CIO and the Director of the NSA are well aligned. "Real issues rise to the surface quickly when you're not concerned about turf." He said that Cyber Command shares best practices, tactics, techniques, and procedures freely with partners in the Government.

In response to a question from the audience, McLaughlin said that he found retention of cyber talent more challenging than recruiting it.

One of the morning's panelists, James Kilbride, asked whether McLaughlin thought it possible to change distrust and misperceptions about military cyber. McLaughlin answered by saying that we work transparently and legally. "But, he elaborated, "that's DC technospeak." We try to engage, to get our story out to colleges to help inspire trust that we can be both effective and compliant.

Asked about OPM breach, McLaughlin said he's as unhappy as anyone else, but the personal threat is now something we deal with. Professionally, however, OPM (not Cyber Command's responsibility, he carefully noted) has caused us to think hard about key data repositories.

Government CIO Priorities to Enhance US Cybersecurity

Earl Matthews (CISSP, Vice President, Enterprise Security Solutions, Enterprise Services, US Public Sector, HP, and former Director, Cyberspace Operations, Office of Information Dominance, Office of the CIO, US Air Force) moderated this panel. Participants included Karl Matthias (CIO, US Marshals Service), Major General Garrett Yee (US Army), Michael Johnson (CIO, US Department of Energy), and Rear Admiral (retired) David SImpson (Chief, Public Safety and Homeland Security Bureau, US Federal Communications Commission).

Matthews began with a question about CIO budgets. Yee said, "We've needed a finer pencil

recently," and that, to get a capability, we often have to ask what we need to give up? "We're tech refreshing fewer items over time, and learning from our sister services how to shrink down what we're buying." Mathias observed that organizations with an operational mission make IT/non-IT trade-offs, too.

These constraints occur in the private sector as well, Simpson reminded his Government colleagues. "Don't underestimate how thinly resourced many companies are." He's met broadband companies with five—five—employees. Do you think they have a large and dedicated security staff?

"We heard," Matthews said, "Kevin Mandia talk about the human element. What are some of you initiatives in this area?" Yee thought we had to change our culture "at so many levels." He described US Military Academy cadets now being commisioned into the still-new Cyber branch. Simpson noted that one could change a culture through recruiting younger talent, but that the reality is that you won't be good at cyber "until you recognize that you own it, and until it's aligned with your mission." He went on to add that, in the communication sector, "We believe the marketplace is the right accountability mechanism." Companies need to have, in their ranks, a strong sense of cyber accountability.

Mathias looked at the audience (in which, presumably, CISOs and their posses were heavily over-represented). "You don't realize this," he told them (to considerable laughter), "but you're the enemy. My CIO staff constantly complains about the CISO slowing them down." So cultural change is needed in the CIO's shop. CIOs must lead, and bring the security culture to their own people.

Johnson agreed, and thought that part of the Government's CIO problem was apathy, and apathy at the CIO level. You're happy, unfortunately, if an incident falls below level of what's reportable to Congress, and you simply move on, thereby missing a chance to improve.

A questioner asked about the analogy drawn several times during the day between securty measures and seatbelts. "Go back to your seatbelt analogy—seatbelts are easy to use; cyber tools aren't. What are you doing about this?" This prompted a reflection by Yee on the more punitive aspects of instilling good cyber habits and practices. These, like enforced seatbelt laws, get people's attention. "Repeated action is required—that's how the military changes culture." Johnson liked the seatbelt analogy, but thought it easily misunderstood. "You forget that the issue of belts wasn't ease of use, but restriction of freedom." From an IT modernization standpoint, he argued, we should emphasize infrastructure as a service (with appropriate hygiene). And Simpson substantially agreed: "In some parts of the mobile environment, you shouldn't have to think about cyber security. It should just happen for you."

An Overview of a Young Command

Brigadier General Robert Skinner (Deputy Commander, Joint Force Headquarters, Department of Defense Information Networks) delivered the afternoon's second keynote. He explained the challenge of balancing risk with operational capability throughout the cyber domain. "We hold decisive advantages in other four domains, " he said, but not necessarily in cyberspace.

He saw great scope for partnership with industry and universities. "We have a suboptimized technology architecture. We're working on this, with industry partners."

Encryption: Point and Counterpoint

Robert Bigman (President, 2BSecure) moderated this two-person panel, holding the ring for Jon Callas (CTO and Co-Founder, Silent CIrcle) and Richard "Dickie" George (Senior Advisor for Cybersecurity, the Johns Hopkins University Applied Physics Laboratory). The panel's topic is the "great" difficulty of securely implementing encryption.

Bigman began by noting that some people are proposing a return to escrowed keys, or to using escrowed data. What are the panelists' thoughts on this? George expects such proposals to receive significant pushback. The obstacles to escrowing are political and procedural, not technical. But it is hard to design such a system that no one else could get into. Callas described escrowing as, essentially, setting up a privileged party. "And 'trusted party' means 'weak point'."

To a question about advances in quantum computing—are you worried about them?—George answered "Yes—especially on the commercial side. We aren't ready." Callas agreed that we weren't ready, "but I don't view this as a problem" because when we get quantum computing, it won't arrive as a surprise. "We don't use quantum-resistant encryption now because it's big and slow." George thinks we'll see breakthroughs, but that we don't yet really know the capabilities of the quantum computer.

"All-Star Military Cyber Commanders and Leaders Roundtable"

Shawn Purvis (Vice President and General Manager, Cyber Division, Northrop Grumman Information Systems) facilitated the conference's final panel. Her interlocutors were Vice Admiral Jan Tighe (Commander, US Fleet Cyber Command, and Commander, 10th Fleet), Lieutenant General Edward Cardon (Commander, US Army Cyber Command), Major General Burke "Ed" Wilson (Commander, 24th Air Force, and Commander, Air Forces Cyber, Joint Base San Antonio-Lackland), and Chris Inglis (Distinguished Visiting Professor in Cyber Security Studies, US Naval Academy, and former Deputy Director, US National Security Agency).

Tighe summarized the challenge as the speed of the adversary's evolution. She described how the Navy was actively recruiting to meet its future needs, and explained some of the aptitude testing they were engaged in.

Wilson addressed rapid acquisition issues, matters of considerable importance for cyber commands. Smaller acquisitions can be more agile. Big programs are effectively limited to traditional acquisition pathways. His command has some fast-tracking prototype authority for emergent needs.

Cardon said that experiments at the Combat Training Centers have been eye-opening. Electronic warfare and information operations are converging in the cyber domain.

The key piece in cyberspace is people, Inglis observed, which means we need to properly equip them. We need an "all, many, few approach," but we also need general involvement. The young, he finds, especially as he teaches midshipmen, know how to use computers ("they're all power users) but they don't (because they haven't needed to) know how computers work, what goes into them, and so on. Thus the Naval Academy requires two cyber courses of all midshipmen, teaching them not only technology, but ethics, history, and an understanding of the human dimensions of this domain. We teach cyber not for cyber's sake, but for the sake of operations.

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 10.13.15