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

# Borderless Cyber 2015

September 15-16, 2015 Washington, DC

*Borderless Cyber 2015 convened at the World Bank in Washington, DC, on September 15, 2015. Organized by OASIS, the not-for-profit open standards organization, the conference addressed the challenges and opportunities cyber information sharing presents internationally.*

*World Bank Sr. Director Pierre Guslain opened the conference with an invitation for the cyber security industry to address the challenges of creating culture of security worldwide, fostering joint approaches, standards. His brief remarks concluded with a call to partnership in serving the cyber needs of the developing world.*

*OASIS General Counsel Jamie Clark welcomed the symposiasts, thanked the World Bank, and, before introducing the day's speakers, praised the community's progress in open source standards.*

## September 15

### Our Cyber Security Landscape: The need to prioritize today and tomorrow

Jonathan Litchman, Co-Founder and CEO, the Providence Group. Communicating about the threat, he argued, is a fundamentally human endeavor that occurs only against a background of trust: people are persuaded only by trusted messengers. He outlined how the current landscape of the cyber domain affects that human transaction.

He sees five current trends. The first is convergence: the ways in which threat actors, whether criminal, hacktivist, or state-controlled, have come to resemble one another. The second is velocity: the speed with which attack surfaces now increase is staggering. Gravity, the increasing size and impact of cyber incidents, is the third trend. The fourth trend Litchman called "imbalance": the attackers are becoming increasingly sophisticated and successful, across many sectors, and their advantage over defenders grows correspondingly. The fifth trend is governance, especially the ways in which public-private cooperation is being redefined in cyberspace.

Any consideration of how, even whether, to improve information sharing must be considered in the light of these trends. Litchman asked his audience to consider the metaphors that have become commonplace in discussions of cyber security. We are warned against a digital Pearl Harbor, told to reconceive cyber security along epidemiological lines, and advised to pay close attention to IT hygiene. Litchman suggested, rather, that the cyber domain is more like an iceberg: most of our knowledge lies beneath the surface.

He closed with some thoughts on the prospects of information sharing. He lamented the lack of information sharing standards, and observed the way legal uncertainty retards their development. He urged governments in particular to recognize the indispensability of building trust, and cautioned that information sharing can't be a cloak for espionage or surveillance.

### Cyber Security in a Borderless World.

Adnan Amjad, Partner, Cyber Threat Risk Management, Deloitte & Touche LLP, sought to define "cyber" in a borderless world. Despite considerable expenditure on cyber, he said, the problem

grows worse. We tend to focus on the adversary. But this is only one side of the coin. Enterprises themselves are doing things that increase cyber risk. "The very things we do to innovate and drive performance are the very things that create cyber risk." By all means you should worry about the adversary, but first get a handle on your own enterprise, your networks, your data, and your intellectual property. Achieving such self-awareness is neither easy nor trivial. Some of the biggest risks today arise from third parties—customers, suppliers, and business partners.

So how can an enterprise you fix this? Amjad argued that any enterprise should seek to become, vigilant, and resilent. The idea of protecting everything is a fallacy. Instead, protect what's vital, and monitor who's accessing that. Intelligence about the threat has a central part to play in achieving those three goals. You need to know the actors, their tools, their techniques, and their processes. This, he stressed, should be intelligence, not unanalyzed information ("atomic data," as he called the latter). You need to know who's coming after you, what they're after, and how they'll do it.

And finally you need resilience. "Most mature organizations now hold regular cyber resilience exercises." Know the challenges peculiar to your sector. Retail, NGOs, food producers, etc. have very different security needs. Your industry knowledge matters, because cyber risks vary considerable (as do regulatory requirements).

In response to a question about how well we're doing at sharing information across borders, Amjad said, "very poorly," althought he singled out the financial sector and the FS-ISAC as being ahead of other areas. As we design information sharing systems, we continue to miss the big picture for the atomic details. And we need to blend intelligence developed from threat feeds with internal information. Basic hygiene, Amjad maintained, is common across sectors. Its tactics, techniques, and procedures are similar, however different the atomic data may be.

In response to a question about obstacles to information sharing, Amjad thought that competitive pressures tend to inhibit informationsharing more than regulatory concerns. It's difficult to achieve the trust necessary to sharing with competitors. Another persistent obstacle that arises when business shares information with law enforcement organization is the set of issues that surround classification and security clearances.

Amjad thought that the most important information to share about a cyber attack are techniques and malware samples. He suggested that the two sectors that had the most work left to do were life sciences—especially big pharma—and energy—including not only power utilities, but also the oil and gas sector.

## Keynote Address: Digital Dignity in an Era of Cyber Insecurity.

Nuala O'Connor (President and CEO, Center for Democracy & Technology recalled the 9/11 attacks, and asked her audience to remember, or imagine, the sense of vulnerability one felt when "someone was out to kill me for nothing I've done, as an individual." She would return to individual dignity and vulnerability throughout her presentation.

She urged that we not forget that information about individuals lies the center of security systems, and that information in the aggregate she called the "digital self." The US Supreme Court is getting this issue right, she thought, in its findings that the boundary between the state and the individual has not changed. Rather than consider data as property, we should recognize that our digital self hasn't fundamentally changed those boundaries. She has found the concept of habeus data (from Europe) useful.

The data surrounding the digital self falls roughly into three categories: data about us, data we create, and data others create about us.

Taking up the first category, O'Connor noted that "Just being able to collect doesn't mean that we ought to collect." We undeniably share our data, but we do so for specific purposes in specific transactions. Legitimate governmental purposes are not indefinitely expansive into secondary and tertiary uses. All enterprises, and governmental ones particularly, should recognize, she argued, that "Not having data is sometimes a great thing. We could do more with less." In hindsight, she believed, Admiral Poindexter was on the right track in his intent to pursue anonymized, de-identified data.

Thus data limitation with respect to personally identifiable information is essential to digital dignity. But we tend to overlook the importance of a second class of data is data we create: content. And our content is under threat. Governments experience a perennial temptation to control or censor thought and speech. This temptation often arises from relatively benign motives—consider present concerns about the real threat extremist content poses. But any such control has a demonstrably chilling effect on free speech.

The third category comprises data others create about you, which O'Connor found "wonderful and terrifying," with the embedded algorithm particularly worrisome. (Her illustrative example concerned the personalized recommendations a customer receives from Amazon.) O'Connor believed that "we'll get this right" through transparency and the ability to appeal providing the necessary sunlight. She regarded stress-testing of algorithms for disparate impact very important.

O'Connor concluded with strong advocacy of freedom of speech, and opposition to any limitations on it. And she stressed that the digital self, in its relationships with friends, family, and associates, however those relationships might be mediated through some third party, has nothing to do with a government's right to any person's data.

## How cybersecurity is a global issue fostering collaboration.

Chaired by World Bank Senior Operations Officer Sandra Sargent, ths panel included Belisario Contreras (Program Manager, Organization of American States), Fernando Nikitin (Principal Auditor, Inter-American Development Bank), Amir Becker (Director of Cyber Cooperation, Embassy of Israel), and Bram Reinders (Alliander).

Contreras opened discussion by identifying a change of culture and development of coordination as the principal challenges we face in the Americas. Because they are enduring issues, cyber challenges require a common approach.

Nikitin thought that uncertainty about the dimensions of the cyber problem is increasing. Process and an integrated approach, he believed, are more important than technology.

Becker asked the conference to remember that with cyber, we're creating something new, something for the future. And Reinders emphasized the importance of a global dialogue about cyber matters.

Inequality persists even as connectivity extends to all corners of the world. Such inequalities can be a generational as they are geographic, Nikitin thought. "We speak of threat we now see, but it's different from the threat that's coming." He was particularly concerned to draw attention to the importance of the deep web, which he say as having both good and malicious uses. The deep web is the locus of a serious generation gap—the ability to navigate it is becoming common among the young.

Becker offered an account of Israeli success at nurturing entrepreneurship in the cyber security sector. There are, he said, about two hundred fifty cyber companies in Israel, some one hundred of which are startups. Israel understands cyber as a national issue. The government took a decision to protect infrastructure, including networks, and then stepped back from

close regulation of the new industry. Strong economic support in a relatively permissive regulatory regime has fostered innovation. The government's decision to devote 8% of IT budgets to cyber has promote security in the private sector without recourse to prescriptive law or regulation.

Reinders, descibing approaches taken in the Netherlands, saw a "moral imperative" to share information. He thought it particularly difficult to share lessons learned, especially insofar as doing so might disclose shortcomings. He strongly emphasized the importance of corporate board understanding of and involvement with information sharing. As an example, he noted the vulnerabilities that have been found in smart meters, and how those vulnerabilities can compromise grids. Yet we've seen people fear bringing this bad news to boards. He urges that cyber not be perceived as a competitive advantage.

In response to questions, Contreras said that cyber is a comprehensive issue, not one confined to IT or telcos. And it needs a budget in development agencies. Nikitin urged that professional organizations not be neglected when we consider marshaling groups for cyber collaboration, and he stressed the importance of UN involvement.

Becker finished with a caution for planners and policy makers. Because cyber is a new domain, it bears little similarity to what we've known from the past. Decision makers' intuitions are a poor guide to this new, artificial domain.

## Building an Information Sharing Environment: Moving Forward Based on What We've Learned.

Kshemendra Paul (Program Manager, the Information Sharing Environment) gave an early, positive, shout-out to the United States Constitution's 10th Amendment (which reserves powers not enumerated to states or people). This distribution of power and authority animates Administration policy with respect to information sharing.

Paul described the various fusion centers, a geographically centered approach to building capacity at the state and local levels. Transparency, participation, and local control are essential aspects of this approach.

The Information Sharing Environment's mission emerged from a post-9/11 effort to improve public safety situational awareness. Such collaboration, Paul noted, requires common operating models. The difficulty of achieving security in a federated enterprise lies always in the implementation, which requires consistent standards. The IT industry plays a foundational role in evolving such standards, and Paul closed by pointing out that if you want general adoption of information sharing frameworks, the onus is on those who develop such standards to adapt them to market imperatives.

## International Cooperation: Opportunities for, and Obstacles to, Sharing Information across Borders.

Facilitated by James Clark (General Counsel, OASIS), this panel included Ken Ducatel (CISO, the European Commission), Ryuichi Hirano (Counsellor, National Center of Incident Readiness and Strategy for Cybersecurity, Government of Japan), and Adam Sedgewick (Senior Information Technology Policy Advisor, US National Institute for Standards and Technology).

The panelists described their organizations' various roles and missions. Describing EU policy, he noted that breach notification was required, but that other information sharing remained voluntary. The EU CERT is central to information sharing. Hirano described the impact of Japan's large pension fund breach on national policy. His government's objective is to advance a free, fair, secure cyber space. Sedgewick, speaking of US policy, described the mix of legislation, executive order, and interagency administrative coordination the Administration uses to advance cyber security goals.

Sedgewick noted two peculiarities—positive ones, in his view—of the US approach. First, US law requires that the US to turn to international standards first when it begins evolving its own. Executive Order 13636 itself emphasized the importance of addressing international standards for the Cyber Security Framework. And he noted the Government's longstanding view that it's better to turn to industry first rather than to simply evolve standards within Government. He described some of NIST's work on privacy engineering (which the Institute sees as a cognate set of problems to those of security).

Hirano described the challenges involved in developing a trained cyber labor force, education for which he believed should begin as early as elementary school. Yet education cannot be confined to students: it's equally important to educate corporate executives so they know how to employ a trained labor force.

Metrics are needed that can enable corporate executives to understand their cyber situation. Yet, Ducatel lamented, executives quickly become inured to the bad news their CISOs (and the media) routinely serve up. Those executives need to ensure that their organizations are configured for resiliency against the unknown unknowns. Sedgewick closed with an overarching observation about cyber security: "Every organization owns its own risk. Technological change affects the kind of people you need to manage it."

## Cyberthreats Spawn a New Era of Public-Private Collaboration

Alexander Howard (Senior Editor, Technology and Society, Huffington Post) chaired the day's final panel, whose members included Marco Obiso (Cybersecurity Coordinator, ITU), Eric Hibbard (CTO Security & Privacy, Hiatchi Data Systems, INCITS, IEEE), and Scott Algeier (Founder, President, and CEO, Conrad Inc., also Executive Director, IT-ISAC).

Obiso cautioned the audience against assuming that information sharing could or should be a one way street. In particular, he advised the developed world to avoid thinking it had nothing to learn from the developing world.

Standards, Hibbard explained, respond to known threats, "So we're always behind the 8-ball." We arrive at standards slowly, through consensus, and their final form is therefore seldom complete. Definitions are crucially important: "If you can't define a technology, you probably can't secure it" (or secure privacy within it). He thought the PCI standards a good example of an excellent rallying point and forcing function for the private sector.

Hibbard also asked about criteria for trust, which he sees (citing the OPM incident as a cautionary tale) as having seriously eroded. He also thought issues of prosecution and liability surrounding information sharing remain to be addressed. "Companies worry about this. Lawyers salivate over it. In the US at least, we have to assume we'll be involved in litigation if we share information."

He added some thoughts on the technical direction information sharing must take. Information must be actionable, and time is of the essence given the speed with which the threat changes. Thus automation is essential to keeping pace with the threat.

In general the security profession is short-staffed, but especially within the Government. This exacerbates, Hibbard thought, the troublesome if inevtiable place cyber occupies as part of the competitive landscape, for both nations and companies.

Algeier, speaking from the perspective of the IT-ISAC, stressed the importance of co-leadership of programs, consensus decision-making, and maintenance of close interest in stakeholder concerns. Proper evolution of best practices is essential: the consequence of not following best practices in public-private partnership is failure.

Questions raised the issue of anonymity in data sharing, which both Obiso and Hibbard agreed limited the utility of any data collected. Algeier thought anonymization posed three challenges: reliability (of the source), deduplication (of incident reports), and exchange of lessons learned. Obiso disagreed: he thought anonymized data were not anonymous data. Objections to anonymization can be overcome, partly through third-party intercession.

## September 16

*The second and final day of Borderless Cyber 2015 continued the discussion of the role standards play in fostering information sharing, and how that sharing can best be conducted internationally*

### Internet-of-Things or Internet-of-Insecurity?

Barbara Grewe, Principal Policy Advisor, the MITRE Corporation, opened the second day with a talk on Internet-of-things (IoT) security. Its security implications, she said, include new threat surfaces, physical consequences, machine autonomy, redefined trust. The Target breach had its roots in the IoT, since those who compromised the retailer's point-of-sale network did so via an HVAC contractor. (She compared this particular attack vector to the wolf's spoofing of the grandmother in Little Red Riding Hood—IoT networks need to be able to recognize wolves.)

The IoT also has significant implications for privacy. Disclosure of private information falls into three "buckets": 1) Intentional, 2) Tacit, 3) Illegal, and 4) Undisclosed. The fourth has swiftly become the smallest. As the IoT transforms almost every device into a sensor, our current concept of privacy is nearing extinction.

Losing control of your data can cause you to lose ownership of your data. There are no obvious remedies for this. Grewe rehearsed various unresolved questions surrounding this issue. Consider the European right-to-be-forgotten. How will this work? Consider how it would work, for example, with social media like Twitter. Do you own your tweets? Do you own retweets of your original material, or do those belong to the parties who retweeted them? And who's responsible for protecting your data? You, or some third party? Who controls the cloud? And which of the many intersecting privacy policies control your data? The strongest? The weakest? All these questions await resolution.

The growing autonomy of devices in the IoT will raise significant issues of liability. It's unclear where legal intent resides in cases of autonomous machines. What are the manufacturers' responsibilities? What are users' duties to respond to notices of vulnerabilities? The Wyndham decision has given us an insight into "the brave new world of liability," as administered by agencies like the Federal Trade Commission. Grewe concluded by advising IoT developers to bake security in from the beginning. Develop and apply better system hygiene. Use data to your advantage. Share information, and develop consistent international standards, "cyber seatbelts."

### A Funny Thing Happened on the Way to OASIS: STIX/TAXII — From "Specifications" to "Standards"

Richard Struse, Chief Advanced Technology Officer, NCCIC, US Department of Homeland Security (and principal architect of STIX/TAXII) delivered the morning's second address, describing the movement from "specifications" to "standards."

The goal of STIX/TAXII is creation of an ecosystem where actionable cyber intelligence is automatically shared in real-time. This doesn't mean, he stressed, turning everything over to the machines, but rather a division of labor in which humans and machines were empowered to do, respectively, what they do best.

The economics of cyber conflict favor the adversary. We need, Struse argued, to change this. We've been chasing their robots; they should instead be chasing ours. "My detection should become your protection. This is the point of information sharing." If we share effectively, and are known to share effectively, the adversaries will know they've burned an attack technique on first use. They will become unable to reuse their tools.

Standards don't usefully evolve out of traditional requirements processes. Agility and iteration are essential. Struse was gratified to see how governance of a central aspect of the Federal government's approach to cyber security, STIX/TAXII, has transitioned to OASIS, an international standards body. STIX/TAXII exemplify a healthy, bottom-up as opposed to top-down, approach to standards development. This approach lets the market vet a standard before it's codified for compliance. "Thus a de facto standard becomes a de jure one, which is the right direction." This process preemptively avoids conflict between a standard and its community of users. Don't assume people will read elaborate specifications. Instead, give the users of standards a good API so they don't have to build to specification, and don't assume that the need for any particular standard will be immediately obvious to everybody.

Struse said that OASIS was picked to administer STIX/TAXII for its track record. Its membership is broad. It provides standards free-of-charge, in perpetuity.

## Borders — Securing Cyberspace, Preserving Openness, Fostering Innovation

Michael Chertoff, Executive Chairman and Co-Founder, The Chertoff Group, and former Secretary of Homeland Security, delivered the morning keynote.

He opened with a discussion of how new technology presents both opportunity and risk. No sector immune to cyber attack. Reviewing the history of Internet, he noted that trust wasn't an issue at the Internet's inception (nor was commerce, for that matter), and thus security wasn't built into it. The Internet's default position is openness.

Threats now operate across full spectrum of connected devices. "Our challenge isn't risk awareness, but risk management. You can't avoid cyber risk. You can, however, manage it. Risk comes down, traditionally, to threat, vulnerability, and consequence. The last is very important: consequence management and self-awareness are key elements of risk management."

Security must be intuitive. It's not achieved through technical means, but through technical means intelligently applied by human users, and in the end it depends upon well-placed trust. Positive security innovations involve encryption, the cloud, mobility, and analytics (and big data). The prospects of big data are especially promising for behavioral analytics.

Warning of the vast attack surface the IoT presents, Chertoff noted that the mere possibility of connection isn't an imperative for connection. He advised mindfulness with respect to connectivity.

Finishing with issues of government access to private data, Chertoff thought there were better ways of accommodating legitimate law enforcement access to data than by weakening encryption. "We ought not to sacrifice security of networks simply to make it easier for authorities to access data." He recommended the Mutual Legal Assistance regime as a way of rationalizing access to data internationally. He thought that the international community needs to deal with issues of exporting rules and regulations (like the right to be forgotten). Some of these rules (like, again, the right to be forgotten) will prove ultimately to be unexportable. He closed with a call for international standards that foster privacy, security, freedom.

## A New Security Dimension: Industry Experience Using Open Standards to Accelerate Threat Response

Dark Reading Editor Tim Wilson chaired a panel on industry's use of open standards to accelerate response to threats. The panelists were Jason Corbin (Vice President, Product Management and Strategy, IBM), Paul Kurtz (CEO, TruSTAR), Ted Julian (Co-Founder and Vice President, Product Management, Resilient Systems).

Kurtz pointed out that market and reputational risk remain principal barriers to information sharing. But the Target and Sony breaches have given industry huge wake-up calls. Corbin perceived significant momentum, however, especially in the financial sector, toward greater information sharing. But even relatively weak sharing is still feared because of the enforcement actions it might attract. (And this is a shame.)

In reponse to a question about the attribution problem, Julian said that attribution is far from companies' minds. Overwhelmed, they want respite from attacks. Kurtz agreed: attribution concerns, he argued, are largely media-driven. Companies want to stop the pain, and, to its credit, the Government (and now OASIS) has boiled STIX/TAXII down to fields that present information companies will find actionable. Wilson noted that, while there points are compelling, disagreement over the value of attribution persists in the security industry.

Kurtz closed with the observation that correlation of data is where you'll find the incentive to share. In response to a question about the business case for information sharing, he noted the relatively low cost of information sharing. "We need to connect the good guys, and this can be done at a nominal cost."

## Preventing and Mitigating Potential Threats at Large-Scale Events: A Look at Past and Future Plans Involving the Olympics and Super Bowl

The first afternoon panel, chaired by Kazuo Noguchi (Senior Manager, Hitachi America) addressed the challenge of cyber threats to large scale events like the Olympics and the Super Bowl. Panelists included Andy Williams (Cyber Envoy, UKTI Defence & Security Organisation), Michael Meglino (of the US Office of the Director of National Intelligence), and Ko Ikai (Counsellor, National Center for Incident Readiness and Strategy for Cybersecurity (NISC), Government of Japan).

Williams described the British experience with security for the 2012 London Olympics, which, thanks to widespread broadband, were called "the first digital games." The fundamental cyber risk was to the reputation of the host country. The cyber threats included the traditional ones: crime, espionage, terrorism, and hacktivism. The lessons learned included the value of collaboration, the importance of commitment to secuity on the part of stakeholders.

Some of the measures taken to secure the Olympics had enduring value for the United Kindgom. They stood up an Olympics CERT at a time when there was as yet no UK CERT, and the UK CERT organized after the games benefited from the Olympic experience.

A second lesson is the importance of preparation: planning and (especially) testing. Two serious national-level cyber incidents occurred in conjunction with the opening ceremony. One of these still cannot be discussed, but the other was an attempted shutdown of electrical power. Preparation enabled the authorities to cope with them.

Another lesson learned was the importance of picking the right technology parrtners (retrofitting is expensive). "If we'd had the means of pushing cyber standards across the supply chain, we would have done so."

After Ikai's discussion of preparations for the 2020 Tokyo games, Meglino described information sharing in both anticipated and unanticipated events. He's found both

interpersonal contacts and technological infrastructure important for information sharing, and he emphasized the importance of resilience. Quoting US NSA Director Rogers, he emphasized that "we have to learn to operate while we're hurt."

## Privacy, Identity, and Information Sharing: Risks and Opportunities

The afternoon's second panel, chaired by Jeremy Grant (Managing Director, the Chertoff Group) took up the risks and opportunities presented by privacy, identity, and information sharing. Panelists included Aquiles Almansi (Lead Financial Sector Specialist, World Bank), Joseph Lorenzo Hall (Chief Technologist, Center for Democracy and Technology), and Peter Alterman (COO, SAFE-BioPharma Association and StC Member, OASIS IDtrust). Grant opened with a review of the benefits and concerns surrounding collaboration for cyber security. The biggest concerns are security, privacy, liability, and information overload.

Almansi described conflicting institutional commitments and offered suggestions about how to deal with them. Evidence from financial sector suggests very uneven information sharing policies (and consequently situational awareness). He presented results of an extensive security self-assessment his organization conducted. The strongest self-assessments came "from things in the care of the IT guys." The weakest "came from stuff in hands of senior managers." And alas, simulation exercise results are fully consistent with those self-assessments. Almansi called for an effort to convince senior leaders ("important people") that cyber security is essentially an institutional problem.

Hall said that information sharing was in unstable equilibrium. He argued that information sharing, if it's to protect rights while enhancing security, should be "carefully calibrated adversarial collaboration." Relationships that are too cosy are also too risky, and both government and the private sector need mechanisms to ensure their relationships don't become too comfortable. "There are good reasons to share, and good reasons to withhold. We should calibrate what we share, and share only information that we need and can practically use." Liability, in this context, has a positive role to play.

Hall also argued that enterprises need actionable data, not masses of raw data (which only the largest enterprises can handle). Take both security and privacy seriously. Don't take security as a given, and above all don't undermine trust.

## Emerging Trends in Critical Infrastructure Protection

Peter Allor (Senior Cyber Security Strategist, IBM) facilitated the afternoon's panel on critical infrastructure protection. Panelists included Denise Anderson (Executive Director, National Health Information Sharing and Analysis Center), Catherine Lotrionte (Director, Institute for Law, Science, and Global Security, Georgetown University), and Parham Eftekhari (Senior Fellow, Institute for Critical Infrastructure (ICIT)).

Lotrionte opened the discusson by providing historical perspective on the evolution of current international norms with respect to cyber conflict. These have generally aimed at preservation of the peace and general accessibility of cyberspace. The international community achieved some early agreement on peacetime norms: no targeting of critical infrastructure, no targeting of cyber first responders, assumption of a responsibility to assist when requested, and no use of proxies to carry out attacks in cyberspace. We've also seen a general recognition of a national right to self defense, and a general commitment to control proliferation of cyber weapons. So we've seen some progress in the development international norms governing cyber conflict, although we remain short of achieving general consensus.

Eftekhari described troubling trends in critical infrastructure security. The attack surface is evolving and expanding, our infrastructure depends upon archaic legacy systems, and we

face dedicated, diversified adversaries. We're seeing wider availability of turnkey exploit kits (available in the deep web), and we suffer from an absence of cybersecurity training. He reviewed attack basics: social engineering, custom exploit kit development, spearphishing, network access, lateral motion, and damage to systems or exfiltration of data. So we need education (not only of workers, but of leaders and legislators), legislation, and technology.

Anderson described how ISACs work and collaborate. They tend to be operational, not policy-focused, and constitute communities of trust with strong reach into their sectors. ISACs are also now global, operating in some 38 countries. She described sharing mechanisms, which range from conference calls to list servers to secure portals. As early adopters of STIX/TAXII, they're also committed to sharing machine-to-machine. Anderson lamented the ways in which policy overlooks operational realities. She noted that many sectors were sharing information before they'd received a mandate to do so, and that the way to foster information sharing is to make it easy.

## Concluding Remarks

The conference wrapped up with a closing summation from the World Bank. The Bank made another call for sharing information with developing world, and asked for help conveying the ethical message that hacking is wrong—a message particularly important for the young in the developing world. Both the World Bank and OASIS thanked the symposiasts, and looked forward to further dialogue.

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 10.22.15