Hearing on “Cyber Threats and Implications for the 21st Century Economy”

Written Testimony of Gregory E. Shannon, Ph.D.

Chief Scientist for the CERT Division

Carnegie Mellon University

Before the Subcommittee on Oversight and Investigations

U.S. House of Representatives Committee on Energy and Commerce

Future Technologies for a Trustworthy and Resilient Cyber Economy

March 3, 2015

Chairman Murphy, Ranking Member DeGette, and members of the subcommittee, thank you for inviting me to testify on cyber threats and implications for the 21st Century.

My name is Greg Shannon, and I am the Chief Scientist for the CERT Division (www.cert.org) at the Carnegie Mellon University Software Engineering Institute where I lead efforts to sustain and broaden CERT’s strategic research, development, and policy initiatives. I also chair the Cybersecurity Initiative for IEEE (www.ieee.org); my goal is to accelerate innovative research, development, and use of efficient cyber security and privacy technologies that protect commerce, innovation, and expression.

On behalf of Carnegie Mellon University and IEEE, I am honored to discuss future technologies for a trustworthy and resilient cyber economy.

Summary of Major Points

To sustain and expand our economy, consumers and businesses need to trust the cyber-infrastructure ecosystems upon which commerce and innovation now depend. Those ecosystems must also thwart capable adversaries who seek to execute economy-disrupting cyber-attacks.

Currently there is no manner in which an entity, public or private, can fully protect itself without simultaneously eroding its value. There are neither existing technologies nor any amount of money that would stop all serious cyber-attacks and allow for the efficient function of electronic commerce. We simply do not yet know how to do both of those together.

In the short term, we need to push for more and better measurement of outcomes. The best-secured organizations continuously monitor how their performance (breaches) correlates with their practices. Without meaningful feedback, organizations (and technologies) cannot improve. Furthermore, if we can determine which data subsets are essential to combating the cyber threat, then less data would need to be shared to productively handle cyber risks.

In the medium term, we need to improve access to data for security and privacy innovation. Science or technology are only as good as the data it is created from, and currently researchers and developers have limited access to data, resulting in sub-par solutions and slower innovation.

In the long-term, we need coordinated national strategies to sustainably build trust and thwart our cyber adversaries. For example, we need to eliminate the possibility that a single weakness can threaten the economy. Considering computational and human energy as a barrier, it's possible to create and operate a strategically-advantaged cyber infrastructure that requires adversaries to expend exceptional energy in order to pose serious cyber-threats to our economy.

Testimony

As we strive to grow our Nation's 21st century economy, we must expand trust of the cyber-infrastructure ecosystems used by both public and private users. Today, national and global commerce depends upon those critical cyber ecosystems, yet a multitude of threats exist across the spectrum from individuals to collective groups that seek to disrupt commerce through cyber-attacks. Maximum global economic advantage will come to those ecosystems that can best thwart increasingly sophisticated adversaries.

Currently there is no manner in which an entity, public or private, can be fully protected without simultaneously destroying its value. Today, there are neither the tools, technology, nor resources, to stop all serious cyber-attacks and allow for efficient function of electronic commerce. We simply do not yet know how to do both of those together, which makes enabling continued technology research and innovation essential.

Innovation

Merriam-Webster defines *innovation* as a new idea, device or method. While people often think of a novel device when they hear the word *innovation*, we must remember that it can also refer to innovative concepts in business models, policy, social interactions, education, etc.

In business, innovation brought the Freemium[1] model, a pricing strategy by which a basic product or service is provided free of charge, while money (premium) is charged for proprietary features. Innovation in social media delivered crowd sourcing and open source solutions. Disruptive policies such as the European Union's (EU) "Right to be Forgotten" have influenced and changed our world. Even the long-standing framework for Internet governance with ICANN

[1] See Anderson's book *Free*, published in 2016.

(Internet Corporation for Assigned Names and Numbers, the private sector, non-profit corporation created in 1998 to assume responsibility for administering IP addresses), IETF (Internet Engineering Task Force) and IAB (Internet Architecture Board) were truly innovative. Similarly, in education, we have distance learning, adaptive learning like CMU's OLI initiative[2], and immersive team virtual learning in CERT's STEPfwd platform.[3]

The bottom line is that when we discuss innovation we do not want to pigeonhole ourselves to only hardware and software. Instead, we need to expand our view to include that which will advance us from the status quo.

Technology Outlook for the Future

When discussing cyber security—past, present or future—it is important to understand the four mainstays of cyber technology and innovation: trust, people, efficiency, and measured outcomes. Innovation and the adoption of new technologies must take into account those four pillars.

The technologies I discuss later broadly facilitate these pillars and provide a sound basis for a trustworthy cyber infrastructure that thwarts successful attacks. First, I want to explore near-term, medium-term, and long-term technology research opportunities.

[2] http://oli.cmu.edu/get-to-know-oli/
[3] https://stepfwd.cert.org/

Near-Term Opportunity

In the current reality, individuals, businesses or national organizations cannot expect to prevent every serious cyber attack. Such entities must be aware, resilient, enabled, and capable to continue operations and meet their missions when disruption occurs. Organizational resiliency requires a structured approach to managing security risks, business continuity, and information technology operations within the context of business objectives. But without proof about which ideas, processes, or devices work, or in other words, return on investment (ROI), adoption rates of such approaches languish. Consequently, in the short term, we need to push for more and better measurement of outcomes to galvanize adoption rates.

It is not news that cyber connects us all: private and government, personal and business, entities and individuals. Collectively we're unlikely to be "undone" by the weakest link, if most everyone practices good cyber hygiene. However, you cannot expect everyone to adopt a new idea without proof of efficacy, especially when implementation rarely comes free. We, as a Research and Development (R&D) community, need to ensure innovation is scientifically and operationally validated and provide compelling return on investment metrics to incentivize adoption.

There are two working approaches we can use to set in motion a protocol of gathering feedback to produce meaningful metrics. The first, and most obvious, is the NIST Cybersecurity Framework (CSF). With incentives and a sound legal framework, organizations could begin to extract data, employ metrics and share those with both their peers and the Federal Government.

The second model is the Department of Energy's (DOE) successfully deployed Cybersecurity Capability Maturity Model (C2M2), which is a public-private partnership effort established as a result of the Administration's efforts to improve the electricity subsector

cybersecurity capabilities. The C2M2, focused on the implementation and management of cybersecurity practices, helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity capabilities.

Moving forward, policymakers have the potential to enable progress in the science of cyber security with explicit guidance that policies, best practices, technologies, standards, products, and large-scale operational plans are scientifically and operationally validated and will produce valid, outcome-based, efficacy measurements. The best-secured organizations continuously monitor how their performance (breaches) correlates with their practices. Without meaningful feedback, organizations (and technologies) cannot improve.[4]

Medium-Term Opportunity

Medium-term goals must include access to data for research and development (R&D). Currently, the R&D community has limited access to data, resulting in sub-par solutions and stunted innovation. Information sharing is often seen as a defensive strategy; however, providing operationally relevant data to researchers and engineers accelerates innovation. I've personally seen such acceleration in sponsored research and the development of commercial technology.

Richer data needs to be shared with the research and development community — meaning not only incident data but also datasets that enable understanding of what "normal" resembles (in terms of network activity, user behavior, etc.). If situational awareness is to develop beyond simple indicators, researchers and developers need access to everyday data so that they can begin to recognize what datasets are important. If the research community were able to successfully

[4] A paper by Ericsson, asserts the need for meaningful feedback in order to become a capable expert. Consistent with current business research, I believe that the same applies to improving an organization's resilience.

determine which features in datasets were essential to combating the cyber threat, then in effect, over time less data would need to be shared to productively handle cyber risks.

It is imperative that policymakers include research in the information-sharing vernacular. To encourage unencumbered information sharing, of course, solid protection procedures need to be in place. This will likely require both legislative updates and policy changes, which must be done with the utmost consideration of privacy and civil liberties.

It is the Federal Government's role to generate situational awareness beyond what any private entity has the incentive to produce. But we must be mindful to not simply generate compliance-driven information while incentivizing minimal disclosure. Building trusted relationships with stakeholders becomes essential to avoiding limited information exchange and is fundamental to a successful response.

I realize additional information sharing tends to exacerbate an already contentious relationship between security and privacy. Security and privacy advocates often are at odds with one another in discussions of how security degrades privacy or privacy degrades security. This is an unhealthy condition, and our adversaries are exploiting it and degrading cyber space for us all. Privacy advocates contend without privacy there is no security. But given our ever more interconnected world, the loss of anonymity is unavoidable, and I believe that without security there is no privacy.

Long-term Opportunity

In the long term, our Nation needs a coordinated and integrated cyber security strategy to build trust between public and private entities and thwart our capable cyber adversaries. Cyber innovation and research need to address the threat in a more holistic manner. Currently, we have tools and solutions to address pieces of the cyber problem. Organizations have to filter hundreds of options to pick the few that fit within their budgets. At the same time, they have to hope that their choices will deflect the majority of attacks. Researchers and policymakers should work towards technologies and innovation that make cyber attacks exceptionally more complicated than exploiting a single weakness.

We all know that there is no silver bullet, but consider if we created a cybersecurity solution that could increase the trustworthiness of cyber infrastructure while simultaneously providing a significant and structured energy-based barrier to cyber attacks. Today, it takes only modest energy (computing and human) to find and execute economy-threatening attacks. This creates an environment that favors the adversary by orders of magnitude. Given the energy we already expend in security defenses (firewalls, anti-virus, intrusion detection systems, etc.) and data analysis of network and host behaviors, we could (1) optimize our (energy) investments to create a most robust defense, (2) utilize recent research and new technologies that make the computational cost of compromise exceptionally high, and (3) we could optimize the energy efficiencies and costs in each technology.

We believe that if we can create and operate a strategically advantaged cyber infrastructure that requires adversaries to expend astronomical amounts of energy to find and execute economy-threatening attacks, then energy becomes the currency in which one traffics to protect or attack commerce around the world. The kilowatt-hour unit of energy is well-defined,

measurable, cannot be counterfeited, and has real value, thus making it an excellent form of symbolic currency—in this case the tender to employ or thwart cyber attacks.

Director of National Intelligence James Clapper told Congress on Feb. 26 that he is most worried about the moderate, iterative and constant barrage of cyber attacks on U.S. infrastructure that will "impose cumulative costs on U.S. economic competitiveness and national security." DNI Clapper's recent testimony on this "insidious trend" supports my belief that energy resourcing will be necessary and required as part of a comprehensive national security strategy to effectively thwart cyber invasions.

Such an energy-based obstruction to cyber threats would require us to first create more energy-efficient technologies to ensure operational cyber security and to establish valid assertions about the amount of energy required by adversaries to compromise the security. Finally, we would have to apply energy to the secure creation, operation and monitoring of cyber operations. With innovation for efficiency and our own national energy resources, only peers with similar resources are even strategically competitive.

This could be a game-changer and would certainly level the playing field. Requiring a greater expenditure of energy currency could also form a barrier to entry for smaller groups and individuals—eliminating foes before they start. Furthermore, embracing the "energy currency" would allow us to standardize and better measure how much we spend, or need to spend, on cyber security as well as force our adversaries, to include nation-states, to prioritize and even reduce the extent of attacks they are able to attempt. Ultimately, access to energy could become a deterrent to economy-threatening cyber attacks.

A DIMACS- and IEEE-sponsored workshop at Carnegie Mellon University in June[5] will explore the theoretical and technical foundations for this strategy.

[5] http://dimacs.rutgers.edu/Workshops/ESCAPE/announcement.html

Technologies to Watch

An excellent resource for understanding future cyber technologies is the IEEE Computer Society 2022 Report,[6] a survey of 23 technologies that could change the world by 2022. Notably, the first technology that this report addresses is security cross-cutting issues, Trust issues (i.e., privacy) are considered throughout the report.

I would like to draw attention to some of the key emerging technologies I believe will enable us to sustain cyber trust and impede cyber adversaries over the short-, medium-, and long-term.

Key Short-Term Technologies

- Risk modeling and management: the only viable strategy for dealing with limited resources, uncertain knowledge, and incomplete solutions
- Two-factor authentication: an effective and scalable technology with many variations
- Cyber intelligence analysis:[7] know and track adversaries on their specific objectives, techniques, and operations

Key Medium-Term Technologies

- Resilient trustworthy ecosystems: "app stores" for mobile phones, secure software updates, enterprise cloud computing services
- Efficient security & privacy architectures, design methods,[8] and development tool chains
- Cyber-relevant theory and models of humans (individuals and communities): Understand how/where the range of human behaviors can enhance/degrade security and privacy.

[6] http://www.computer.org/2022
[7] Information sharing is helpful, but it is not a panacea for the overall cyber threat.
[8] A first step in towards secure designs: Avoiding the Top 10 Software Security Design Flaws, http://cybersecurity.ieee.org/images/files/images/pdf/CybersecurityInitiative-online.pdf.

Key Long-Term Technologies

- Security- and privacy-preserving computing: fully secure encryption, private database queries, verified computation
- Proofs of correctness and searches for counter-examples (e.g., bugs, exploits): already used to verify device drivers and some protocols, and to find exploits in deployed code
- Quantum-secured communication: solves an important but narrow part of the problem: concerns about scalable deployment

Education and workforce development

Both the public and private sectors must have an agile and prepared workforce to deal with the cyber environment and should to be able to train them in a cost effective and scalable manner. Responding to critical cyber events requires technical knowledge and skills, decision-making abilities, and effective coordination—all while moving rapidly.

Institutions like Carnegie Mellon University, with its numerous degrees and professional training programs as well as its technologies rooted in the science of learning like OLI, and the IEEE, with its Cybersecurity Initiative,[9] are well suited to ensure that we have the workforce trained and equipped to handle future cyber threats.

Keeping the workforce up to date is a major challenge given the rapidly changing and dynamic nature of cybersecurity. Curriculum creation needs to be an agile process, with the capability to easily add and modify material. Likewise, education delivery needs to emphasize simulations and scenarios. Currently the most common workforce development training solution is traditional classroom training. While easy to implement, the classroom training solution is not

[9] http://cybersecurity.ieee.org/

adequate for providing effective, large-scale training to a technical workforce. It is also not optimal for training the workforce in a rapidly changing field such as cybersecurity.

The best way to prepare the workforce is to provide practice opportunities under realistic conditions using interactive simulations. Participants across multiple locations are working together in these simulations, to analyze and respond to threats and attacks. This training needs to be delivered on a platform that safely mimics how the internet would respond to stress and exposes participants to real-world, job-relevant scenarios, events, and activities.

CERT's workforce development research focuses on the problems of time, efficiency, scale, and cost. Our researchers, engineers, and subject matter experts search for innovative ways to compress the time it takes to build cyber expertise and to amplify that expertise across a globally distributed workforce. We perform this important research and development to determine how expert content and custom delivery platforms can be used to facilitate efficient transference of knowledge and skills to the cyber workforce.

We have developed custom training platforms that support a range of learning methodologies from traditional, static learning content all the way to interactive, hands-on cybersecurity training scenarios. We provide two comprehensive solutions, STEPfwd[10] and FedVTE, which provide cybersecurity professionals a rich resource of training and skill development important to their work. We facilitate cyber training exercises to apply skills in environments that simulate real-world infrastructures and attacks. Multiple installations of the same exercise can be deployed simultaneously to accommodate a large number of participants.

[10] https://stepfwd.cert.org/

Conclusion

Over the last 45 years we've created the Internet and a modern, evolving 21st century economy. The trust and resiliency challenges have been created by our collective innovation and success. Over the next 45 years, I believe that we can sustain this new economy by making it fully trustworthy and resilient.

Institution Backgrounds

Founded in 1900 and located in Pittsburgh, Pennsylvania, Carnegie Mellon University is the youngest of the top 25 universities in the United States and consistently ranks among the top U.S. universities in computer engineering, computer science, the arts, and public policy for information technology. A global institution with campuses in Silicon Valley, Qatar, Portugal, Australia, Rwanda, and China, Carnegie Mellon is the birthplace of research on artificial intelligence, home to the first university robotics institute, and the first graduate program in entertainment technology. It is among the top U.S. academic institutions in spinning out companies, launching over 75 companies in just the past two years. By any metric, CMU spins out more companies per dollar of federal research funding spent. Recognized as a leading force in the transformation of the Pittsburgh economy, it is credited with helping to attract Google, IBM, Apple, General Dynamics, Network Appliances, Disney Research, Caterpillar and Uber to southwestern Pennsylvania. Over 80 faculty are engaged in life sciences related work that ranges from the development of assistive heart devices to cognitive neuropsychology.

The CERT Division is part of the Carnegie Mellon University Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) sponsored by the Department of Defense. The SEI is headquartered in Pittsburgh, Pennsylvania, with facilities in

Arlington, Virginia (www.sei.cmu.edu). As the birthplace of modern cyber emergency response capabilities in 1988, the CERT Division (www.cert.org) researches, develops, promotes, and operates technology and systems management practices to resist attacks on networked systems, limit damage, restore continuity of critical systems services, and investigate methods and root causes. CERT works both to mitigate cyber risks and to facilitate local, national, and international cyber incident responses. Over the past 26 years, CERT has led efforts to establish more than 110 computer security incident response teams (CSIRTs) around the world, including the Department of Homeland Security (DHS) US-CERT.

With more than 400,000 members in over 160 countries, IEEE— founded as the Institute of Electrical and Electronics Engineers, Inc.—is the world's largest organization for technical professionals, and a leading educational and scientific association for the advancement of technology. The IEEE Computer Society is the trusted information, networking, and career-development source for a global community of technology leaders that includes researchers, educators, software engineers, IT professionals, employers, and students.