TRENDS IN TECHNOLOGY AND DIGITAL SECURITY

DIGITAL THREATS SYMPOSIUM – FALL 2017 – COMPENDIUM OF PROCEEDINGS

Center for Cyber & Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

Raytheon

THIS PUBLICATION IS THE EXCLUSIVE WORK PRODUCT OF THE CENTER FOR CYBER & HOMELAND SECURITY.
IT WAS MADE POSSIBLE THANKS TO THE FINANCIAL SUPPORT OF RAZOR'S EDGE VENTURES AND RATHEON COMPANY.

RAZOR'S EDGE

Foreword

On September 14, 2017, the George Washington University Center for Cyber & Homeland Security (CCHS) convened a Symposium on Trends in Technology and Digital Security. Four panels addressed emerging threats and their implications for security policy, with a focus on digital infrastructure protection and anticipatory analysis. In addition, a featured speaker from abroad presented a country-specific case study.

In a series of Issue Briefs, compiled herein, CCHS shares the findings and recommendations that emerged from the Symposium, primarily on a not-for-attribution basis. The subject and title of each Brief is as follows:

- Methods of Analysis and the Utility of New Tools for Threat Forecasting
- Artificial Intelligence for Cybersecurity: Technological and Ethical Implications
- Space, Satellites, and Critical Infrastructure
- Cybersecurity in the Financial Services Sector
- Israel: The Making of a Cyber Power (Case Study)

This volume is produced in and reflective of the spirit of CCHS's work, which is to address advanced technologies and emerging ("next generation") cyber threats, from the standpoint of U.S. policy. CCHS functions as a network of networks, acting as a hub for upcoming companies, emerging technologists, and cutting-edge public policy.

Steve Pann
Chairman, Board of Directors
GWU Center for Cyber & Homeland Security

About Us

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

Website http://cchs.gwu.edu **Email** cchs@email.gwu.edu **Twitter** @gwcchs

Contents

Methods of Analysis and the Utility of New Tools for Threat Forecasting

Issue Brief Series on Trends in Technology and Digital Security

Speakers/Panelists
Charlie Allen - The Chertoff Group
Mike Davis - CounterTack
Sean Kanuck - International Institute for Strategic Studies
Jason Matheny - Intelligence Advanced Research Projects Agency
Teresa Shea - In-Q-Tel

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

The Threat Climate: National Security at a Time of Rapid Technological Change

The current pace of technological change is striking. The world has more engineers than ever before and there are institutional mechanisms such as peer review that allow individual discoveries to be incorporated into technology much faster than ever before. The dark side to this is that there are more technologies to worry about now than ever before. Think advanced cyber weapons, drone swarms, and synthetic viruses—none of which could be anticipated 70 years ago. This accumulation of risk includes offensive asymmetric opportunities that render defensive systems disproportionately costly, disproportionately effective, or only temporary in their effectiveness.

Perhaps most significant as a driver of these trends is the share of commercial innovation relative to that of government, which means that the most disruptive technologies are now often publicly available in a way that was not true before the 1960s. In addition, the period of superiority for the U.S. government's defense science and technological innovation is shrinking over time. What used to be a period of 5 to 10 years of superiority or dominance in areas of technology in which the government invested is now 6 months to 1 year, if that—and there are even some areas where the government may lag behind industry (at least its median level).

This shift to a world in which most technology is publicly available and commercially funded makes for a technological environment that is increasingly more complicated and consequential. From a U.S. government standpoint, in general, the focus ought to be on the threats that pose existential risks to the country—such as nuclear war, electromagnetic pulse (EMP), cyberattacks that permanently cripple infrastructure, a large-scale pandemic, and certain emerging threats posed by biology.

Consider the especially worrisome aspects of biology. The difficulty of controlling even naturally occurring diseases like malaria or tuberculosis—even when massive resources are applied—is sobering. What if intelligent adversaries were applying some ingenuity to creating diseases? Those organisms can be weaponized effectively to spread efficiently throughout populations—evolving not by random mutations, but by engineering principles. While most of this type of knowledge used to

be locked up in large-scale national programs; that changed in 2003, when the first virus was synthesized from scratch. No longer did you need a sample of the organism; instead all you needed was the sequence of DNA or RNA that would encode the virus, and the raw chemicals to turn that code into biology. Biology was thus transformed into computer science or an engineering discipline.

In fact just last month, a Canadian scientist using commercially available equipment and chemicals, synthesized from scratch at a cost of $100,000 the first pox virus. This kind of technology is getting cheaper at double the rate of Moore's law, and it will get more sophisticated with the introduction of tools like CRISPR (which is used for gene editing) or with the development of things like gene drives which allow particular genes to become prevalent in a population very quickly. The upshot is that a misanthrope with biology training could, for example, re-create smallpox in his or her basement. Another potent illustration: the blueprint for the influenza virus is publicly posted on an NIH website and could now be re-created for $1,000,000. That virus is more effective than a hydrogen bomb in terms of mortality. (A naturally occurring influenza outbreak killed 100 million people worldwide in 12 months, about a century ago; it was the most statistically significant mortality event in human history).

As the requisite skills and budgets continue to shrink in accessibility, biological threats present a particularly challenging national intelligence problem. It is harder to detect distinct signatures of a biological weapons effort, and the set of actors that we have to worry about is large. Individuals are especially challenging as they leave a smaller digital footprint (than nation-states or groups) and have a broader set of motivations—including motivations are not subject to deterrence. Apart from the malicious actor, with powerful technologies, accidents can become especially catastrophic and kill tens of millions of people, even if they are infrequent.

Against this background, we need to think about new phenomenology that can help to reveal low-signature, dual use activities. We need improved measurement and signature intelligence (MASINT) for being able to assess chemical, biological, radiological, and nuclear (CBRN) activities from standoff distances. We need to broadly strengthen U.S. capabilities for scientific and technical intelligence. This list is merely illustrative and not comprehensive. Many of the tools that we have focus on looking at publications or patent trends, but we also need tools that look at what is increasingly becoming the playing field for emerging science which is conferences or social media. We also need to find new tools that are able to bring down the analytic burden for our relatively small number of S&T analysts.

The initiative will always remain with the attacker, but we should prepare for surprises even if cannot prevent them all.

Forecasting Threat: Methods and Tools

The mission of the intelligence community (IC) is to avoid surprise—to understand threats, see them early, and take action. Yet the historical record is checkered. The Arab Spring, the so-called caliphate declared by the Islamic State, and Russia's move into the Crimea all came as a surprise to, rather than a warning from, the IC. Looking ahead however, there is a transformation occurring in the form of digital information and big data analytics that we can bring to bear in the field of anticipatory intelligence. We now have great opportunity to gather, store, and analyze more information than ever before. In terms of tools and equipment, consider the Oak Ridge supercomputer that will be up and fully running in less than five years; it will be the most powerful in the world, second to none.

The National Intelligence Strategy put out in 2014 under then-Director of National Intelligence Clapper discussed anticipatory intelligence and the need for having a cross-cutting mission to make sure that we get "left of boom"/left of surprise. As one panelist stated, "My view is that we're a long way from that." While the country trains people in such a way that when we go to war we do it better than anyone in the world, there is no analogue for anticipatory analysis or warning—it is not taught at the CIA's Kent School, nor is it taught in requisite detail at the National Intelligence University.

One area that we have clearly not done well at is threat forecasting in cybersecurity. In this context, you can think about threat forecasting in an architectural framework that is composed of three pieces: digital intelligence (collection and analysis); trusted infrastructure (countermeasures and the analysis you apply); and an underpinning by analytic workflow and the ability to do agile operations. Technologies will drive threat intelligence and threat forecasting. Machine learning, a subset of artificial intelligence, is being applied today in: behavioral analytics, especially the insider threat; situational awareness of your networks, to identify things that are happening on your networks in real-time, thereby giving you things to take action against; and threat intelligence, automating rote tasks that the IC's analytical staff spend a lot of time on.

Threat intelligence has to be both actionable and timely. There is a difference between threat data and information, and threat intelligence. Analysts are overwhelmed with the amount of data and information that they are getting. They are consumed by trying to correlate these disparate pieces of information to provide context around threats. A lot of this work can be done today with machine learning which results in threat intelligence. However this intelligence has to be tailored to your particular environment and this is where we fall down.

Consider threat forecasting in the cyber context. Tailoring the intelligence to that environment means that you have to be able to answer the questions: What are my digital assets? And which ones are most important? We tend to treat all the data the same, but not all the data is the same. Really knowing what are those priority assets (or priority information or priority intellectual property) that we actually want to protect, allows us to prioritize vulnerabilities and have cybersecurity analysts focus on those top-tier threats against your highest risks. In turn, that enables faster action against threats, faster decision-making on what is being seen, and discovery of new threats you might not have known were out there.

It is important to think through the goal of the action you want to take, based on threat intelligence. There are at least three levels at play here. The first is strategic. In this instance, you care about attribution, e.g., is this an advanced persistent threat (APT)? If so, they will not give up and have lots of resources. Think about what you will do with that information. Second is the operational level. This is where tactics, techniques, and procedures (TTPs) are coming at you. These must be understood in order to address your vulnerabilities—not just in the network and in the equipment—but also those individuals susceptible to clicking on emails, files, or phishing schemes (that keep getting better and better); people are always the greatest weakness factor. Third is the tactical level. Here the relevant questions are: Do I really have all my vulnerabilities patched? What are those vulnerabilities? And where do I apply my precious cyber resources?

As one panelist put it, "You don't have a needle in a haystack problem. You have a needle in a needle-stack problem. There are all kinds of threats (biological, nanotechnology, etc.); so it's the analysis problem that's really plaguing us right now." And that problem, in turn, breaks into two parts. First, we do have a lot of data, yet analysts are still not able to get the information they actually need to make a decision in a timely manner, especially from a cyber perspective. Second, the analysts themselves are not even looking in the right spots: for many years we have been

ignoring the workstation, laptops, and servers in our environment, while almost all of our effort has been on the network. This is the equivalent of going to a crime scene investigation for a murder in a home and not being able to leave the street. It is only in the past two years that we have been looking at the endpoint—the actual systems we use, that connect to the assets that are actually critical.

There is also a cross-domain issue with cybersecurity. What happens if we have a Stuxnet from the biological perspective, meaning that somebody thinks they are making a legitimate virus that could actually help us, and unknowingly the software is actually creating a bad virus underneath them? When you blend these two domains (biology and information security) together you start getting a situation for which analysts are not ready. And when it comes to training at information security in cyberspace, we are good at training in one domain (such as network, or threat intelligence); but we are not good at bridging domains, or looking at information from each of several domains and then applying it.

With threat forecasting and threat analysis, there are certainly some great opportunities around machine learning and big data; but these opportunities are double-edged: already attackers are using machine learning to improve their phishing campaigns. The same things that work to better target advertising are being used to better target phishing. The adversary is getting just as smart in terms of the cost and speed of their innovation; and this far outpaces our defenses because we just do not have the right type of training or technology in place to look at the right type of data.

What is the best use of the assets in the intelligence community? Bear in mind, for instance, that some of our private sector companies are now able to do forensic attribution of cyber incidents as well or better than IC assets (except where they have very particular secret accesses). The template of knowns and unknowns is useful to invoke here in answer to the question. First consider the known unknowns. These are the frameable questions such as who will win the next election in Country X? Humans are not gifted at probability analysis or at predicting these things, yet we are finding increasingly that the technology we are creating is much better at that. Consider big data analysis of sentiments on social media, or meme propagation where you want to infect or influence behavioral patterns. Therefore this may not be the best place for our human analysts, since we are automating it better and better.

Second, consider the unknown knowns. This is where you are looking for specific indicators such as which would-be terrorists are talking about a bomb event. This is where you know what you are looking for, but you have just inordinately large data sets that you need to find the datum in. That data culling again needs to be automated, and that is where we are progressing towards. To put this in a cyber context, this is what red teams and hunt teams need to be doing. The red teams are looking for vulnerabilities, and the hunt teams are looking for indirect evidence of a previous compromise. Again, this needs to get increasingly automated.

Third, consider the unknown unknowns. Here the question is what do I need to be worried about? More specifically, what is happening anomalously in the contextual environment I am in, for which I am unprepared? This is the domain of genuinely anticipatory intelligence. And it is complicated by the fact that in previous decades and centuries, we were dealing with disruptive applications of known technology such as radar; whereas today it is the technologies themselves that are disruptive. This is a huge difference, brought on by the time horizon cycle of technological innovation. For example, if you were supposed to be doing strategic forecasting on the Arab Spring five years out, you would not even know the term "social media" let alone be in a position to assess the impact of social media on it—because Facebook had just left Harvard's campus a year earlier, and Twitter wouldn't be invented until 2006.

Where does this leave us when trying to consider existential risks in strategic forecasting? You have to turn the lens, instead of on the threat actors, you need to turn it introspectively—look at your society, your assets, and what are your critical digital assets that need protecting. Think about the Saudi Aramco cyber event a few years back. It devastated their corporate networks, but it did not get to and harm their production and transmission networks, the core assets of the enterprise. One could debate whether that was luck or design or prevention; but the important point is that Saudi Aramco suffered a huge price-tag but it was one they could weather and survive.

Coming back to biology, the most critical database that we need to be worried about is the human genome, and external efforts to undermine the integrity of that database. And it is not just information security coupled with biology; you also have to add in nanotechnology, because just as we are becoming increasingly able to undermine the integrity of organic platforms through molecular-level production and material science, you can also undermine the integrity of (or introduce unwanted additional features into) inorganic materials and platforms on which we rely in our daily life. Returning to the question of where do we need to spend those very limited critical human assets in the intelligence community, on things we cannot yet automate; that is the strategic forecasting question—and to get the most bang for your buck, you need to look introspectively at your society and your crown jewel assets that are based in carbon, because that is ultimately where your risks lie.

Specially-engineered crops that cannot be digested; or person-specific pathogens designed to go after particular races, or political leaders. This is no longer the stuff of fiction or wild imagination. It is in our best interests to seek to shape the future. There is plenty of scientific and technological talent worldwide, not all of it in friendly settings. For instance, how many nuclear scientists and cryptologists from the Former Soviet Union ended up in

North Korea and Iran? Meeting the national security challenges of the day requires better training and more exquisite tradecraft than we have today within the intelligence community. And until information sharing is at a higher quality, it will be hard to get better decisions. But the lessons of the past are clear: we have to be able to share information and break down bureaucratic silos—because historically, when this has not happened, we have been surprised.

Although our thinking tends to concentrate upon adversaries and malicious actors, the technologies that exist today and that continue to develop rapidly are extraordinarily powerful, and the possibility for technological accidents that are catastrophic is vast—so much so that one participant estimated that humanity has only a 70% probability of making it through the next century.

Artificial Intelligence for Cybersecurity: Technological and Ethical Implications

Issue Brief Series on Trends in Technology and Digital Security

Panelists
Michael Brett - QxBranch
George Duchak - Department of Defense
Anup Ghosh - Sophos
Kristin Sharp - New America Foundation

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

Emerging Technologies: Workforce Impact

The impact of emerging technologies on the workforce—including automation and artificial intelligence (AI)—has been explored using the technique of scenario-planning. A 120-participant study brought together technologists, traditional industry leaders, policymakers, and cultural exemplars to think through what they are seeing in AI, its impacts on the way these participants and their companies/organizations are functioning, and to explore a variety of potential futures. In total, the Commission considered 43 different future scenarios sited ten to twenty years in the future, and these boiled down to four categories:

The first is a future of less work, done in a non-traditional form, where we farm out "scut work" to machines, and humans focus on care and craft work. In this scenario, people are using their expertise to train, coach, and educate others. In the care industry, they are working specifically to develop products that are human-based only, and that are appealing to people based on their tactile nature. The second future is a world in which fewer people have jobs, so they are more competitive. Here, corporations would take a larger role in helping the displaced in their communities, and would be an overarching force in the types of jobs that people could have. The third future is a world, called "the contingent world," in which most jobs would be project-based, and most people would have a variety of income sources, a sort of "souped-up" and extended version of the on-demand economy that we see today. And fourth is a potential world in which almost everyone is augmented in some way by technologies, and every action, surface, and technology is interconnected.

Three insights were common across all of these worlds. First, the "one-and-done" model of education that we see and use today—where a student focuses on one thing in high school or college and expects to use that knowledge for the whole rest of his/her career—is done. People will need to constantly retrain and acquire new skills and new information, and use them in different ways throughout their careers. Second, most emerging opportunities will be self-motivated and individually-driven, so people will have to take much more responsibility in finding, creating, and training for the kinds of work they want to do. Third, with respect to this self-driven and self-led feature, the nature of jobs in our economy is such that probably 20-30% of new jobs are contingent

in some way. Yet most people when surveyed or polled in discussions say that their highest priority in a job is some sense of stability and predictability; they are looking for an ability to forward plan their income, to have a sense of benefits, to know that they will be able to have a job going forward. That is not something that employers are providing as much as they used to, so we will have to explore new systems for creating the kind of stability that lets workers be successful.

Cybersecurity is a particularly interesting example field because there are hundreds of thousands of open jobs now that go unfilled. Estimates for the undersupply of talent are anywhere from 30,000 in Virginia, to 300,000 nationally. With the cybersecurity industry as a job category expanding dramatically, and expected to expand dramatically over the course of the next ten or twenty years, we need to think through ways that we can identify, train, and get new types of people into the pipeline—meaning non-traditional students, and those with non-traditional backgrounds, either academic or demographic.

A counter-argument is that since demand far outpaces the supply of qualified professionals with cybersecurity jobs, it is likely that AI software will replace these jobs out of necessity. For example, traditional security operations centers (SOC) are mostly staffed with tier one analysts staring at screens, looking for unusual events or detections of malicious activity. This activity is similar to physical security personnel monitoring video cameras for intruders. It is tedious for humans, but it is a problem really well-suited to machine learning. So, when we talk about unfulfilled demand for people in cybersecurity, you will see that software will begin to replace conventional and mundane cybersecurity jobs with techniques like machine learning for pattern recognition.

Deep-Learning Neural Networks: Battling Malware

Our cybersecurity defenses as a nation are ill-equipped to deal with the nation-state-level threats that we are being attacked by. Historically, the U.S. Government and defense sector classified nation-state attacks and other breaches on its networks, which meant the commercial sector was largely unaware of the critical details of these attacks and could not develop technology to protect against them. Accordingly, a goal of one Symposium participant—Anup Ghosh, Founder and CEO of Invincea, a Sophos company— was to develop defenses that did not need signatures of threats in order to defend against them. Ultimately that led Dr. Ghosh down the path of machine learning. Part of his company was a group that did Defense Advanced Research Projects Agency (DARPA) R&D, and participated in a program where the basic idea was to look at the whole corpora of malware and identify the core attributes of malware that you can learn. If you create a model, you can then detect variants of this. Note that a super-majority of malware is variations of previously released malware.

The company developed these techniques using deep-learning neural networks and it worked remarkably well—so well, that a larger commercial anti-virus firm bought the company because they understood that innovation in machine learning is critical to combating current and future threats. The acquisition will result in machine learning technology reaching a very broad market through its products. The target market of the acquired company is small- to mid-sized business, which is a market segment that is largely ignored by just about every startup and next-generation security company—yet 99% of all businesses are small- to mid-size. This is the soft underbelly of American companies that gets attacked, and has no protection. Now, this underserved segment will get state-of-the-art machine learning technology to defeat threats not previously known.

Quantum Computing: Applications and Implications

Another Symposium participant, Michael Brett, Chief Executive Officer of Q^{x}Branch, explained the work that his company does applying predictive analytic technologies to a range of commercial outcomes. Working with the financial, insurance, and technology sectors, the firm conducts pricing and risk analysis, and seeks better understanding of customer behavior, using a range of probabilistic and predictive analytics techniques.

Quantum computing is an emerging technology that the company considers to be a strategic long-term enabler of advanced predictive analytics. Quantum computing has attracted significant investment over the past five years and is rapidly gaining attention from enterprises with high computational analytics needs. Q^{x}Branch has been involved in the field for about four years, with access to early stage hardware; and is working with partners in the commercial sector to explore and validate applications and the potential impact of the technology.

Some of the organizations that this company is working with to help understand the impact of quantum computing are banks, pharmaceutical groups, and oil & gas companies—to look at the kind of problems that quantum computing can assist with solving. These are all data analytics problems that, within those industries, are very computationally intensive—or practically unsolvable using classical techniques. Quantum computers will allow us to efficiently solve quantum math; and that could help to unlock some new breakthrough applications.

Quantum computing is at a really interesting stage of its technology development, where the focus is transitioning from research labs and universities, into corporate R&D. We have recently seen major investments from Google, Microsoft, and IBM; they are investing significant R&D resources into their own capabilities plus a startup ecosystem. There are also significant efforts led by the U.S. government including the programs run by the Intelligence Advanced Research Projects Activity, the National Research Foundation, and NIST. Globally we are observing a major push forward in the maturity and the availability of prototype quantum computing hardware that companies are getting access to; and this enables us to start to explore and validate the applications relevant to both industrial and national security issues.

Placing Artificial Intelligence in Context

Artificial intelligence has been around for over sixty years. A lot of the algorithms that you are seeing now are not new, but are things that we can do now because of the confluence of different technologies—including the GPU, big data analytics, and the massive connectivity of the cloud, where you can actually take data, exploit it, and use it at scale. About ten years ago, Ray Kurzweil was quoted as saying that all companies are essentially information companies—largely because information and the automated handling of it, is foundational to a firm's operations. Ten years from now, one participant suggested, I think we will say that all companies will be AI companies—largely because now that you have the information, you have to do something with it: exploit it, try to extract value from it. And the way that we are doing that now is this intersection of big data analytics, improved hardware, and AI.

On September 13, 2017, the Deputy Secretary of Defense, Mr. Shanahan, signed off on a memo saying that the Department of Defense is going to accelerate its movement to the cloud. That was largely motivated for purposes of exploiting data, using and applying AI to a lot of our problems in defense. Data, specifically training data, is the feedstock of AI. General training data, available to everyone, is often used to train AI algorithms. Democratized training data gives no one a competitive advantage. Algorithms are rarely a discriminator, but the training stock, data, often is. In the Department of Defense (DoD), probably 99%-plus of the data that it collects is dark, that is, never exploited. It just sits someplace, waiting for daylight. The movement to cloud is to try to get

this data to be exploited. Our competitive advantage in DoD is the data we collect, with national technical means or otherwise. This is data that is not in the public domain—which gives us a competitive advantage in whatever AI algorithms that we have developed. The very premise of AI is the ability to learn from the data that is continuously collected.

As we discuss AI for cybersecurity, we should also talk about the cybersecurity of AI. We need to protect our models and data from manipulation. A canonical example of an image classifier, panda in this case, will result in the panda being classified as a gibbon with the introduction of a small perturbation in the training data. These "adversarial" examples show us that even simple modern algorithms, for both supervised and reinforcement learning, can act in surprising and unintended ways.

From a commercial standpoint, companies are the most competitive where they are able to bring a unique data set to that opportunity. The world is pretty flat when it comes to algorithms and machine learning techniques; but the world is not flat when it comes to access to unique and well-curated data. One of the competitive advantages that a company has is curating datasets that it owns (that are proprietary to it), that match somehow its industry partners' internal dataset. For example, a bank that has lots of transaction data; a company being able to match that with some other commercially available data that creates a force multiplier effect, is where a company is able to compete and obtain a win over others.

Is data a strategic advantage? Yes, in the Department of Defense; but less so in the commercial sector. You need really good data scientists, but besides your training data, it depends on your ability to execute that as a product. The industry group, Cyber Threat Alliance, believes that threat intelligence should be a public good; and that companies should feed on the ability to execute. On the other hand, one of the challenges with a common dataset is that you do develop blind spots to emerging threats. Machine learning is fallible to training on homogeneous data, so, to develop a really robust model you need a very diverse training set as well. Moreover, on the question of whether datasets are a strategic advantage that may shift, as we see improvements in unsupervised learning. In the future you might gain advantages from simulations or from simulated environments, more than you would/will from datasets.

Will AI benefit the attacker or the defender more? AI offers both promise and peril. It will be used for both offense and defense. It is too early to say for certain which side will have the advantage. Cybersecurity firms are using AI and machine learning to prevent attacks, and attackers are using AI to craft and respond to these defenses. At this stage, the technology is democratized—both parties have access to AI technology, and either side can use it. The discriminator, however, will be in the AI system that can learn and adapt the fastest. For example, we can use machine learning to write tweets that people will click on, for phishing. Or, we can use machine learning to write vulnerabilities in software that vendors can use to patch, and that adversaries can use to exploit. It is not a question of if or when; it is already happening. So, it is another continual evolution of technology for the good and the bad, at once.

Similarly, quantum computing has many great, beneficial applications; and then it also has some applications that are going to be very complicated for the United States and for the world. Consider breaking public key encryption: whether we would want to accelerate or decelerate the breaking of RSA encryption is really complicated, and there does not appear to be agreement about that, even within government. The encryption-breaking aspect of quantum computing, solving Shor's algorithm, is what seems to get all the press. Another use, in the era of big data, is using quantum computing for database search employing Grover's algorithm. Grover's algorithm searches for an entry in an unordered database with a polynomial speed advantage over the best classical

algorithms. In the Department of Defense, this speed advantage can be a competitive advantage when optimizing command and control systems across air, land, sea, space, and cyber domains, for an optimized course of action.

Space, Satellites, and Critical Infrastructure

Issue Brief Series on Trends in Technology and Digital Security

Panelists
Chris DeMay - HawkEye 360
Caitlin Durkovich - Toffler Associates
Nick Eftimiades - Penn State University
Shang Hsiung - Raytheon

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

Old Space, New Space, and the New Space Economy

In the words of the Department of Defense, space today is congested, competitive, and contested. The last 30 to 35 years have witnessed remarkable change: at the outset of that interval, we did not have the Global Positioning Systems (GPS)[1]; or at least it was not publicly used at that point. There were no smartphones. The World Wide Web was just coming on. There were no laptops, digital cameras, DVDs, hybrid cars, or 3D printing. Artificial Intelligence was in a very nascent form. There was no commercial remote sensing. All of this happened in the space of just one career, as one Symposium participant noted. During that period, the ground itself shifted—relative to society—and that really impacted our understanding of space, how we are able to use it, and how it affects us.

Now, space is a $340-billion industry, every year—and that does not include all the secondary and tertiary uses of space that occur every day (for example, how much FedEx saves when it is using GPS, just-in-time delivery programs, and things of that sort). Seventy nations have assets, significant interests, in space today. Yet, 40 years ago, there were just two: the United States and Russia. Space has become essential, not only to the government and to our ability to project power; but to the American way of life. It is a necessity for disaster mitigation, diplomacy, intelligence, and the economy—it is becoming increasingly commercial.

This is what we are faced with; but we must also add into that mix the changing dynamic of how space is used and how much of a role it plays in society, as well as a threat ramp that is escalating very, very, quickly. It has been for the last 10 years, but the technology is advancing dramatically—the miniaturization technology, our ability to put up small satellites, nanosatellites and such, is advancing tremendously. More and more, space is becoming a commercial endeavor; and then you start adding in the nation-state roles (China and Russia)—and then you have an environment in which we are not really used to dealing.

[1] GPS is a satellite-based system that provides three essential services: position, navigation, and timing. That third piece, timing, is particularly important and enables much of the operational efficiency of our infrastructure and the systems as a whole. It is critical to how we operate as a society and as a people—global commerce, the Internet, mobile technology, and essential services (such as transportation, electricity, banking, and food and agriculture).

When you think about the military's applications in space in particular, it is amazing: in World War II, in order to hit a target that was 60-foot by 100-foot, we averaged 1,500 B-17 sorties dropping nine thousand 250-pound bombs. Fast-forward to current, and we have got one B-2 with sixteen 2,000-pound bombs, able to engage 16 targets. Due to our space communications backbone, we also have automated air re-tasking as well as all-weather flight capabilities. That is an extraordinary change; and that is just in the past decade or two that we have really advanced that type of precision use of space services: blue-force tracking, air/shipping navigation, command and control, drone use—all using space, as the backbone.

In fact, many military simulations, if you start taking out the space-related services of remote sensing and GPS, the casualty rates go up significantly—dramatically so—for U.S. forces. Of course, the Armed Forces exercise these scenarios and try to develop mitigation measures; and change tactics accordingly, as you would hope the military does. But the threat to U.S. forces is still there. We have this issue to contend with in the military; and we have it in civil applications and commercial applications, from weather and urban planning, all the way through to automated autonomous cars and precision agriculture.

All countries in the world that have any interest in space are banking on this new space economy and moving aggressively in that direction. In Tokyo, for instance, the new space economy is much discussed, and the government there is making concerted efforts to move industry into that economy.

So, this is where we live at this point. Is the United States prepared for the future on this, as an issue of policy, and security? One participant, Nicholas Eftimiades of Penn State University, thought not, observing that we still have STRATCOM, which plays the major role in protecting space. Professor Eftimiades questioned whether that is an appropriate paradigm for the future, noting further that the old law of the sea doctrine is a common analogy for space protection. The reality, however, is that this paradigm might not be appropriate for the future. Space is a critical part of this nation's future—it is critical infrastructure—far more critical than a power plant in a given U.S. state. Where are we in dealing with that, in terms of: our policies, our governance of it internationally, and how we are going to identify all the red lines that policy needs to do, to be able to ensure safety and security in space? We are nowhere near the refined level of process and policy that is required.

Satellites, Large and Small: Security Implications

Turning specifically to satellites, one participant in the Symposium, HawkEye 360 co-founder and Chief Operating Officer Chris DeMay, detailed his professional background in government, where he learned much about what it means for large and small spacecraft to be designed with security in mind. After transitioning to the corporate setting, he began learning quite a lot about state of the art in small-satellite technology. Security was not an afterthought in the corporate setting, but certainly the entrepreneurial startup mentality is heavily focused on product development and value delivery.

HawkEye 360 is an analytics company that is developing a novel suite of geo-analytic products and services that utilize radio frequency (RF) data collected from space. The company is launching and operating small satellites in order to get a unique data set that has not been seen commercially before. The company's full constellation of satellites will likely be about thirty satellites in ten clusters. As the company starts to roll out its capability and launch its first satellites next February, it will have something very powerful and very important that is following in the footsteps of what commercial imagery did 20 years ago. Here is a capability that, historically, has been a government capability; that has now been brought commercially, using private funds. Those private funds are

invested with the intent of developing capability, in this case, for commercial purposes. But those commercial applications still need security in mind.

HawkEye 360 recognized that to be successful, there must be a day one commitment to systems and operational security. With a startup culture and budget, the company has by design built a team with deep experience in all aspects of security.

The company noted the commercial market is increasingly becoming as demanding as government markets for security. The converging security interests of the private and public sector have led to innovations in cloud technologies that the company works to leverage in combination with its own security practices. Security risks from previously unidentified threats escalate every day. Given that environment, the company hopes the U.S. government community and commercial community will continue to work together to develop and continually evolve best in class security practices. The company is looking to the commercial world and seeing what is being done to leverage proven commercial solutions, including managed cloud solutions. For instance, in the offices of HawkEye 360, you would not see racks and racks of equipment because the company is leveraging the security that Amazon and Google have already built; HawkEye 360 is taking advantage of that. The company seeks to deliver to customers a solution that is transparent, and provides active defense that is seamless.

Another Symposium participant detailed his company's work over the years for the national community in space, emphasizing that security has been a big driver for the company. To this point, a number of different changes have been implemented within the company, including the creation of a cyber group which is primarily trying to bring DOD-level security capabilities into commercial markets.

From a security perspective, loss of assets in space is a concern. Part of the concern, if not a major concern, is that when it takes 15 to 20 years to put that first asset up, the loss of that is critical. But then, you look at a small company (like the previous participant's) which has been in existence for not a very long time, and they have a six-month order-to-orbit model; one then wonders: how does that impact security, because, if I can indeed put up a payload or a capability now, in months instead of years, how can we leverage that model? The participant's company, a large enterprise, is looking at that question in terms of how do we leverage these capabilities in order to help better serve the national security market? By the same token, from the government perspective, what are the capabilities there that could be leveraged as well, directly to the government?

This puts us at an interesting paradigm: what happens to the Defense Industrial Base that is regulated by the Federal Acquisition Regulations (and many other regulations), that appear to go by the wayside when you are dealing with a commercial company? How do we level that playing field? That is something we need discussions about. When a government agency could buy something from a commercial company, maybe there is a competition, maybe there is not; maybe there are all these rules, maybe not.

From a government perspective, there is also risk aversion on the government side. The government tends to want to take 15 years to deploy a program because they want to make sure it is absolutely, positively successful. So, we will spend $10 billion to launch a satellite. Or, one could spend—divide that by 100—and one could launch 100 smaller satellites in significantly less time; is that a better model, if 90% of them fail? Is it better, now, to take the six-month order-to-orbit and say, well, for that kind of money, for that kind of speed, is it worthwhile to fail some, to succeed some? When you have these short cycles, they actually do improve your security, because you have alternatives to waiting; you have alternatives to the loss now (although, to achieve higher resolution

or higher sensitivity, costs more money and takes more time). The smaller satellites may be thought of as a quick replenishment capability, to support as needed, and thereby help deter some threats. There is a potential to do something different; maybe you do not achieve the same effect, but maybe you can achieve an effect that is good enough. The model, whereby the government invests and industry invests, could work—meaning, if the venture is successful, then government is paid back for its investment; or, if the venture is not successful, then both parties lose.

Critical Infrastructure—Positioning, Navigation, and Timing:
Outdated Policy Negatively Impacts Security

Another Symposium participant, Caitlin Durkovich, a director at Toffler Associates and previously the Assistant Secretary for Infrastructure Protection at the Department of Homeland Security, referenced the ubiquity of GPS (Global Positioning System) and PNT (positioning, navigation, and timing), emphasizing the fact that this is a government-provisioned service, it is free, and it is in nearly every critical infrastructure. As such, it underpins our way of life, and certainly our economy—from precision agriculture, to location services, to the efficiency of the electric grid; and, increasingly, as we look at smart cities, the autonomous environment, it is critical to the future. At the same time, it is a single point of failure. We do not have a backup or, at least, a holistic backup to this critical system. There are fragmented solutions that are leveraged across industry; and some of the options that would make it more resilient and more redundant—leveraging other systems like GLONASS and GALILEO—are fraught with their own vulnerabilities as well.

A further problem is that space-based positioning, navigation, and timing is governed by a very outdated policy: NSPD-39, which dates back to 2004. Policy here is largely governed within the space directorate of the National Security Council (NSC). Every now and then other parts of the NSC, such as the Resilience Directorate, or the Office of Science and Technology Policy, get involved; but it is fragmented, within the Executive Office of the President. Equally important, the governing policy gives primacy to the Department of Defense and the Department of Transportation, with some responsibility to the Department of Homeland Security. Given the ubiquity of GPS and PNT, however, the policy is outdated. Consider: when you convene the interagency on this issue through the National Executive Committee (EXCOM) for Space-Based PNT, Treasury and the Department of Energy do not even have an official seat at the table—which is somewhat ironic, given how much they have come to rely on these services. Even more important, because the EXCOM falls outside of the modern NSC processes, its recommendations have no teeth; they do not end up going to a deputies' committee or principals' committee meeting. This policy needs to be front and center, number one priority, in terms of updating Presidential Policy Directives.

Another challenge is that this area very much embodies what the public/private partnership is, yet it does not leverage some of the principles that have come to define that relationship—primarily, around how we share threat information with, not only manufacturers, but the users of the chips and of the signal itself—to help them understand what is driving government policy, and why maybe we are not making what is in their minds smart business decisions. In turn, this lends itself to the question: should space be another critical infrastructure sector? The idea has certainly been bandied around. Given that, in some ways, it is an outdated framework and an outdated structure that prevails, we do need have to have a serious conversation about this idea—much like we did with election systems and whether they should be designated critical infrastructure. At a minimum, all of the stakeholders should be brought together for discussion. Another Symposium participant proposed that we need not get too hung up on the question of whether space should be designated a critical infrastructure, since government prioritizes its efforts according to the following criteria: is it a system, asset, or network that is so important that its disruption would have a debilitating impact

on security, economic security, public health and safety, or a combination thereof? Since many of the assets, systems, and networks in space meet that definition, they will be treated accordingly, regardless of declarative status.

As we increasingly leverage technology and push towards where we are going in new space, we have to keep security in mind, and we have got to have the same kind of risk management approach that we have applied to terrestrial infrastructure. That means appreciating the threats and hazards that exist, and the whole concept of security by design. According to the director of security for a new entrant in the aerospace industry in California, however, innovation still stands in the way of security—just basic practices that we have learned about over time (concerning, for example, the insider threat). We must learn from the lessons of the past; we have to put the security experts next to the coders, developers, and builders, as we move forward. In short, as we rush to adopt technologies in the marketplace, industry needs to better understand the risks that come with it. Security and resilience need to be part of what companies do, too. A breach of security will cause you brand, regulatory, operations, and other problems; and it will cost you money. Yet, security is an afterthought, until it is not there.

The New Space Race Takes Shape

China is leading the play in space. It has poured much into this, and has much coming from foreign sources. Europe has served as an open-source support element for the Chinese space program. Since most advanced European nations do not have laws regarding just discussion, there is a running stream of European scientists going to and from China, spending 3 or 4 months twice a year (at Beijing University and other places throughout the country), developing China's small-satellite program. As a result, China has moved tremendously quickly in a very short period of time. By comparison, the way our own systems are working is deeply problematic. Consider the Austrian scientist who tried moving his work through the European Space Agency (ESA) for 3 years, and could not get anywhere with the massive bureaucracy, until he went to the Chinese. And now it is China that is doing groundbreaking work in quantum communications.

Cybersecurity in the Financial Services Sector

Issue Brief Series on Trends in Technology and Digital Security

Panelists
John Carlson - Financial Services Information Sharing and Analysis Center
Adam Palmer - Financial Services Roundtable
Scott Petry - Authentic8

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

The Ecosystem: A Snapshot

Banks are on the front lines, under cyber-assault daily, since that is where the money is. However, banks are stress-testing and exercising aggressively; and can absorb the intelligence surrounding cyber incidents, since the sector is dedicating significant resources to cybersecurity. When you think about public-private partnerships in the context of cybersecurity, they tend to be long on nouns and short on verbs; but when it comes to the financial services sector, it is the gold standard. Industry groups that seek to foster collaboration within and beyond the financial services sector, for cybersecurity and other purposes, include the "FS-ISAC" and "BITS".

FS-ISAC: Financial Services - Information Sharing and Analysis Center

What is the FS-ISAC and what does it do? The FS-ISAC consists of about 7,000 financial institutions, now in thirty-nine countries, with about 100 staff members located in eight countries. It is one of the primary vehicles for sharing threat and incident information, both for cyber and physical matters. As a result, the FS-ISAC has been very busy with Hurricanes Harvey and Irma, with a lot of work falling on its plate simultaneously. As a vehicle for sharing information and analysis, it should be emphasized that the FS-ISAC is all voluntary. It is not a government agency. It is a 501(c)6 non-profit organization funded by its 7,000 member-firms and sponsors.

In addition to information sharing, the FS-ISAC is also involved in conducting exercises, many of them in conjunction with the U.S. Treasury Department—through a highly successful series, called the Hamilton series—which looks at different types of cyber-attacks in different parts of the industry, to simulate how industry and government would respond to such events. This activity has been immensely helpful, for both the public and private sector, to understand what our vulnerabilities are, and what are some initiatives that we need to fill the gap.

The FS-ISAC has also been responsive to Presidential Executive Orders, including one that designated some of the largest firms as critical infrastructure. In this regard, the FS-ISAC launched a separate subsidiary—the Financial Systemic Analysis and Resilience Center (the FSARC)—that was formed by eight large financial services firms (now up to sixteen), to come together to collaborate much more deeply on information sharing, intelligence, analysis, and also working with law

enforcement to respond to a growing threat of cyber criminals and enterprises. FSARC's mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cybersecurity threats, through focused operations and enhanced collaboration between participating firms, industry partners, and the U.S. government, including the Department of the Treasury, the Department of Homeland Security, and the Federal Bureau of Investigation.

FSARC collaborates with U.S. government partners and plans to expand its operational processes, establish a physical location for the Center, and add additional financial institutions that are eligible to participate. That initiative is now launched, underway, and getting fully staffed up. The FSARC is another way that the FS-ISAC is working in partnership with the U.S. government to understand threats to the sector, particularly on the critical infrastructure side, with a current focus on liquidity risks and wholesale payments.

The FS-ISAC is thus a platform for collaboration, discovery, and mutual support, not only around events (whether cyber or physical); but also for understanding what the vulnerabilities are, how they could impact the industry, and what the industry should do in response to that. As a result of this collaboration, the FS-ISAC also puts out products—best practices papers—and has done a lot of work, in this regard, around ransomware and account takeover attacks.

The FS-ISAC has also done some interesting work around destructive malware. That was one of the early Hamilton exercises, which simulated a SONY Entertainment type-attack, where malware basically destroyed SONY's systems. What was really concerning about that case, from a critical infrastructure protection perspective, was that the attackers destroyed data. For the FS-ISAC, that was a very concerning development, in that FS-ISAC members are highly dependent upon the availability and integrity of data for consumer and investor confidence. One after-action task was the preparation of a best practices paper on actions financial institutions should consider before, during, and after, a destructive malware attack.

Another outcome of a Hamilton exercise was the creation of another subsidiary of the FS-ISAC—called Sheltered Harbor. Sheltered Harbor was established in 2016 to enhance the financial services industry's resilience capability in the event of a major disaster event. Sheltered Harbor is based on standards and the concept of mutual assistance. Should a financial institution be unable to recover from a cyber-attack in a timely fashion, firms that adhere to the Sheltered Harbor standards will enable customers to access their accounts and balances from another financial institution. Sheltered Harbor members access specifications for common data formats, secure storage ("data vaults") and operating processes to store and restore data, and receive a Sheltered Harbor acknowledgement of adherence to the specification. Accordingly, there is a mutual support component, and also an extra layer of consumer protection. The idea is, hopefully, to mitigate market impact, in terms of concerns about the integrity of data across the industry (systemic risk).

The above are examples of what the FS-ISAC is involved in, but it really starts with people coming together voluntarily in a trusted environment, through emails, conference calls, and the entity's secure portal in which one can post information. Having control over how that information may be used by others is immensely important; hence, the FS-ISAC operates according to what is known as "the traffic light protocol": "Red" means the information is for the member's eyes only. "Amber" means that you can share with others on a need-to-know basis. And "Green" means that you can share with government partners and others.

Finally, the FS-ISAC's intelligence officer has played a very important role, fostering collaboration with law enforcement, and working with other critical infrastructures. The FS-ISAC intelligence

officer sees information coming through the voluntary channel; she flags it and then seeks consent from the relevant parties to be able to share that information with government parties, in order to make requests of government agencies to see if there are other pieces of information that they can share and potentially declassify. This process builds trust between the public and private sectors.

BITS: The Technology and Policy Division of the Financial Services Roundtable

The Symposium was joined by Adam Palmer, Vice President of Cybersecurity Risk Management at the BITS division of the Financial Services Roundtable. The Financial Services Roundtable (FSR) consists of roughly the top 100 financial services companies, as determined by market capitalization. FSR is involved in regulatory policy issues, housing policy issues, and cybersecurity matters. The FSR cybersecurity focus group is BITS, which concentrates upon operational cybersecurity issues/risks.

A top BITS priority is regulatory harmonization for cybersecurity. Here the goal is to try to encourage government to harmonize, not duplicate; to align, not layer. BITS also seeks to encourage the regulators and the government to step up their game, to have strong data security for BITS members. BITS also seeks to encourage public-private partnerships, in order to foster collaboration across the government and with BITS member-firms, with the aim of trying to improve policy as it pertains to response during a major incident.

In terms of key programs, the policy group of the regulatory arm of BITS is currently highly focused on the issue of domestic alignment—rather than duplication—in the context of the question: What if all fifty U.S. States were each to develop their own cybersecurity frameworks? (New York, for one, has done so). But, what if each State framework were different? The matter is also an issue at the international level.

BITS seeks to identify best practices, for efficiency, and for other purposes. As an example, BITS is presently hosting joint meetings of its Security group and its Fraud group, looking at the synergy and shared concerns between the two. Despite the existence of overlap, the CISOs and the Fraud (prevention) leaders in organizations are often very siloed. Therefore, BITS is looking at improving this operational structure to foster coordination and faster response.

BITS is also looking at the impact of new technology. Everybody wants technology that is faster, better, operational, scalable, and safe. Here, there are some significant issues concerning the financial services sector, including:

1. Artificial Intelligence. How can you use A.I. to improve and automate overall data governance?

2. Quantum Computing. How close are we to a threat where a quantum computer can defeat encryption?

3. Cloud Computing. While it is not a completely new paradigm (as we have entrusted information to third-party computers externally for a long time), the key is how you implement controls; i.e., how do you effectively monitor your system, and manage those controls that are being enforced?

4. Blockchain. Many financial services firms are considering Blockchain as an authentication tool. It may enhance authentication, and there is much talk about how to implement this distributed ledger technology. And, finally:

5. Active Cyber Defense. How far, from an operational policy standpoint, are you willing to go? What is the role of government and of the private sector? What is allowable from a policy perspective? How far can private entities go to gather intelligence on attackers who are aggressively targeting companies? There is still a feeling that cybersecurity strategy is "4,000 years old", meaning that we are still building a higher wall. As Symposium panelist Adam Palmer explained, BITS members do not just want to be a victim and build a higher wall each year, and then watch the bad guys get together and break through the wall. At some point, companies say: What can I do to empower law enforcement, what can I do to cooperate with the authorities and actively improve my defense? Is there more that I can do to be secure, beyond just improving my defense?

Another important BITS activity is the CEO Council. BITS is working with its CEOs to develop and process responses to major threats. For example, what happens if a major U.S. bank loses all communications with Asia? How does the government provide for mutual assistance, or support in the form of another financial institution stepping in to help? What is the regulatory relief that might be provided to allow this? How would institutions support, in this scenario? The related jurisdictional, policy, and operational issues need to be settled at a high level.

A further concern, at the government agency level, is regulator data security. If there is a data breach and a BITS member has to report that information by disclosing and sharing it with the regulators, are they secure? What does the U.S. government do to secure that data, to protect it? BITS seeks to have an open dialogue about how that data is to be used and protected.

In summary, BITS tries to be proactive, not reactive, to these issues in the financial services sector, keeping in mind that financial services firms are on the front line of cybersecurity. Adam Palmer, the Symposium member from BITS, emphasized the need to focus not only on risks, but on positive solutions.

Taking a Different Tack: Neutralizing the Threat Space with a Remote Browser

Rather than analyzing the threat space more deeply, another Symposium participant detailed a different, less traditional, approach to cybersecurity, pursuant to which the central question is: What if the threat space was irrelevant? To this end, the participant's company builds a one-time use, disposable browser, in the cloud. It allows you to interact with the Web through a full-fidelity interactive display, but no Web code ever reaches your environment. In fact, no IP attribution of your environment is ever exposed to the Internet.

The concept is simple: the browser is built fresh at the start, you use it, and it is destroyed at the end of the session. There is no need to worry about the content coming into your network, if it never touches you. No cookies, trackers, or malicious code ever reaches the end device. All you receive is an encrypted remote display of that session. You do not need to worry about links you may have just clicked. Any malware has no access to local system resources, like the registry or file system; and since that malware executes in a virtual environment and gets destroyed at the end of the session, it cannot persist. By analogy, it is like using rubber gloves when you change the wheel of your car; you do not need to worry about washing your hands, since you have rubber gloves on.

Virtualizing the browser is not an inherently new idea. Citrix and VMware have been doing things like this "forever." Cloud infrastructure is not inherently new either. The cloud has been around for years, and has become commonplace. We have seen ebbs and flows between centralized and decentralized computing capabilities since the dawn of the computer age. The browser is a completely decentralized application. And the ability to manage applications with enterprise policies is not inherently new.

But the participant's company has combined the virtualization and embedded policies within the browser, which has not been done before—a secure remote browser with policies to govern things like access controls, user credentials, data loss prevention policies, and more. When packaged as an integrated solution that allows an organization to deploy a browser that supports specifically their mission—whether it is safe browsing for employees, regulated employees accessing regulated data without violating compliance, or mission analysts conducting open-source intelligence for cybersecurity counter-research— through a spoofable and disposable infrastructure, the solution is highly disruptive.

By contrast, consider the present state of the cybersecurity industry: I.T. is conditioned by the cybersecurity vendor community to buy the latest, greatest, next-generation technology. Every time a new threat emerges, a new set of "next-gen." technologies are marketed, which promises to solve the latest threat. It started with executable blocking and IP blacklisting; then data analytics; now it is machine learning and artificial intelligence.

Yet, if you look at what data is coming into the network and puts it at breach, a large percentage of that data comes from the browser. The browser was designed in the 1980s, at the research consortium CERN, which was what Tim Berners-Lee described as "a safe environment"—for sharing research papers, text-based, internally within the research community. The protocols are brilliant and resilient. But they were not designed with any concept of security or content controls. Basically, a browser makes a connection to a host, the host bundles up a big blob of data, delivers it down to the browser, and the browser dutifully renders that content.

Since then, however, that environment has exploded dramatically: today, every page view delivers a payload to the browser that contains cookies, trackers, potentially malicious links, redirects, suspect or malicious content like Flash or Javascript. And the cybersecurity industry sells to I.T. more single "drugs" to attack more single "bugs" to try and close that environment. These solutions try to detect the threat after it has reached the network and device. This "one bug, one drug" approach is "a mess"—I.T. is on a never-ending "hamster wheel" of purchasing more technology that works too late—after the malware has breached the network. The participant's company offers an alternative, simpler approach: put the browser in an environment that does not expose your environment—a browser that runs remotely and that you can throw away when you are done.

Israel: The Making of a Cyber Power (Case Study)

Issue Brief Series on Trends in Technology and Digital Security

Featured Speaker
Dr. Eviatar Matania
Director General, Israel National Cyber Directorate
Prime Minister's Office

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

The Role of Government in Technology and Innovation

Why is Israel so successful in the cyber domain? What ingredients make up that ecosystem? While it is tempting to talk about technology in reply, Dr. Eviatar Matania, the Director General of Israel National Cyber Directorate (INCD) within the Prime Minister's Office, spoke in-depth about government—specifically, how the Government of Israel approached the cyber challenge, and how it sought to mitigate the problems the country faced in this domain. What follows is a lightly adapted version of his remarks.

Before turning to cybersecurity, it is important to understand the unique role of a government in developing national capacities. While governments are often considered to be a negative factor in regards to innovation, Israel offers a few interesting examples for positive government involvement.

The first case study starts in 1992. Israel was a small economy (and still is), with a high percentage of its GDP attributable to exports/imports. At the beginning of the 1990's, Israeli imports amounted to more than 35% of the country's GDP, while exports were below 20% of GDP, which showed that Israel had a problem: the import-export gap.

During the 1950's and '60s, agriculture was the leading export branch of the Israeli economy. Step by step, the country entered into the industrial revolution and, in particular, into the hi-tech arena. At the beginning of the 1990's, everything was ready for a new economy: Israel had both experience and success with its technology-oriented defense industries. The country had very talented graduates of its military units. Many experienced engineers and managers returned to Israel from the corporate arena and the hi-tech economy of the United States. Israel also enjoyed skilled immigration from Russia, including a great deal of engineers. All of these elements were in place, but nothing happened. Yet there was a need, a real need, to have a new economy in Israel.

And then the Government stepped in with a pioneering program, called "YOZMA" (Hebrew for "Initiative"), that changed everything. It was a very small program, but with a regulator that did not think the way government regulators usually think. The question was: how to build a hi-tech economy in Israel? At the time, Israel had almost no venture capital funds (VCs) and the industry lacked reliable sources of investments. Therefore, the Government of Israel called investors to

establish VCs in the country. The "YOZMA" program promised to investors to match their investments, through a very tempting mechanism: the Government would share the risk together with investors, but the upside would belong only to the investors—the Government would step out at that point.

The ten "YOZMA"-backed VCs in Israel were very small, about $20 million each. However, they were very successful and later grew into $50-100 million funds, while many other local and foreign VCs joined the community. All in all, several dozens of billions of dollars have been raised by the hi-tech sector in Israel since the introduction of "YOZMA." Israel became what is now called "start-up nation" or "hi-tech nation."

During the last decade, Israel exported much more than it imported, while 50% of Israel's exports derive from the hi-tech industry. The Government of Israel knew when to enter the market, but also had the wisdom to get out—leaving the business community to do the rest.

The second successful case study was water. Israel was a thirsty country; it did not have enough water. The country needed water for drinking water, agriculture, industry, etc.; but had only very small sources of water. The first step was to build awareness through an educational campaign to "save each drop." Then, the Government decided to step in, with a program that encouraged the business community to build water desalination facilities, with a promise of 25-year contracts; and a program encouraging the use of recycled water in agriculture.

In recent years, Israel has, marvelously, become a country which has enough water; and not just for its own needs, but also for its friends and neighbors (Jordan, for example). Today, over 85% of the water in Israel is re-used—which makes Israel the leading country in the world in this regard, with a re-use percentage far higher than any other country. Over 50% of drinking water comes from desalination plants. In the past four years, Israel has suffered a severe drought; but this was hardly felt by Israeli citizens. Nevertheless, water is still a challenge, especially in regards to ecological concerns—in fact, Israel is now preparing to bring water back to the Sea of Galilee.

Building a Cyber Ecosystem in Israel

These cases were in my mind, as Director General of Israel National Cyber Directorate within the Prime Minister's Office, when I was instructed by the Prime Minister in January 2012, to make Israel one of the leading cyber powers in the world. Israel was already in a great position, but the question was what should be the role of the Government in taking the country another step forward.

In addition to its more obvious role in building national security in and through the cyber domain, the Government of Israel also understood that Israel needed a strong and flourishing cybersecurity ecosystem in the country. To achieve this, the Government first had to consider existing strengths: in the country's universities, there were a lot of researchers in computer sciences. Four of Israel's faculties of computer science were included in the top-twenty leading in the world. The Hebrew University mathematics department was one of the three leading in the world. Israel was in a good position; however, there was not enough cyber research.

Next, we went to see what was happening with the industry. A lot of ideas, a lot of startups, and technology; but, industry said, we do not have enough people, we need more human capital.

At that point, the Government introduced a national program. First, as part of the strategy, Israel aimed (and continues to aim) to develop high quality human capital. Starting at the ages of 14 and 15, the state nurtures cyber skills. With the Israeli Defense Forces, which everyone goes through

because of the country's compulsory service, Israel trains the best people to work in cybersecurity during their term of service; and then, to go out and be part of industry and academia. Together with its universities, Israel finds and screens the best students at the age of 15, to take them to preparatory study, to high school; and to study for the B.Sc. in computer science or technical engineering, with two more years before military service, to complete their degree and then go into the military service.

Second, the Government approached all of the country's universities, declaring the need for cyber research centers, because, if we want to be a cyber power, we need universities to step in. However, the universities demanded that the Government fully finance new cyber centers. The Government, on the other hand, was ready to match funds and be a partner: for each dollar the universities raised, the Government would match with another dollar. Eventually, most universities participated, and now Israel has six cyber research centers.

On the industry side, the Government also initiated national programs where there was a need; again, not to replace the business community, not to tell them what to do. The programs sought to do just one thing: initiate more startups, by sharing the risk in very risky research and development (R&D) projects. Together with some funds from the Minister of Economy, the Government presented some tools, where very risky R&D projects can come to the Government, and it will share 50% of the risk, for one to two years. At that point, the Government simply requires a return of the investment if that project succeeds. If you do not succeed, the Government shares the risk. That's all. And with very small funds (in government terms), some $25 million for two years, the program initiated a lot of risky projects, thus pushing the industry forward.

The current situation in the cyber arena in Israel is phenomenal: if you look at the hi-tech industry of Israel, it is the highest in the world per capita (e.g., the number of engineers and scientists—Israel is first in the world, relative to other nation-states). Israel's R&D, as a percentage of GDP, is first in the world. Largely thanks to the national programs, Israel is objectively (not just per capita) second in the world in cyber; second, of course, to the United States. The revenues of Israeli cybersecurity companies have almost doubled themselves in five years, from $2 billion in 2012 to nearly $4 billion in 2017, which is 10% of Israel's hi-tech exports. Israel has more cyber companies than the world combined, with the exception of the United States. Israel attracts almost 20% of the world's private investment. Yet Israel is just 0.01% of the world's population. While these statistics are a source of pride, Israel is doing what it does out of necessity, because of the country's security needs and economic needs. The Government tries to look for partners, adopting a humble mindset, that it is not the only entity with the "right" ideas.

Lessons Learned, Moving Forward

Looking at small- to medium-sized countries around the world, government has a role. Analyzing the success of the Government of Israel in the above cases yields four key pointers: first, the Government succeeded when there was a real need, a necessity (be it water, the economy, or cyber). Second, a national program succeeded when the Government tried to understand the whole ecosystem, and not just interfere where it should not be. Most of the time, the right thing for a government, is to understand where it does not have to be (for example, with cyber: Israel has almost no regulations). Third, the right framework: how to initiate, how to encourage the business community? Funding alone, in and of itself, will not work; the government must find the right way to harness the market through a national program. Fourth and finally, it cannot happen if there is no base: if the industry is not there, if the investors are not there, the government could not replace them. The government needs to examine what is missing, identify market failure, and explore ways to trigger the desirable actions.

To conclude, I would like to refer again to cyber. Cyber is one of the most important phenomena of this age—changing our economies, our way of life, and our national security—and it is just beginning. We are now at the point at which government may still have the possibility of shaping this new world, and harnessing cyber as a power for encouraging growth and welfare. To do so, government must act decisively, and formulate grand strategies to cope with this issue.

Contributor Biographies

Steve Pann
Razor's Edge Ventures

Steve is a Founding Partner at Razor's Edge Ventures. Steve focuses on investments in big data, high performance computing, sensors, space, and visualization, situational awareness and geospatial mission tools. He presently serves on the Board of Directors of Razor's Edge portfolio companies Ryft Systems and Altamira Technologies and is an observer to the Board of Directors of HawkEye360. He is also actively involved in managing the Fund's investment in Spaceflight Industries.

Steve currently acts as a consultant with the Raytheon Advanced Concepts and Technology Organization.

Before joining Razor's Edge, Steve was the Chief Strategy Officer at Blackbird Technologies, a co-founder, and member of Blackbird's Board of Directors. He leveraged over thirty years of experience developing and deploying unique technologies in support of Government operations both as a career science and technology officer and in his former role as Blackbird's strategic planning leader. Steve is widely recognized within the national security community as a thought-leader with a truly unique capacity and unrelenting drive to anticipate and shape technological change. He has a strong history of investing in and creating highly successful technology companies. Over the past fifteen years, Steve has consistently leveraged his emerging technology expertise together with his entrepreneurial instincts to architect, plan and expand some of Blackbird's most strategic programs in the areas of persistent surveillance, information operations and cyber security. Steve is a highly respected leader in the mid-Atlantic technology community and greater Washington D.C. business community.

Steve earned a bachelor's degree in Political Science and Criminal Justice from American University and served as an infantry officer in the United States Marine Corps prior to joining the Government.

Frank Cilluffo
GWU Center for Cyber & Homeland Security

Frank J. Cilluffo is an Associate Vice President at The George Washington University and Director of the Center for Cyber and Homeland Security, is co-director of GW's Cyber Center for National and Economic Security, and along with the School of Business, launched the university's World Executive MBA in Cybersecurity program.

Cilluffo is routinely called upon to advise senior officials in the Executive Branch, US Armed Services, and State and Local governments on an array of national and homeland security strategy and policy matters. He also frequently briefs Congressional committees and their staffs and has testified before Congress over 25 times at high profile hearings on counterterrorism, cyber threats, security and deterrence, weapons proliferation, organized crime, intelligence and threat assessment, as well as emergency management, border and transportation security. Similarly, he works with US allies and organizations such as NATO and Europol. He has presented at a number of bi-lateral and multi-lateral summits on cybersecurity and countering Islamist terrorism, including the UN Security Council.

Cilluffo has published extensively in academic, law, business, and policy journals, and magazines and newspapers worldwide, including: ABC News, Foreign Policy, The Journal of International Security Affairs, The National Interest, Parameters, Politico, Studies in Conflict and Terrorism, USA Today, US News & World Report, The Washington Quarterly and the Washington Post. He currently serves on the editorial advisory board for Military and Strategic Affairs and routinely acts as a reviewer for other publications and for grant-making foundations.

CCHS is a prominent nonpartisan "think and do tank" dedicated to building bridges between theory and practice to advance US security. CCHS has hosted numerous Cabinet Members and agency directors, military and law enforcement officers, Members of Congress, diplomats, business executives and academics and has issued dozens of reports widely cited by media, research institutions, think tanks and governments.

Sharon Cardash
GWU Center for Cyber & Homeland Security

Sharon L. Cardash is Associate Director of the George Washington University Center for Cyber and Homeland Security. Her publications on cybersecurity, counterterrorism, and homeland security issues have appeared in major newspapers, a wide range of digital media sources, and scholarly journals. Before joining GW in 2005, she served as security policy advisor to Canada's Minister of Foreign Affairs. Prior to that, she worked at the Center for Strategic and International Studies, where she managed task forces on counterterrorism and cybersecurity. Cardash holds a Law degree (J.D.) from the University of Toronto, a Master's degree (M.Phil.) in International Relations from the University of Cambridge, and clerked for Justice Joseph T. Robertson, then of the Federal Court of Appeal of Canada.

The Honorable Charlie Allen
The Chertoff Group

The Honorable Charles E. Allen, also known as Charlie, serves as a Principal at The Chertoff Group, LLC. At DHS, Hon. Allen developed the department's intelligence architecture, integrated its intelligence activities and ensured that they were continuously aligned with the department's evolving priorities. He also accelerated and expanded the department's processes for sharing intelligence with state and local security and law enforcement officials. He has extensive experience in intelligence program management, analysis and production; intelligence collection management; system acquisition and warning intelligence.

During his more than 40 years at the CIA, he became as much a legend as a respected senior official. He earned a reputation for plain speaking, even when his opinions differed from those of senior officials. He became the principal adviser to the Director of Central Intelligence on collection management, where he revolutionized the way the various national intelligence agencies coordinate and target their activities. He served as an Assistant Director of Central Intelligence for Collection since 1998. Hon. Allen chaired the National Intelligence Collection Board, which united all intelligence agencies under common collection strategies. He also served as CIA's National Intelligence Officer for Warning, Director of the National Warning Staff, National Intelligence Officer for Counterterrorism and Deputy Chief for Intelligence of CIA's Counterterrorism Center.

He directed the DCI Hostage Location Task Force, which focused on locating American hostages held by Hezballah in Lebanon. He served as Director of the DCI Hostage Location Task Force from 1985 to 1987. He serves as a Member of Advisory Board at The KEYW Holding Corporation and MicroLink, LLC He serves as Member of Advisory Board at Camber Corporation. He serves as a Member of Strategic Advisory Council at Vencore, Inc. He serves as a Member of Strategic Advisory Group at A-T Solutions, Inc. He is a graduate of the University of North Carolina and a distinguished graduate of the Air War College; he also did graduate studies at Auburn University.

Michael Brett
QxBranch

Michael co-founded QxBranch to drive commercial application of advancements in data analytics and quantum computing. QxBranch focuses on analysis of challenging analytics problems in for finance, insurance and technology customers, applying expertise in quantitative analytics with quantum computing technology. The company has offices in Washington, D.C., Adelaide, Australia and Hong Kong. Prior to QxBranch, Michael was Chief Operating Officer of Shoal Group (formerly Aerospace Concepts), a systems engineering firm based in Canberra, Australia where he was responsible for daily operations and project delivery across the company. At Shoal Group, he worked in several project leadership roles on systems engineering projects, including predictive risk analysis for hypersonic flight vehicles, delivery of broadband satellite communications to Antarctica, helicopter training simulation and safety analysis of the atmospheric re-entry of the Japanese Hayabusa spacecraft.

Earlier in his career, Michael was lead systems engineer with start-up company Flaik to develop the award-winning tracking system for recreational skiers and snowboarders which has since been rolled out to around 15 major ski resorts in North America. He began his professional life as a systems engineer with Ball Aerospace developing mission planning software for the Australian Department of Defence. Michael's work in leading technology organizations has been recognized many times including selection as one of five global Young Space Leaders by the International Astronautical Federation in 2014, an Australian Leadership Award in 2013, and one of the Most Inspiring Young Engineers by Engineers Australia.

He has authored several technical publications in the field of probabilistic risk analysis and has been interviewed by news outlets such as Washington Post, Australian Financial Review, South China Morning Post, and ABC Science Online. He holds an Executive Master of Business in Complex Project Management and a Bachelor of Engineering in Aerospace Avionics, both from Queensland University of Technology in Brisbane. In his free time, Michael is an avid runner, cricket enthusiast and terrible snowboarder.

John Carlson
Financial Services Information Sharing and Analysis Center

John W. Carlson is the chief of staff of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and active in the Financial Services Sector Coordinating Council (FSSCC), including vice chairman from 2015-17. The FS-ISAC is a non-profit corporation formed in 1999, funded by its 7,000 member organizations and focused on assuring the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global

economy. Prior to joining FS-ISAC, Carlson served as the Executive Vice President of BITS/Financial Services Roundtable and Managing Director of Morgan Stanley.

John also served in a variety of roles at the Office of the Comptroller of the Currency, U.S. Office of Management and Budget, Federal Reserve Bank of Boston, and United Nations Centre for Human Settlements. Carlson holds a Masters of Public Policy from Harvard's Kennedy School of Government and a B.A. from the University of Maryland.

Mike Davis
CounterTack

As CounterTack's CTO, Michael Davis is responsible for driving the vision and advancement of CounterTack's Endpoint Threat Platform, as well as leveraging his visionary approach to push defenders ahead of attackers. Davis is one of the nation's leading authorities on information technology, authoring top selling book, Hacking Exposed, and contributing to publications such as InformationWeek and Dark Reading.

He was voted one of the "Top 25 under 25" by BusinessWeek, and named semi-finalist of the Ernst and Young "Entrepreneur of the Year" award. In 2005, he founded Savid Technologies, an IT security consulting firm. By 2010, Savid was ranked 611 on the Inc. 5000 list of fastest growing companies in America. Prior to Savid, he served as senior manager of global threats at McAfee, where he led a team of researchers investigating confidential and cutting-edge security analysis.

Chris DeMay
HawkEye 360

Chris, HawkEye 360's co-founder and COO, came up with the idea for HawkEye while serving at the NRO, where he was responsible for space-based intelligence technology development projects and programs. He spent fourteen years in various leadership positions with the U.S. Federal Government, and was the proud recipient of the NRO Gold Medal of Distinguished Performance and the Frank Beamer Award for Exceptional Service. Chris holds an MS in Systems Engineering and a BS in Business Information Technology, both from Virginia Tech. He is a fan of third-wave coffee, traveling, and graphic design, and fondly remembers his stint as lead singer of his college rock band. Chris lives in Chantilly with his wife and two children.

George Duchak
U.S. Department of Defense

George Duchak was recently named Director, Defense Innovation Unit – Experimental, by the Department of Defense. He is the former Director, Air Force Research Laboratory's Information Directorate, Rome, NY; a former DARPA (Defense Advanced Research Projects Agency) Program Manager; and a businessman with more than a decade of private industry experience.

DIUx is a Silicon-Valley based initiative that will serve as a conduit between leading edge innovators and the Department of Defense. After retiring from the United States Navy, George was recruited by DARPA where he developed and transitioned a variety of programs in the broad area of C4I and Cyber. In private industry he started several companies that served the US Government by providing technical consultancy or product. The product focus was principally in the area of intelligence

exploitation using crowd sourcing techniques and big data analytics. George most recently led the Air Force's and nation's premier research organization for command, control, communications, computers and intelligence (C4I) and cyber technologies.

The mission of the Information Directorate is to explore, prototype and demonstrate high-impact, game-changing technologies that enable the Air Force and nation to maintain its superior technical advantage. He directed basic research and advanced development activities in information exploitation, information fusion, information understanding and management, cyber operations, connectivity and networks, command and control, and advanced computing architectures.

He oversaw a workforce of 1,166 military, civilians, and on-site contractors and executed an annual budget of over $1 billion. George earned a Bachelor of Science degree in mechanical engineering from the U.S. Naval Academy, a Master of Science in Aerospace Avionics and the Degree of Aeronautical Engineer both from the Naval Postgraduate School, a Master of Business Administration from The Ohio State University, and a Doctorate of Philosophy in Public Policy from George Mason University. He is a graduate of the Advanced Management Program at the University of Chicago Booth Graduate School of Business and completed the Program Management Course at the Defense Acquisition University. He is a member of the Senior Executive Service.

Caitlin Durkovich
Toffler Associates

Caitlin's expertise in critical infrastructure security and resilience, including cybersecurity, makes her a uniquely valuable asset to clients navigating the complex operational challenges posed by our increasingly interconnected and interdependent global economy. Over the course of nearly two decades of developing physical and cyber risk management approaches, she has successfully advanced public-private partnerships that drive thought leadership, influence policy, and evolve industry practices to manage security and operational risks.

Prior to joining Toffler Associates, Caitlin served as Assistant Secretary for Infrastructure Protection with the Department of Homeland Security under President Obama. She led the mission to protect critical infrastructure and redefined public-private risk management for emerging issues like complex mass attacks, electric grid security, cybersecurity, GPS resilience, and climate adaptation planning. Her experience also includes leading homeland security projects with several government agencies while at Booz Allen Hamilton and pioneering early warning cyber intelligence at iDefense (acquired by Verisign).Caitlin earned a B.A. in public policy studies from the Terry Sanford Institute of Public Policy at Duke University and a certificate in business strategy from The Aspen Institute.

Nick Eftimiades
Penn State University

Nicholas Eftimiades graduated from George Washington University with a B.A. in East Asian Studies and the National Defense Intelligence College with a M.S. in Strategic Intelligence. He also did undergraduate and graduate work in Asia. He is a Visiting Research Fellow at King's College, War Studies Department, London, United Kingdom, and has a 30 year government career which includes seven years at the National Security Space Office leading engineering teams designing "generation after next" national security space capabilities. He was also Senior Technical Officer in the Defense Intelligence Agency, Future's Division, and Chief of DIA's Space Division. He served as DIA's lead for national space policy and strategy development.

Mr. Eftimiades has provided numerous briefings and testimony on national security, technology, and space exploration issues to senior policy officials and the U.S. Congress. He testified before the President's Commission on Implementation of United States Space Exploration Policy. He has sponsored and chaired international conferences on U.S. and foreign defense policy issues. He is a frequent lecturer and public speaker on future technology and societal changes and national security issues.

Anup Ghosh
Sophos

Anup Ghosh is Chief Strategist, Next Gen Endpoint at Sophos. Ghosh was previously Founder and CEO at Invincea until Invincea was acquired by Sophos in March 2017. Prior to founding Invincea, he was a Program Manager at the Defense Advanced Research Projects Agency (DARPA) where he created and managed an extensive portfolio of cyber security programs.

He has previously held roles as Chief Scientist in the Center for Secure Information Systems at George Mason University and as Vice President of Research at Cigital, Inc. Anup has published more than 40 peer-reviewed articles in cyber security journals.

He is a frequent on-air contributor to CNN, CNBC, NPR, ABC World News, and Bloomberg TV. A number of major media outlets carry his commentaries on cyber security issues including the Wall Street Journal, New York Times, Forbes, Associated Press, FoxNews, CSM Passcode, Federal Times, Market Watch and USA Today. He has served as a member of the Air Force Scientific Advisory Board and the Naval Studies Board, informing the future of American cyber-defenses.

Shang Hsiung
Raytheon

Shang Hsiung is an Engineering Fellow with Raytheon IIS Advanced Concepts and Technology. In this role, he is responsible for providing technology guidance in strategic areas as well as supporting growth initiatives across ACT including commercial integration, analytics, cyber and space activities. Shang has over 30 years' experience in Intelligence, Surveillance, and Reconnaissance programs, twenty eight with Raytheon.

Prior to his current role, Shang led business development at RTN Applied Signal Technology. He also led the airborne component of the High Energy Laser Enterprise Campaign and was the capture manager for Laser Weapon System programs. He was Photon Research Associates' Innovation Cell director where he was chartered to create new concepts and mission solutions for customer hard problems. Shang was the Chief Engineer of the Advanced Programs, Ground Enterprise Solutions and Strategic Intelligence Systems product lines in IIS. He led the corporation's Horizontal Integration Enterprise Campaign which developed integration and information sharing technologies to improve the capabilities of the intelligence community.

His background prior to the enterprise campaign was in tactical systems, primarily airborne and associate ground SIGINT and was the chief engineer for the Tactical Intelligence Systems product line. He was the chief systems engineer as well as hardware lead for the current generation of U2 RF INT systems. Before joining Raytheon, he worked at Norden Systems, M/A COM Linkabit and HRB Singer from 1982-1988. Shang holds a bachelor's degree in Electrical Engineering from the University of Maryland.

Sean Kanuck
International Institute for Strategic Studies

Sean Kanuck was appointed as the first National Intelligence Officer (NIO) for Cyber Issues in May 2011. The NIO leads the US Intelligence Community (IC) in cyber analysis, directs the production of National Intelligence Estimates, and represents the IC on cyber issues when briefing the White House and testifying before Congress. Kanuck previously served in CIA's Information Operations Center, as an Intelligence Fellow with the National Security Council, and on the US delegation to the UN Group of Governmental Experts on international information security.

He is a professional attorney whose academic publications focus on information warfare and international law. He holds degrees from Harvard (A.B., J.D.), the London School of Economics (M.Sc.), and the University of Oslo (LL.M.).

Eviatar Matania
Director General, Israel National Cyber Directorate, Prime Minister's Office

Dr. Matania is the Director General of Israel National Cyber Directorate (INCD) since its establishment, in direct subordination to the Prime Minister, and a global leader in cyber policy and national cyber strategies.

The INCD leads the formation of Israel's national cyber strategy and promotes the national efforts it requires, both the capacity building and the operational defense. Dr. Matania is a graduate of the elite academic program 'Talpiot'. He holds a B.Sc. in Physics and Mathematics (Hebrew University), a M.Sc. in Mathematics with an expertise in Game Theory (Tel-Aviv University), and a Ph.D. in Judgment and Decision Making (Hebrew University). Dr. Matania has diverse experience both in military and civilian R&D, including system analysis and project management, focused primarily on entrepreneurship of ideas and entities. Among others, he co-edited a book on Israeli start-ups and taught venture capital courses and decision making in distinguished Executive MBA programs.

Jason Matheny
Director, Intelligence Advanced Research Projects Agency

Jason Matheny has led IARPA's research and forecasting efforts on national security issues and managed the *Foresight and Understanding from Scientific Exposition*, *Forecasting Science and Technology* and *Open Source Indicators* programs.

He initially joined the Office of the Director of National Intelligence in 2009 as the *Aggregative Contingent Estimation* program manager within IARPA's Office of Incisive Analysis, where he oversaw the transition of technology to the intelligence community. Matheny previously worked at the University of Oxford, Johns Hopkins University Applied Physics Laboratory, and the University of Pittsburgh Medical Center's Center for Biosecurity and Princeton University and a recipient of an IC award for individual achievement in science and technology and holds a doctorate and a master's degree from Johns Hopkins.

Adam Palmer
Financial Services Roundtable

Adam Palmer began his career as a U.S. Navy JAG Officer focusing on cybercrime prosecution, and has now joined The Financial Services Roundtable's (FSR) cybersecurity, fraud, and technology division, BITS, as Vice President of Cybersecurity Risk Management. In this role, Mr. Palmer will manage key aspects of FSR's cybersecurity program including security, authentication, and encryption standards as well as information and technology sharing between the financial sector and government partners.

Mr. Palmer brings a blend of cybersecurity operations and policy experience from roles in both the public and private sector over the span of nearly two decades. He served most recently as Director of International Government Relations for FireEye, and previously led cybersecurity initiatives at the United Nations and Symantec. Mr. Palmer holds a B.A. from Valparaiso University, a J.D. from Duquesne University School of Law, a Certificate in International Management from Pacific-Asian Management Institute, and an M.B.A. from the University of Hawaii.

Scott Petry
Authentic8

Scott Petry is Co-Founder and CEO of Authentic8. Prior to Authentic8, Scott founded Postini and served in a variety of C-level roles until its acquisition by Google in 2007. He served as Director of Product Management at Google until 2009. Prior to Postini, Scott was General Manager and Vice President of Cygnus Solutions (acquired by Redhat), Director of Advanced Messaging Products at SkyTel, and a Product Manager at Apple Computer.

He graduated with a B.S. degree from San Diego State University. Scott was a member of the U.S. National Rowing Team and earned a bronze medal in the world championships. Scott is currently a director of Authentic8, Return Path, Virtru and Scriptrock.

Kristin Sharp
New America Foundation

Kristin Sharp directs New America's Initiative on Work, Workers, and Technology. In 2016, she co-founded and ran Shift: The Commission on Work, Workers, and Technology, a joint project of New America and Bloomberg.

Prior to launching SHIFT, she had an extensive career in technology, innovation, and national security policy in the U.S. Senate, most recently serving as deputy chief of staff to Sen. Mark Warner (D-Va.), and the architect of his initiative examining the impact of the on-demand economy and contingent workforce on capitalism.

In the Senate, Sharp also held positions as legislative director for Sens. Mark Pryor (D-Ark.) and Amy Klobuchar (D-Minn.). In addition, she held a variety of senior staff roles on the Senate Homeland Security and Governmental Affairs Committee and was an advisor to Sen. Richard Lugar (R-Ind.) on the Senate Foreign Relations Committee.

In addition to her work at New America, she is a frequent speaker on the future of work and advises a variety of private start-ups and venture capital firms. Sharp is a member of the board of the Herbert

Scoville Peace Fellowship. She has an M.A. from Duke University in Political Science, and a B.A. from the University of Michigan.

Teresa Shea
In-Q-Tel

Teresa Shea is the Executive Vice President of IQT Technology where she oversees In-Q-Tel's technology practice teams. Ms. Shea joined IQT after her career with the National Security Agency, where she served in numerous key positions including as the director of signals intelligence.

She is the recipient of several honors including the Department of Defense Medal for Distinguished Civilian Service, the National Intelligence Distinguished Service Medal, and two Presidential Distinguished Rank Awards.

Teresa is a graduate of Georgia Institute of Technology (BSEE) and Johns Hopkins University (MSEE).

About Us

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

Website http://cchs.gwu.edu **Email** cchs@email.gwu.edu **Twitter** @gwcchs