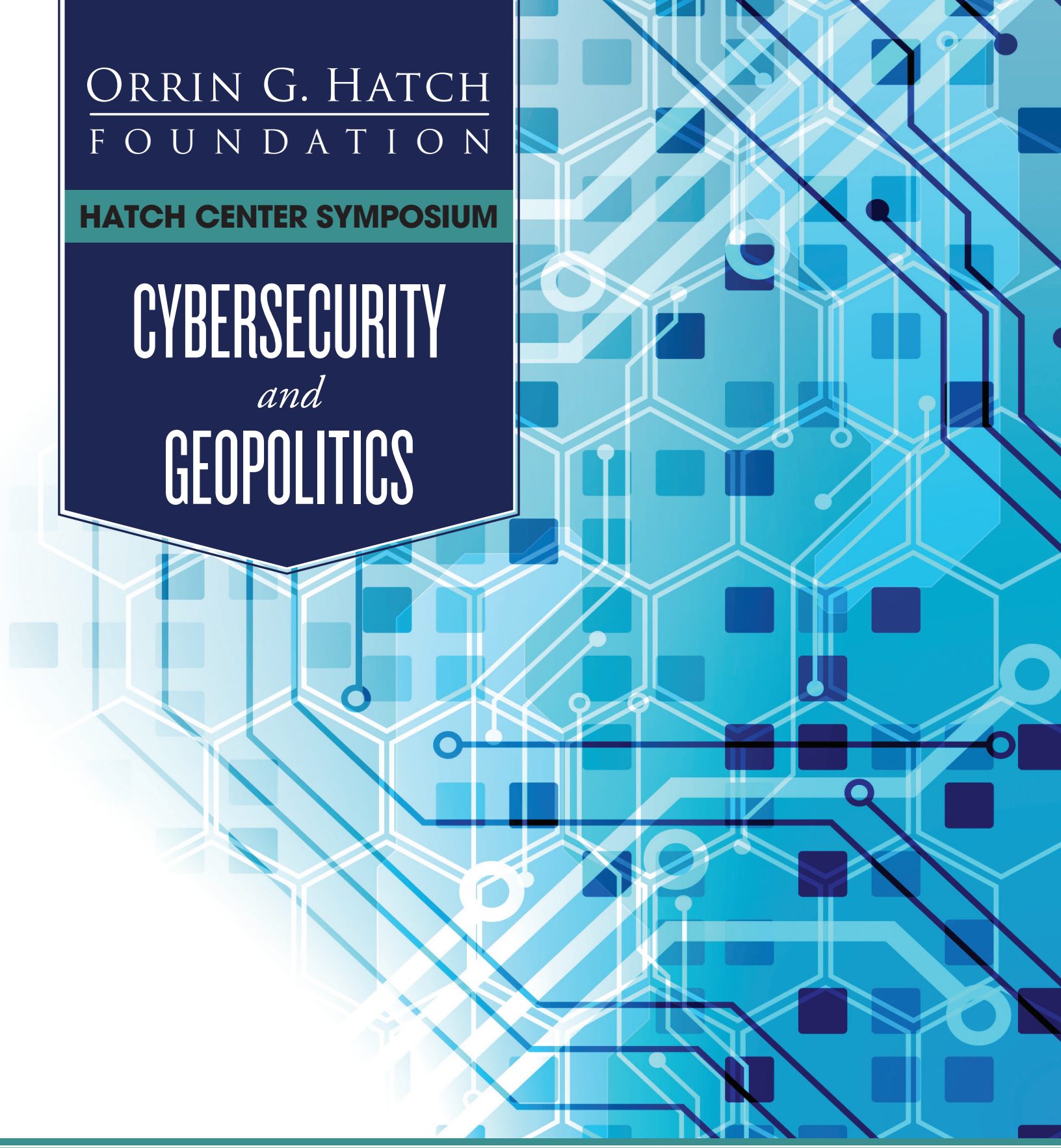
ORRIN G. HATCH
FOUNDATION

HATCH CENTER SYMPOSIUM

CYBERSECURITY *and* GEOPOLITICS



SYMPOSIUM REPORT

October 2019

Introduction

Technology has permeated nearly every corner of our personal and professional lives. As security guru and blogger Bruce Schneier recently observed: "Your modern refrigerator is a computer that keeps things cold. Your oven . . . is a computer that makes things hot. An ATM is a computer with money inside. Your car is . . . a distributed system of over 100 computers with four wheels and an engine. We wear computers: fitness trackers and computer-enabled medical devices . . . . Our homes have smart thermostats, smart appliances, smart door locks, even smart light bulbs. . . . The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in."[1] The ubiquity of technology has grown in a relatively short time. Consider internet usage: In 1995, only 0.4 percent of the world's population used the internet. Ten years later, users had jumped to 10 percent of the world's population. And as of June 2019, nearly 60 percent of the world's population uses the internet.[2]

The private sector is not the only beneficiary of technology, however. Cities, for example, are embedding smart sensors in roads, streetlights, energy grids, and transportation networks.[3] Some cities have shifted to cloud computing models, allowing residents to quickly report urban problems using geo-positioning data.[4] State governments are working to streamline and improve the election process through electronic voting equipment, poll books, management systems, and other hardware.[5] As for our military, computers are everywhere too: defense sensors, aircrafts, unmanned aerial vehicles, and missiles are all integrated computers. And the systems and networks used between the intelligence community and other government entities are all digitally connected as well.[6]

For better or worse, "[o]ur daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace."[7] Unfortunately, we have seen an ever-increasing barrage of cyberattacks that threaten both our public and private sectors.[8] Just in the first half of 2019, there were 3,800 *disclosed* cyber breaches with over 4 billion records exposed.[9] When compared to the first six months of 2018, reported breaches have increased over 54 percent.[10] Among these attacks, the most notable are the 2019 Capital One breach, exposing 106 million customers;[11] the 2014–2018 Marriott International/Starwood breach, exposing nearly 500 million customers;[12] the 2014 eBay breach, exposing 145 million users;[13] the 2017 Equifax breach, exposing

143 million consumers' personal information and 209,000 consumers' credit card data;[14] and the 2013–2014 Yahoo breach, compromising 3 billion user accounts (the largest to date).[15] One University of Maryland study estimated that an internet-connected computer is attacked on average every 39 seconds,[16] and another database estimates that 69 records are stolen every second.[17]

But the private sector is not the only target. As the Comptroller General recently stated before a House subcommittee, the "IT systems supporting federal agencies and our nation's critical infrastructures are inherently at risk" as well.[18] For example, in 2015 hackers accessed a US voter database, exposing over 191 million records. And in 2017, over 35,000 cybersecurity incidents were reported by US federal agencies.[19] More recently, local governments are experiencing an increasing barrage of debilitating ransomware, through which hackers hold data hostage until the demanded ransoms are paid.[20] Just last May, Baltimore's data was held at ransom for tens of thousands of dollars.[21] Ultimately, the city refused to pay, but it estimates repairs to its systems will cost nearly $20 million.[22] Along with private attacks, state-sponsored attacks are also becoming more prevalent.[23]

Responding to this growing threat, the federal government is taking a more deliberate approach to improving US cyber health. In 2018, the Department of Defense issued its Cyber Strategy Report,[24] and the President signed a law establishing the Cybersecurity and Infrastructure Security Agency (CISA) with the national capacity to defend against cyberattacks, provide cybersecurity tools and incident response services, and to bolster our government's cybersecurity.[25] Federal information technology expenditures are also projected to exceed $50 billion in 2021.[26]

As part of this ongoing and critical dialogue to improve both public and private cyber health, the Hatch Center—the policy arm of the Orrin G. Hatch Foundation—hosted its Cybersecurity and Geopolitics Symposium, which convened key players from government, the private sector, and academia to discuss efforts combating these growing concerns. This report provides both a general overview of the most salient challenges facing cybersecurity and a summary of the Hatch Center's recent symposium.

Technology provides massive benefits to our daily lives. Artificial intelligence, cloud computing, and machine learning all could provide us greater computing capability,[27] efficiency,[28] and safety.[29] That said, new technology is not without its challenges: varied attack type, attribution issues, asymmetric cyberwarfare, the weaponization of artificial intelligence, public-private cooperation, and cyber illiteracy all create serious challenges for our overall cyber health.

Attack Type

Cybersecurity can be compromised in an ever-growing number of ways. A "cyberattack" is defined as any type of offensive action that targets computer information systems, infrastructures, computer networks, or personal computer devices.[30] These attacks could include things like overwhelming a network or system to render it inoperable ("Denial-of Service" (DOS) or "Distributed Denial-of-Service" (DDOS)); hijacking communications between a client and a server ("Man-in-the-Middle" (MitM)); sending emails from "trusted" sources that dump malware on a device or scrape personal information when opened ("Phishing"); gaining control over an app, website, or software that then automatically downloads malware when visited or used ("Drive-by" or "Cross-site Scripting" (XXS)); blocking access to data until a ransom is paid ("Ransomware"); or even simply guessing or using algorithms to uncover passwords.[31] Even if a robust security software manages to prevent each of these types of attacks in all their iterations, hackers are constantly creating new, "more sophisticated, harder to detect, and potentially more dangerous" ways of attack.[32] Thus, our overall security will depend on our ability to combat both existing and emerging types of attack.

Attribution

Cyberattacks also come from many sources, which are often obscured. Unlike street crimes or traditional warfare where the actor is known, cybercriminals are usually successful in masking their identity or geographical location.[33] Marshaling enough evidence to convincingly attribute an attack to an individual or group poses its own prosecutorial challenges. But even if an individual or group claims responsibility for the attack, these claims are often met with suspicion.[34] What's more, virtually anyone can launch an attack thanks to the accessibility and economies of scale that the internet and other technologies provide.[35] This means that attacks could be private or state-sponsored, from foreigners or locals, outsiders or insiders. Thus, our overall security also depends on our ability to combat attacks from a variety of malicious actors.

Asymmetric Cyberwarfare

These issues are only compounded when state-actors—such as Russia, China, Iran, or North Korea—use these various attacks to engage in cyberwarfare. In this new era of modern warfare, enemies can attack with traditional military powers, launch a cyberattack, or both—and the blurred lines between state-sponsored and foreign independent hackers only add to the attribution challenge.[36] To complicate matters more, cyberattacks could take the form of propaganda, media manipulation, or other interferences on top of traditional hacking methods.[37]

Even for countries with unsurpassed military prowess like the United States, a cybersecurity weakness could severely threaten national security. As one reporter put it: "Military dominance is undermined if the home-front is woefully vulnerable to a catastrophic attack. While we read headlines about long-range missiles being tested in North Korea or developed in Iran, the fact is that a takedown of a country's energy grid or transportation network or heath service is a far greater risk."[38] As of 2016, the Office of the Director of National Intelligence (DNI) estimated that over 30 sovereign states had developed or were developing offensive cyber-operation programs.[39] This number is only likely to increase as countries which once had no military prowess can easily access and deploy debilitating cyberwarfare strikes against their once-more-powerful enemies. Without increasing our capacity to combat these new methods of cyberwarfare, our cyber-integrated systems will remain key targets.

Weaponization of Artificial Intelligence

Of all these challenges, the weaponization of artificial intelligence (AI) poses one of the greatest threats. Generally, AI opens up a world of new beneficial technology where computers can learn, reason, self-correct, and even complete tasks that once only humans were capable of.[40] At the same time, AI can supercharge malware, hacking at machine rather than human speeds.[41] Whereas hackers once had to personally maintain communication with compromised systems, AI malware could *autonomously* determine how to best infiltrate a system—which would also make it harder to detect.[42]

Recently, IBM Research created an AI-based malware to help programmers understand how to combat similar attacks. The malware would autonomously identify a target through social media indicators, including facial recognition, geolocation, and voice recognition, and avoid detection until it had delivered its payload.[43] Rudimentary AI-based cyberattacks were reported as early as 2017,[44] and they are

John Sherman

Chief Information Officer, Office of Director of National Intelligence

John Sherman was appointed by President Donald J. Trump to serve as the Chief Information Officer (CIO) of the Intelligence Community (IC) and was sworn into this role by the Principal Deputy Director of National Intelligence on September 11, 2017. In this capacity, he is responsible for leading the ongoing modernization efforts with the IC Information Technology Enterprise (IC ITE) and other areas of the overall IC Information Environment, as well as ensuring the security and protection of the IC's IT systems.

Prior to his appointment, Sherman served as the Deputy Director of the CIA's Open Source Enterprise (OSE), where he helped lead the transformation of Open Source Intelligence, leveraging new technologies and interagency partnerships to enhance the growing OSE mission.

He previously served in several senior executive positions at NGA, dealing with analysis, collection, homeland security, organizational strategy, and international affairs. Earlier, he served as the Principal Deputy National Intelligence Officer for Military Issues on the National Intelligence Council, and as a White House Situation Room duty officer. He began his IC career in 1997 as a CIA imagery analyst assigned to the former National Imagery and Mapping Agency, now known as NGA.

Sherman is a 1992 Distinguished Military Graduate of Texas A&M University, where he commanded the Corps of Cadets and received a BA in History, and later earned an MPA from the University of Houston. Following graduation from Texas A&M, he served as a US Army Air Defense officer in the 24th Infantry Division. He is a graduate of the Department of Defense CAPSTONE course, ODNI's "Leading the IC" course, and the CIA Director's Seminar. He has been awarded the Meritorious Presidential Rank, the Intelligence Medal of Merit, NGA's Meritorious Civilian Service Medal, and Canada's Chief of Defense Intelligence Medallion.

He is married with two grown children and enjoys spending time with his family and reading about military history when he is not focusing on his day job of leading IT modernization activities.

expected to become commonplace in the near future.[45]

In the military sphere, AI can reduce operating costs and human casualties by creating autonomous weapon systems with greater speed, persistence, and accuracy.[46] But other countries could also weaponize AI as a supercharged method of asymmetric warfare: at machine speed, a state could directly attack and catastrophically incapacitate its enemy's network systems. Of course, states could also use AI as a powerful defense mechanism, allowing cybersecurity systems to autonomously process vast amounts of data, predict, and even defend against adversarial or abnormal events.[47] That said, hackers have already begun creating tools to manipulate AI and turn it against its user or controller.[48] In this new AI "arms race"[49] of the 21st century, exploiting the benefits and mitigating the risks of AI will prove decisive.

Public and Private Cooperation

Another challenge facing cybersecurity is the cooperation between public and private actors in combating cyberattacks. Private actors are often key targets. They own around 85 percent of our most critical infrastructure (defense, gas, oil, electrical, healthcare, communications, transportation, and financial systems), and these systems rely heavily on digital connectivity.[50]

The government, on the other hand, is better equipped to collect intelligence, collaborate with international actors, and assess critical information about potential threats.[51] And while a traditional military strike poses serious security issues, a cyberattack on these private systems could be just as devastating to our security, economy, or even democracy.[52] But in working together, public-private partnerships can better identify, defend against, and prevent cyberattacks that could otherwise debilitate the country.[53]

Despite the benefit of these partnerships, private actors often hesitate to establish relationships with government.[54] Involving the government could require providing open access to the attacked company's data and ceding autonomy over an investigation into the attack.[55] Moreover, some companies are concerned that the confidential nature of

government information will lead to one-way information sharing.[56] The largest challenge, however, is that in disclosing information about a breach, a company could expose itself to adverse economic effects or even civil liability.[57] For example, after Target reported and accepted responsibility for its cyber breach in 2013, the company saw declines in holiday sales and stock prices, C-level executives were encouraged to step down, and the retail store is expected to spend billions of dollars in litigation and remediation.[58] Without overcoming these trust-related challenges and adverse incentives of disclosure, strengthening the necessary public-private partnerships will prove difficult.

Preparedness and Education

Even if we managed to develop perfect systems with no technical vulnerabilities, cybercriminals could still exploit human vulnerabilities. Cyber criminals often target and exploit employees rather than trying to find loopholes in exhaustive programming.[59] One study reported that 78 percent of security professions believe that the biggest threat to cybersecurity is the negligent practices of individuals.[60] Setting aside malicious employees, cyber illiteracy poses yet another threat to effective cybersecurity.[61] In a recent study, 82 percent of employees reported a shortage of cybersecurity skills with 71 percent believing their talent gap directly and adversely impacted their own organizations.[62]

Critical skills such as intrusion detection, secure software development, and attack migration are all in short supply.[63] Studies estimate that 314,000 cybersecurity positions will remain unfilled in 2019 and upwards of 1.8 million by 2022.[64] No doubt the creation of Chief Information Security Officers (CISOs)[65] and a greater focus on cyber education[66] will help combat this illiteracy, but humans, including non-IT employees, remain the "weakest link in the information security chain."[67] As Jeanette Manfra, assistant director for cybersecurity at DHS, said, "[i]t's a national security risk that we don't have the talent regardless of whether it's in the government or the private sector. We have a massive shortage that is expected [to] grow larger."[68]

Against this backdrop, the Hatch Center, in conjunction with Utah Valley University's Center for National Security Studies, gathered cybersecurity professionals, academics, and key government officials to discuss ways in which we can overcome cybersecurity challenges and ensure that the United States retains its global position in the coming years. John Sherman, the Chief Information Officer (CIO) of the Office of the Director of National Intelligence, provided the keynote address. As CIO, he is tasked with leading the intelligence community's ongoing modernization efforts by ensuring the security and protection of its IT systems. Following Mr. Sherman's remarks, a panel fielded questions related to the challenges discussed above. On the panel, Mr. Sherman was joined by Mr. Ryan Vogel, Director of the Center for National Security Studies at Utah Valley University; Mr. John E. McClurg, Vice President and Ambassador-at-Large of BlackBerry | Cylance; Mr. Matt Berrett, Cofounder of the Center for Anticipatory Intelligence at Utah State University; Mr. Adam Marre, Head of Security Operations at Qualtrics; Mr. Eric Jensen, Professor of Law at the J. Reuben Clark Law School of Brigham Young University; and Mr. Andre Jones, a graduate research student at American University.

John Sherman, CIO, Office of the Director of National Intelligence

Mr. Sherman's call to arms focused on ensuring America's resilience in the digital age. For much of Sherman's career, a mission to defeat communism or terrorist threats defined his focus. But he emphasized that as more battles take place in digital domains, we must adapt and adjust if America is to keep her current position in the global order. Several threats are particularly worrisome to both Sherman and the intelligence community at large: hybrid or asymmetric warfare that changes the tactical strategies of US national security operations and potentially exposes the country to detrimental cyberattacks; digitally enabled propaganda that exploits social media and other internet-based platforms to incite violence or distribute false information; ransomware that immobilizes and disrupts municipalities,

Ryan Vogel

Director, Center for National Security Studies, Utah Valley University

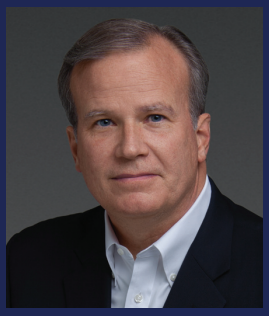
Ryan Vogel is the founding director of the Center for National Security Studies at Utah Valley University. He advises the National Security Society and UVU Journal of National Security Society, directs the NSS program at UVU and teaches a variety of courses on international law and national security subjects.

Before coming to UVU, Vogel served at the Pentagon as a senior policy advisor in the Office of the Secretary of Defense. He began his career at the Pentagon through the Presidential Management Fellowship program and was awarded the Medal for Exceptional Civilian Service in 2014. Vogel has also served at the Public International Law & Policy Group, at the US Senate, and at the State Department. He has taught law and national security courses at American University in Washington, DC, BYU Law School, and the Chicago-Kent College of Law. Vogel holds an LLM in public international law, with a certificate in national security law, from the Georgetown University Law Center. He earned a JD and an MA in international affairs from American University and is an alum of Utah Valley University, where he graduated with a BS in integrated studies.

businesses, and schools; cyber and electronic surveillance that allows different actors to collect and conglomerate data on individuals and organizations; financial, identity, and data theft; and supply chain or insider threats.

To combat these concerns, the Intelligence Community Information Technology Enterprise (IC ITE) was created in 2012. During its first epic, IC ITE focused on modernizing technology use, moving the intelligence community to the cloud and all federal agencies to one common desktop. This one-size-fits-all approach, however, proved less successful than anticipated. As IC ITE moved into its second epic in 2017, it shifted focus: whereas the first epic sought to keep up with modern trends in technology, the second epic increased focus on securing data systems as equally (if not more) important. As part of this effort, IC ITE promulgated a comprehensive cybersecurity plan built around three key principles: (1) know your enterprise; (2) manage your enterprise; and (3) share the state of your enterprise with the rest of the intelligence community. Moreover, based on broad reference architectures or cybersecurity principles, agencies now have latitude to build a cybersecurity plan tailored to their specific needs rather than a uniform cybersecurity approach. Sherman was confident that this increased focus on and flexible approach to cybersecurity would greatly increase America's resilience in the digital age.

He concluded his remarks with a reference to President Kennedy and the Space Race. As a young child, Sherman was inspired by the vigor, courage, and patriotism that undergirded President Kennedy's statement, "We choose to go to the Moon!" And now, several decades later, Mr. Sherman called all to join the great race of our day: "Ensuring American success in the cyber and digital domain is this era's Apollo program. We will have to innovate, engage, and improvise with the same energy that defined the Space Race so many years ago."



John E. McClurg

Vice President and Ambassador-at-Large, BlackBerry | Cylance

John E. McClurg serves as Vice President and Ambassador-At-Large at BlackBerry | Cylance where he engages enterprises around the globe on the risk challenges of today and how BlackBerry | Cylance uniquely mitigates them. McClurg champions a move from a historically reactive security posture to one focused on proactively predicting and mitigating future risks.

Before BlackBerry | Cylance, McClurg served as Dell's CSO, where his responsibilities included the strategic focus and tactical operations of Dell's internal global security service. Before joining Dell, McClurg served as the Vice President of Global Security at Honeywell International; Lucent Technologies/Bell Laboratories; and in the US Intelligence Community, as a twice-decorated member of the Federal Bureau of Investigation (FBI), assisting in the establishment of the FBI's new Computer Investigations and Infrastructure Threat Assessment Center. McClurg also served on assignment as a Deputy Branch Chief with the CIA, helping to establish the new Counterespionage Group. McClurg was voted one of America's 25 most influential security professionals. He also co-chaired the Overseas Security Advisory Council (OSAC) of the US Department of State and served as the founding Chairman of the International Security Foundation.

He currently serves as a Special Advisor to the FBI's Office of the Private Sector and as a Fellow at Utah Valley University's Center for National Security Studies. He holds a JD from Brigham Young University as well as MA in Organizational Behavior and advanced doctoral studies in Philosophical Hermeneutics at UNC-Chapel Hill and UCLA.

Matt Berrett

Cofounder, Center for Anticipatory Intelligence, Utah State University

Matt Berrett joined Space Dynamics Lab in July 2017 as its Director of Analytics after retiring from the Central Intelligence Agency as an Assistant Director. His other senior positions at the CIA included serving as Mission Manager for the Near East, South Asia, and Africa in the Directorate of Science and Technology and as the head of three analytic offices: Iraq; Near East and South Asia; and Middle East and North Africa. He also served under Director of National Intelligence James Clapper as Director of the President's Daily Brief, the premier, multiagency enterprise that informs US presidents and their top national security advisors of key global developments.

Often asked to contribute beyond his formal duties, Mr. Berrett was the CIA presenter in the Agency's 2015 TEDx event. He has provided numerous guest lectures at various US universities and at Oxford and has helped teach courses at CIA University, including one featuring a methodology he created with Jeannie Johnson, an associate professor and strategic culturist at Utah State University. In addition to Mr. Berrett's current duties at Space Dynamics Lab, he and Professor Johnson have established The Center for Anticipatory Intelligence, which brings STEM and social-sciences students together to research, understand, and prepare for the effects of emerging disruptive technologies across the geopolitical, private-sector, and personal realms (cai.usu.edu). The CAI also offers strategic training to public- and private-sector professionals.

Mr. Berrett began his career with the CIA as an economic analyst on Iran after getting an economics degree at the University of Utah and working for a top-50 US bank. He and his wife, Sandi, have four sons.

Panel Summary

Key changes in the cyber landscape

Mr. Berrett pointed to four key changes in the cybersecurity landscape. First, while only a few nation-states were involved previously, the cyber market is now saturated with public and private actors, any one of which could launch debilitating attacks. Second, cybertechnologies facilitate the free-flow of information at even greater efficiencies, which unfortunately provides a platform for even greater dissemination of false information. Third, the targets of attacks have changed dramatically from exclusively public-focused to a mix of public and private entities. And fourth, military strategy has changed to reflect how cyber technology allows actors to engage in asymmetric attacks and level the military playing field.

Mr. Vogel also discussed changes since WWII. After this conflict, we created a world order that served our interests and the international community, but the ubiquity and capacity of cybertechnology largely levels the military playing field. Previously weak nation-states or nonstate actors now can attack in more sophisticated ways. Countries like Russia that pose little traditional military threat still can use cyberwarfare to "saw bit by bit at the world's table legs until they have brought the table down to their level." Of course, we must encourage the peaceful development of other countries, but we must also protect our position at the same time.

In Vogel's perspective, the rise of social media has also had a leveling impact on information warfare. Social media provides a virtually costless network to spread radical and violent messages or to provide means of mobilization. Certainly, government agencies can and do try to intervene in foreign actors' illicit use of social media. But domestically, constitutional limitations pose some challenges to government intervention. At the very least, the intelligence community continues to rely on social media to gather critical information for prevention and response measures.

Greatest cybersecurity concerns in both public and private sectors

For the public sector, Mr. Sherman reiterated the points he made in his keynote address, highlighting the dangers of asymmetric warfare and cyber propaganda. Because this latter concern could have a profoundly detrimental effect on the upcoming 2020 elections, Mr. Sherman took comfort in DHS's special measures to ensure election security and prevent any tampering in the upcoming elections.

For the private sector, Mr. Marre shared some of the same concerns. While companies like Qualtrics are not necessarily concerned with asymmetric warfare, the varied

Adam Marre
Head of Security Operations, QUALTRICS

Adam Marre is currently the Head of Security Operations and Physical Security at Qualtrics SAP where he is responsible for data protection and system security operations in addition to physical security, including executive protection and site security for over 20 offices worldwide. Before coming to Qualtrics, Marre served as a Special Agent of the Federal Bureau of Investigation (FBI) for almost 12 years. Throughout his FBI career, he investigated a wide variety of crimes and national security matters, focusing primarily on criminal computer network intrusions as well as cyber-based national security threats. Marre served as an adjunct professor of the FBI Academy, teaching cyber security investigations globally to hundreds of international investigators. Marre also served as the Senior Team Leader for the FBI SWAT team, commanding teams in the execution over 100 tactical operations and critical incidents. Prior to the FBI, Marre served as a counterintelligence agent and HUMINT collector for the US Army leading teams collecting intelligence, conducting force protection, and counterintelligence operations. Before the Army, Marre was a Video Game Designer at Disney interactive Studios where he led teams of programmers, designers, and artists to deliver platinum-selling video games. Marre holds a BA in Humanities from BYU. He is married and has four children.

methods of attack—like insider threats, denial of service, and ransomware—make it difficult to adequately prepare against and combat any cyberthreats. At Qualtrics specifically, the company focuses on insider threats to combat the enticing financial incentives of compromising company data. But even non-malicious actors can pose security concerns. His experience has shown that many breaches stem from simple human error. Sometimes, employees engage in shadow IT, or potentially compromising activities that cybersecurity personnel do not know about. And often what security officers like Marre fear the most is not what they know, but what they do not know.

But more than shadow IT, it is more common that an individual's lack of basic cyber hygiene leads to a breach. In Marre's opinion, there are three levels of cybersecurity: geopolitical, private, and personal. But by focusing on the individual and improving basic cyber hygiene (e.g., strengthening passwords, training employees against clicking on questionable links, and relying more on multi-factor authentication), our overall cyber health will increase in the other levels as well. Because hackers readily exploit this human element to reach broader systems and networks, we are all virtual border guards and must be on watch—we must all become experts in basic cybersecurity to improve any organization we are in.

Artificial intelligence and cybersecurity

Mr. McClurg discussed how AI could change our cybersecurity focus from reactive to proactive. Much of McClurg's career at the FBI focused on reactively responding to hacking attacks—it was not a question of *if* hacks would occur, but when. In fact, in many ways, the cyber community had almost ceded the battle space and accepted that breaches would occur. Using AI, however, McClurg and others created InfraGard—a system that engages in machine learning to share key information that will help the government and private companies combat cyberthreats proactively.

As the system processes more data, it becomes more able to autonomously defend against a plethora of attacks. In fact, McClurg lamented that with the technology we had in 2015 alone, most of the major hacks in the last few years could have been beaten. When tested against malware, AI was able to combat and stop 99.7 percent of

the attacks. McClurg recognized that malicious actors are trying to leverage or exploit AI as well, so keeping ahead in the AI sphere is critical. That said, InfraGard already has four years of machine learning experience, giving it a sizeable head start.

International law and cybersecurity

Mr. Jensen explained that international law is based on treaties and customs. Unfortunately, there are not yet any treaties addressing cybercrimes, and state custom resembles the Wild West. This means that key legal questions have not been squarely answered. For example, can a country offensively reach into another country's territory to take out a terrorist cell's servers? Developing cyber-focused international laws, either through treaty or custom, will help address these key questions. But until these principles are developed, we are left with analogizing similar, yet more developed, areas of international law to address these concerns.

If countries were to use international law to address cybercrime, cyber threats could be greatly minimized or at least semi-uniformly addressed. One challenge, however, is that many powerful countries do not want to regulate themselves internationally in this space. But even if countries collaborated and established principles governing cyber threats, international law is focused on regulating *state* action—the challenge thus being that nonstate actors, who are often just as dangerous as state actors, would not be regulated. Jensen therefore recommended that international law at least obligate states to accept responsibility for the cyberattacks that originate inside their borders.

Another challenge is that international law does not provide private companies with recourse for the brunt of the cyberattacks that they experience. Congress, however, has pending legislation that if passed, would allow companies to exercise active defense tactics, such as sending a beacon trail or malware back to the initial cyber-aggressor.[69]

Overcoming challenges to public-private cooperation

Mr. Marre discussed the importance of forming strong public-private partnerships. The government clearly has incentives to work with the private sector in combating cyberthreats. With private companies and individuals being on the frontlines of current and future cyberattacks, the private sector provides a crucial view of what is happening on the ground that the government may not have. In a way, private companies can serve as canaries in the cyber coal mines. Private actors can also act as first responders to help prevent the further spread of an attack.

By the same token, private companies also have incentives to collaborate with the public sector: the government has technological resources and intelligence that most companies do not have. Mr. McClurg agreed

Eric Jensen

Professor of Law, J. Reuben Clark Law School, BRIGHAM YOUNG UNIVERSITY

Eric Talbot Jensen is a professor of law at Brigham Young University in Provo, Utah, and recently returned to BYU after serving for a year as the Special Counsel to the Department of Defense General Counsel. Prior to joining the BYU Law faculty in 2011, Jensen spent two years teaching at Fordham Law School in New York City and twenty years in the United States Army as both a Cavalry Officer and as a Judge Advocate. During his time as a Judge Advocate, Jensen served in various positions including as the Chief of the Army's International Law Branch; Deputy Legal Advisor for Task Force Baghdad; Professor of International and Operational Law at The Judge Advocate General's Legal Center and School; legal advisor to the US contingent of UN Forces deployed to Skopje, Macedonia as part of UNPREDEP; and legal advisor in Bosnia in support of Operation Joint Endeavor/Guard.

Jensen is a graduate of Brigham Young University (BA, International Relations), University of Notre Dame Law School (JD), The Judge Advocate General's Legal Center and School (LLM) and Yale Law School (LLM). He is an expert in the law of armed conflict, public international law, national security law, and cyber warfare. He was one of a group of global experts who prepared the *Tallinn Manual on the International Law Applicable to Cyber Operations*. He is co-author on *The Law of Armed Conflict: An Operational Perspective, The Laws of War and the War on Terror*, and *National Security Law and Policy: A Student Treatise*. He has also authored more than thirty law journal publications focusing on international law, the law of armed conflict, national security law, cyber law, and international criminal law.

Andre Jones
Graduate Research Student, American University

Andre Jones is a graduate student at American University's School of International Service studying international affairs and cyber policy in Washington DC, and is currently working at the Department of Homeland Security. As an alumnus of the Center for National Security Studies at Utah Valley University, Andre founded his own academic undergraduate journal as its first editor-in-chief, interned at the US Senate in Washington DC, and served as both a Presidential Intern and Foundation Ambassador.

Since graduating with his BA, Andre has competed in cyber competitions such as the national Cyber 9/12 Challenge at Lockheed Martin's Global Vision Center, where his team placed 4th out of 36 teams by briefing cyber policy experts on threats against the US Census. In addition to working at DHS, Andre is a Graduate Research Associate at American University's Business School, working on cybersecurity industry analytics. In his spare time, Andre enjoys listening to cyber podcasts and going on hikes in Northern Virginia with his wife.

that several times during his work in the private sector, his resources could not discern a cyberthreat. But after teaming up with the government, he was able to discern and combat these threats.

For Marre, getting the government and private industries into the same room is critical to effectively addressing current and future cyber concerns. In Marre's experience as an FBI agent, however, most private companies or individuals had no desire to disclose potential liability—especially to the government. Moreover, any disclosures often came so far after the breach itself that the information's value in preventing further attacks had waned. Currently, there are some programs that facilitate this information sharing (e.g., Information Sharing and Analysis Centers (ISACs)[70]), but Marre considered these insufficiently broad to accomplish the level of coordination needed. Instead, a broader program that both offers some level of amnesty and facilitates information sharing contemporaneously with the attacks themselves has the potential to strengthen our country's overall cyber defenses. And as McClurg added, without trust, any collaboration efforts will see little success.

Several panelists also addressed the challenge with classified information and the often unidirectional flow of information in these partnerships. Currently, there is "below-the-tear-line" intelligence that the government can provide to private companies that distills the most important information without compromising any classified sources. This means that classified information may not impede public-private partnerships as severely because, as Mr. Sherman pointed out, most companies do not need to know the information's source (which is what often causes classification issues). Instead, companies usually just need to know what is happening and how to overcome it—information not limited by classification. That said, Sherman has been working within the intelligence community and DHS to revisit classification rules and more easily provide necessary information to the private sector.

Role of universities and education in combating cyber threats

Several panelists echoed Mr. Sherman's call to arms, focusing especially on universities and educational approaches to combating cyber threats. Mr. Vogel identified two key roles universities can play in combating cyber threats: First, they can host discussions, like this Symposium, on how to improve our cyber health.

Second, universities can prepare the next generation of cybersecurity professionals to address current and future threats. Supporting these points, Mr. Jones shared his own experience graduating from Utah Valley University in national security studies and continuing at the American University's School of International Service studying international affairs and cyber policy. Jones also took advantage of several cyber competitions to augment his education, one of which led to his current position at DHS. Universities play an integral part in shaping the future lawyers, policymakers, technical and nontechnical experts, and ethicists across the public and private sectors that we will need going forward.

Tapping into the vast benefits of technology will only improve our lives. But unless we simultaneously improve our defenses, technology can also do significant harm. We could return to localized data storage and move away from our digitally connected world, but as Mr. Sherman noted during the symposium, locking everything down would inhibit our ability to innovate, interact, grow, and make a better tomorrow. Instead, we can enjoy both the benefits of technology and minimize security threats by improving our nation's cyber health.

As we improve our cybersecurity, we must be wary of too narrowly focusing our efforts. We must, of course, focus on the most obvious areas of concern like developing our technological defenses to protect both the private and public sectors. As Mr. McClurg discussed during the symposium, AI may be the answer to combating the ever-increasing types and sources of cyber threats. But if we only focus on these technological improvements, human cyber illiteracy may still compromise even our most robust security systems. Instead, basic cyber hygiene is something that every American should learn as soon as possible. Installing antivirus and malware software, using network firewalls, updating software regularly, setting strong passwords, using multi-factor authentication, employing device encryption, backing up data regularly, and securing our networks are simple steps we can take to improve cyber health.[71] And learning to identify phishing emails will dramatically help as well.[72]

Moving past individual efforts, companies and organizations can improve their cybersecurity training, which includes random simulations and frequent training tailored to meet the organization's needs.[73] And if breaches do occur, organizations may consider hacker insurance like the city of Baltimore did after its recent ransomware attack.[74] When it comes to public-private partnerships, legislation or regulation incentivizing (or at least not disincentivizing) timely information sharing is key. Perhaps the tack that states and national governments are taking by implementing comprehensive privacy and cybersecurity laws is the answer.[75] But as Mr. Marre suggested, our success in this endeavor will only happen when private and public actors are brought together in the same room to work towards mutual goals.

As Apple CEO Tim Cook said, "[w]e see vividly—painfully—how technology can harm rather than help. . . . Rogue actors and even governments have taken advantage of user trust to deepen divisions, incite violence and even undermine our shared sense of what is true and what is false. The crisis is real. . . . And those of us who believe in technology's potential for good must not shrink from this moment. Now, more than ever—as leaders of governments, as decision-makers in business, and as citizens—we must ask ourselves a fundamental question: What kind of world do we want to live in?"[76] While the Space Race was crucial to the 20th Century, Cook's remarks remind us just how critical the cyber race is to the 21st Century. Success will require both overcoming technological and procedural weaknesses by harnessing emerging technologies and overcoming barriers between public and private actors. At a more fundamental level, success will also depend on the cyber hygiene of everyday technology users. Only through this comprehensive approach can we maintain our country's place in the global order and ensure the security of the everyday American.

Endnotes

1 Bruce Schneier, We have Root: Even More Advice from Schneier on Security 54 (2019). Sayta Nadella, CEO of Microsoft, also said: "Digital technology, pervasively, is getting embedded in every place: every thing, every person, every walk of life is being fundamentally shaped by digital technology—it is happening in our homes, our work, our places of entertainment. It's amazing to think of a world as a computer. I think that's the right metaphor for us as we go forward." *48 Eye-opening Quotes about Tomorrow's Technology: Cloud Computing, AI, and IoT*, Enlightened-Digital.com (Jul. 27, 2018), https://enlightened-digital.com/48-eye-opening-quotes-about-tomorrows-technology-cloud-computing-ai-and-iot/ [hereinafter *48 Eye-opening Quotes*].

2 *Internet Growth Statistics*, InternetWorldStats.com, https://www.internetworldstats.com/emarketing.htm (last updated Nov. 11, 2019).

3 Schneier, *supra* note 1; *see e.g.*, John R. Quain, *Most Cities can't Deal with E-Scooters. Charlotte, N.C., Wants to Show them How*, DigitalTrends.com (May 4, 2019 1:00AM), https://www.digitaltrends.com/cool-tech/charlotte-nc-escooters-passport-lime-bird-skip/; Natalie Staines, *Smarter Cities: Using Technology to Improve City Living*, R2IIntegrated.com, https://www.r2integrated.com/r2insights/smarter-cities-using-technology-to-improve-city-living (last visited Nov. 11, 2019); Jonathan Woetzel et al., *Smart Cities: Digital Solutions for a More Livable Future*, McKinsey & Co. (Jun. 2018), https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/smart-cities-digital-solutions-for-a-more-livable-future.

4 Quartet Service Inc., *3 Cities that use Cloud Computing in a Big Way*, QuartetService.com (Aug. 4, 2019), https://www.quartetservice.com/3-cities-that-use-cloud-computing-in-a-big-way/.

5 *See generally* National College of State Legislatures, *Election Technology Overview*, NSCL.org (Aug. 27, 2018), http://www.ncsl.org/research/elections-and-campaigns/election-technology-overview.aspx.

6 Williamson Murray, *Technology and the Future of War*, Hoover Institution (Nov. 14, 2017), https://www.hoover.org/research/technology-and-future-war.

7 Dep't of Homeland Security, *Cybersecurity*, DHS.gov, https://www.dhs.gov/topic/cybersecurity (last visited Nov. 11, 2019).

8 From 2017 to 2018, there was a 126% increase in the number of personal records stolen. Devon Milkovich, *15 Alarming Cyber Security Facts and* Stats, CybintSolutions.com (Sept. 23, 2019), https://www.cybintsolutions.com/cyber-security-facts-stats/.

9 Dan Rafter, *2019 Data Breaches: 4 Billion Records Breached So Far*, Norton.com, https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html (last visited Nov. 13, 2019).

10 *Id.*

11 *Id.*

12 Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSOOnline.com (Dec. 20, 2018 5:01AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

13 *Id.*

14 *Id.*

15 *Id.*

16 Milkovich, *supra* note 8 (citing A. James Clark School of Engineering, University of Maryland, *Study: Hackers Attack Every 39 Seconds*, UMD.edu (Feb. 9, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds).

17 *Data Breach Statistics: Data Records Lost or Stolen Since 2013*, BreachLevelIndex.com, https://breachlevelindex.com/#!breach-database (last visited Nov. 13, 2019 10:00AM).

18 *Urgent Actions are Needed to Address Cybersecurity Challenges Facing the Nation: Before the H. Subcomm. on Gov't Operations & Info. Tech.*, 115th Cong. 4 (2018) (statement of Gene L. Dodaro, Comptroller General, U.S. Gov't Accounting Office), https://www.gao.gov/assets/700/693405.pdf; *see also* Heritage Foundation, *The Growing Threat of Cyberattacks*, Heritage.org, https://www.heritage.org/cybersecurity/heritage-explains/the-growing-threat-cyberattacks (last visited Nov. 13, 2019).

19 J. Clement, *U.S. Government and Cyber Crime—Statistics & Facts*, Statista.com (Aug. 1, 2019), https://www.statista.com/topics/3387/us-government-and-cyber-crime/.

20 Manny Fernandez, David E. Sanger & Marina Trahan Martinez, *Ransomware Attacks are Testing Resolve of Cities Across America*, N.Y. Times (Aug. 23, 2019) ("More than 40 municipalities have been the victims of cyberattacks this year, from major cities such as Baltimore, Albany and Laredo . . . .").

21 Niraj Chokshi, *Baltimore Hostage: How they Struck and What's Next*, N.Y. Times (May 22, 2019), https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html.

22 Luke Broadwater, *Baltimore Transfers $6 Million to Pay for Ransomware Attack; City Considers Insurance Against Hacks*, Baltimore Sun (Aug. 28, 2019), https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html.

23 Check Point Research, Cyber Attack Trends Analysis 16–17 (2019) (accessible at http://snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf); *see also, e.g.*, Tami Abdollah, *Iran Increases Cyber Attacks on U.S. Gov't, Infrastructure*, InsuranceJournal.com (Jun. 24, 2019), https://www.insurancejournal.com/news/national/2019/06/24/530257.htm; Phillip Bump, *Timeline: How Russian Agents Allegedly Hacked the DNC and Clinton's Campaign*, Wash. Post (Jul. 13, 2018 12:49PM), https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons-campaign/. For a detailed list of global attacks, including attacks on other governments, see generally Center for Strategic & Int'l Studies, *Significant Cyber Incidents*, CSIS.org, https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf (last updated Sept. 2019).

24 U.S. Dep't of Defense, Summary: Cyber Strategy (2018) (accessible at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).

25 Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (2018) (codified in scattered sections of 6 U.S.C.); *see also* CISA Homepage, https://www.cisa.gov/ (last visited Nov. 13, 2019).

26 Clement, *supra* note 19.

27 *E.g.*, Joy Tan, *Cloud Computing is Crucial to the Future of Our Societies—Here's Why*, Forbes (Feb. 25, 2018 9:00PM), https://www.forbes.com/sites/joytan/2018/02/25/cloud-computing-is-the-foundation-of-tomorrows-intelligent-world/#3d0e482a4073; Khalid Durrani, *Cloud Computing: What the Future Holds and How You Can Prepare Your Organization*, Business2Community.com (Jun. 27, 2019), https://www.business2community.com/cloud-computing/cloud-computing-what-the-future-holds-and-how-you-can-prepare-your-organization-02214334.

28 Rajeev Suri, CEO of Nokia, is quoted as saying: "Imagine if we can get information from sensors, compute it in the cloud, and find and plug water leakages—leakage wastes 20 percent of the water in the world." *48 Eye-opening Quotes*, *supra* note 1; *see also* Forbes Technology Council, *10 Effective Ways to Increase Productivity Using Technology*, Forbes (May 16, 2017 8:00AM), https://www.forbes.com/sites/forbestechcouncil/2017/05/16/10-effective-ways-to-increase-productivity-using-technology/#1384304a680f.

29 *See, e.g.*, Kevin Schultz, *3 Safety Benefits of Having Smart Technology in Your Home*, Themocracy.com (Sep. 7, 2016), http://themocracy.com/3-safety-benefits-of-having-smart-technology-in-your-home/; Christine Queally Foisey, *4 Ways Technology is Improving Patient Safety*, Health IT Outcomes (Mar. 1, 2017), https://www.healthitoutcomes.com/doc/ways-technology-improving-patient-safety-0001; *see generally* Heather L. Schwartz et al., *Using Innovative Technology to Enhance School Safety in Practice*, *in* The Role of Technology in Improving K–12 School Safety 35–54 (2016) (accessible at https://www.jstor.org/stable/10.7249/j.ctt1btc150.11).

30 Jeff Melnick, *Top 10 Most Common Types of Cyber Attacks*, Netwrix Blog (May 15, 2018), https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.

31 *Id.*

32 Ciara Byrne, *The New Ways We Could Get Hacked (and Defended) in 2019*, Fast Company (Jan. 7, 2019), https://www.fastcompany.com/90287253/cybersecurity-cybercrime-threats-defenses-2019.

33 *How Do Cybercriminals Get Caught?*, Norton.com, https://us.norton.com/internetsecurity-emerging-threats-how-do-cybercriminals-get-caught.html (last visited Nov. 13, 2019); Larry Greenemeier, *Seeking Address: Why Cyber Attacks are so Difficult to Trace Back to Hackers*, Scientific American (Jun. 11, 2011), https://www.scientificamerican.com/article/tracking-cyber-hackers/; *The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks*, Symantec.com (Oct. 3, 2018), https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks.

34 John S. Davis II et al., Stateless Attribution: Toward International Accountability in Cyberspace 16–18 (2017) (accessible at https://www.rand.org/pubs/research_reports/RR2081.html).

35 *Id.* at 9 ("Cyber attacks may operate on spatial scales ranging from local targets in close physical proximity with an attacker's hardware to global targets

connected by telecommunications technology over great distances. As a result, an attacker, who could be literally anyone in the world, can route attacks through compromised innocent third parties and obfuscate their origin.").

36 Zak Doffman, *State-sponsored Cyberattacks 'Challenge the Very Concept of War'*, FORBES (Aug. 10, 2019 2:27AM), https://www.forbes.com/sites/zakdoffman/2019/08/10/state-sponsored-cyberattacks-challenge-the-very-concept-of-war-report/#795998c54d6c. ("As we have seen in the Middle East with escalating tensions between the U.S. (and allies) and Iran (and Russia and China), non-attributable cyberattacks are themselves an opportunity for aggressor states to suggest nefarious 'false flag' activity on the parts of the 'good guys.' Put simply, misdirecting attention.").

37 *Id.*

38 *Id.*

39 *Foreign Cyber Threats to the United States: Before S. Comm. on Armed Services*, 114th Cong. 5 (2017) (joint statement by James R. Clapper, Director of National Intelligence; Marcel Lattre, Undersecretary of Defense for Intelligence; Michael S. Rogers, USN Commander, U.S. Cyber Command Director, National Security Agency) (accessible at https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf).

40 Chethan Kumar, *Artificial Intelligence: Definition, Types, Examples, Technologies*, MEDIUM.COM (Aug. 31, 2018), https://medium.com/@chethankumargn/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b.

41 Bryne, *supra* note 32.

42 *Id.*

43 Joe Burton & Simona R. Soare, *Understanding the Strategic Implications of the Weaponization of Artificial Intelligence*, NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE 10 (2019), https://ccdcoe.org/uploads/2019/06/Art_14_Understanding-the-Strategic-Implications.pdf.

44 Steve Norton, *Era of AI-Powered Cyberattacks Has Started*, WALL ST. J. (Nov. 15, 2017 11:38AM), https://blogs.wsj.com/cio/2017/11/15/artificial-intelligence-transforms-hacker-arsenal/.

45 Ryan Goosen et al., *Artificial Intelligence is a Threat to Cybersecurity. It's also a Solution*, BOSTON CONSULTING GROUP 1 (Nov. 2018), http://image-src.bcg.com/Images/BCG-Artificial-Intelligence-Is-a-Threat-to-Cyber-Security-Its-Also-a-Solution-Nov-2018_tcm27-207468.pdf.

46 Jayshree Pandya, *The Weaponization of Artificial Intelligence*, FORBES (Jan. 14, 2019 12:51AM), https://www.forbes.com/sites/cognitiveworld/2019/01/14/the-weaponization-of-artificial-intelligence/#51042b8c3686.

47 Joe Burton & Simona R. Soare, *Understanding the Strategic Implications of the Weaponization of Artificial Intelligence*, NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE 9 (CCDCOE) (2019), https://ccdcoe.org/uploads/2019/06/Art_14_Understanding-the-Strategic-Implications.pdf.

48 *Id.* at 10.

49 Byrne, *supra* note 32.

50 Chuck Brooks, *Public Private Partnerships and the Cybersecurity Challenge of Protecting Critical Infrastructure*, FORBES (May 6, 2019 1:24AM), https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#489bc3955a57.

51 *A Look into Public Private Partnerships for Cybersecurity*, WHARTON PUB. POL'Y INITIATIVE (Apr. 18, 2017), https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for [hereinafter WHARTON].

52 *See* Doffman, *supra* note 36 (noting how detrimental a cyberattack can be on infrastructure). Dan Coats, Director of National Intelligence has been quoted as saying: "[T]he threat was growing for a devastating cyber assault on critical U.S. infrastructure," and that "the 'warning lights are blinking red again' nearly two decades after the Sept. 11, 2001, attacks." Brooks, *supra* note 50.

53 WHARTON, *supra* note 51.

54 *Id.*

55 *Id.*

56 Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration*, CENTER ON L. & SEC., NYU 3 (2014), http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf.

57 *See id.* at 4; WHARTON, *supra* note 51. Most states currently have statutes mandating disclosure if the breach passes a certain threshold. *E.g.*, CAL. CIV. CODE § 1798.82(a) (2003); *see generally* National Conference of State Legislatures, *State Security Breach Notification Laws*, NCSL.ORG http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Nov. 14, 2019); Paul Schwartz & Edward Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 924–25 (2007). These laws, however, are not uniform in what triggers a duty to notify. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 172–74 (2013) (providing a chart examining the differences between these laws state-by-state). The most important takeaway is that not all disclosures are required, though total disclosure could help better combat cybersecurity with a wider array of data.

58 Germano, *supra* note 56, at 4.

59 Kratikal Tech Pvt Ltd., *Humans are the Weakest Link in the Information Security Chain*, MEDIUM.COM (Feb. 11, 2018), https://medium.com/@kratikal/humans-are-the-weakest-links-in-cyber-security-of-any-organisation-ac04c6e6e71.

60 *Id.*

61 Marisa Viveros, *Cyber Security Depends on Education*, HARV. BUS. REV. (Jun. 24, 2013), https://hbr.org/2013/06/cyber-security-depends-on-educ (noting a concern that the "heavy demand from employers for people capable of fighting off today's wave of cyber attacks is pulling talent out of the ranks of professionals who would otherwise be educating the next generation, and doing the critical research to advance the state of the art.").

62 CENTER FOR STRATEGIC & INT'L STUDIES, HACKING SKILLS SHORTAGE 4–5 (2016), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.

63 *Id.* at 4.

64 Center for Strategic & Int'l Studies, *The Cybersecurity Workforce Gap*, CSIS.ORG (Jan. 29, 2019), https://www.csis.org/analysis/cybersecurity-workforce-gap.

65 *See generally* Justin Dolly, *The Rise of the CISO*, CISO REVIEW, https://security.cioreview.com/cioviewpoint/the-rise-of-the-ciso-nid-23914-cid-21.html (last visited Nov. 14, 2019).

66 *See, e.g.*, Jessica L. Beyer & Sara R. Curran, *Cybersecurity Workforce Preparedness: The Need for More Policy-Focused Education*, WILSON CENTER, UNIV. OF WASH. (2017), https://www.wilsoncenter.org/sites/default/files/cybersecurity_workforce_preparedness.pdf (describing University of Washington's plans for increasing cyber literacy).

67 *See* Kratiakal, *supra* note 59.

68 Jonathan Shieber, *The Lack of Cybersecurity Talent is 'a National Security Threat,' says DHS Official*, TECHCRUNCH.COM (Oct. 3, 2019 5:02PM), https://techcrunch.com/2019/10/03/lack-cybersecurity-professionals-threat-dhs/.

69 *See generally* Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019).

70 For more information on ISACs, see generally NAT'L COUNCIL OF ISACS, https://www.nationalisacs.org/ (last visited Nov. 16, 2019).

71 Alison Grace Johnson, *Good Cyber Hygiene Habits to Help Stay Safe Online*, NORTON.COM, https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html (last visited Nov. 21, 2019).

72 *See generally How to Recognize and Avoid Phishing Scams*, FEDERAL TRADE COMMISSION, https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (last visited Nov. 21, 2019).

73 *See, e.g.*, *7 Research-Backed Tips to Improve Your Security Awareness Training*, INFOSEC INSTITUTE (Dec. 7, 2018), https://www.infosecinstitute.com/blog/7-research-backed-tips-to-improve-your-security-awareness-training/.

74 Broadwater, *supra* note 22.

75 For example, the European Union recently enacted the General Data Protection Regulation (GDPR) that enhances privacy practices to better protect against breaches. *See generally What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited Nov. 21, 2019). Some states like California, Nevada, and Maine have enacted or are attempting to enact comprehensive privacy laws similar to GDPR. *See, e.g.*, Cynthia Brumfield, *11 New State Privacy and Security Laws Explained*, CSO ONLINE (Aug. 8, 2019 3:00AM), https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html. Note also that several federal legislators are more seriously considering a federal comprehensive privacy law, but no clear steps have been taken in this direction yet. *See* David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It is No Where in Sight*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html.

76 Sara Salinas & Sam Meredith, *Tim Cook: Personal Data Collection is Being 'Weaponized Against Us with Military Efficiency'*, CNBC.COM (Oct. 24, 2018 6:22AM), https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html (quoting Tim Cook during his address at a 2018 privacy conference in Brussels).

(385) 355-4380 | info@orrinhatchfoundation.org

SLC, UT Office | 411 E. South Temple, Salt Lake City, Utah 84111

Washington, DC Office | 1440 G Street NW, Washington, DC 20005

@senatororrinhatch @orrinhatch @orrinhatchcenter

www.orrinhatchfoundation.org