PREPARING FOR THE FUTURE: AN ASSESSMENT OF EMERGING CYBER THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

OCTOBER 22, 2019

Serial No. 116–44

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

40–460 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

CEDRIC L. RICHMOND, Louisiana, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KATHLEEN M. RICE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
BENNIE G. THOMPSON, Mississippi *(ex officio)*

JOHN KATKO, New York, *Ranking Member*
MARK WALKER, North Carolina
VAN TAYLOR, Texas
JOHN JOYCE, Pennsylvania
MIKE ROGERS, Alabama *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
SARAH MOXLEY, *Minority Subcommittee Staff Director*

CONTENTS

PREPARING FOR THE FUTURE: AN ASSESSMENT OF EMERGING CYBER THREATS

Tuesday, October 22, 2019

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:11 p.m., in room 310, Cannon House Office Building, Hon. Cedric L. Richmond [Chairman of the subcommittee] presiding.

Present: Representatives Richmond, Jackson Lee, Langevin, Rice, Slotkin, Thompson; Katko, Walker, and Taylor.

Also present: Representative Joyce.

Mr. RICHMOND. The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation will come to order.

The subcommittee is meeting today to receive testimony on preparing for the future, an assessment of emerging cyber threats.

Mr. KATKO. Mr. Chairman, I ask unanimous consent that our colleague from Pennsylvania, Mr. Joyce, be able to fully participate in today's hearing.

Mr. RICHMOND. Hearing no objection, so ordered.

Good afternoon. I want to welcome the witnesses to today's hearing on how we seek to balance the benefits of technical innovation with the security vulnerabilities that it may bring.

The rapid proliferation of new technology is changing the world. Advancements in artificial intelligence, AI, and quantum computing will equip us with new tools to defend ourselves and break down barriers to new research that could improve the way we live and save lives.

Unfortunately, one man's tool is another man's weapon. Sophisticated nation-state actors like Russia, China, Iran, and North Korea have already weaponized new technologies to disrupt our democracy, compromise our National security, and undermine our economy. As technology improves, so will their ability to use it against us.

I am particularly concerned about the impact of new technologies on our elections. In the lead-up to the 2016 Presidential election, Russia mounted an unprecedented influence and disinformation campaign. They use bots to automatically tweet divisive messages from fake accounts. As we move into the heart of the 2020 election cycle, we must be prepared for our adversaries to use AI-generated

deepfakes to create a false history, sow discord, and inject skepticism into our National elections.

To start, on-line platforms must learn to identify deepfakes and publish policies about how they will handle them. At the same time, we need to educate the public to ensure that they are informed consumers of information.

More broadly, ensuring that emerging technologies are developed and deployed responsibly requires U.S. leadership, and I am concerned that we are not demonstrating that now. For years the Federal Government has cut research and development dollars to meet budget caps, and I am worried that countries like China are outpacing our investment. Our failure to put money into R&D may cost us not only our strategic advantage as the world's leader in technology, but the global influence that stems from it.

What is most alarming, however, is the lack of attention that this administration is giving to this important National security issue. Despite the fact that our intelligence agencies have confirmed that nation-state actors are utilizing their emerging technology for their strategic advantage, the administration annually slashes R&D funding under the false premise that the private sector will make up the difference. Maintaining U.S. leadership in this space will require direction, coordination, and money from the Federal Government.

Before I close, I want to address a final issue that is causing concern in my district and others like it: How AI and automation will affect the work force. Automation has already decreased availability of jobs in the labor market, and I worry about the National and economic security consequences that could result if we do not adequately plan for this transition. I look forward to our witnesses' thoughts on this important issue today.

The success of our Nation and economic security rests on whether the Federal Government can effectively partner with its allies, State and local partners, and the private sector to develop policies that both incentivize investment in emerging technology, and manage the risk associated with it when it falls into the hands of our adversaries.

I look forward to understanding how this committee can assist in the development of safe, secure, and responsible technologies.

[The statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC RICHMOND

OCTOBER 22, 2019

The rapid proliferation of new technology is changing the world. Advancements in artificial intelligence (AI) and quantum computing will equip us with new tools to defend ourselves and break down barriers to new research that could improve the way we live and save lives. Unfortunately, one man's tool is another man's weapon. Sophisticated nation-state actors like Russia, China, Iran, and North Korea have already weaponized new technologies to disrupt our democracy, compromise our National security, and undermine our economy. As technology improves, so will their ability to use it against us.

I am particularly concerned about the impact of new technologies on our elections. In the lead-up to the 2016 Presidential election, Russia mounted an unprecedented influence and disinformation campaign that used bots to automatically tweet divisive messages from fake accounts. As we move into the heart of the 2020 election cycle, we must be prepared for our adversaries to use AI-generated "deepfakes" to create a false history, sow discord, and inject skepticism into our National elections.

To start, on-line platforms must learn to identify "deepfakes" and publish policies about how they will handle them. At the same time, we need to educate the public to ensure that they are informed consumers of information. More broadly, ensuring that emerging technologies are developed and deployed responsibly requires U.S. leadership, and I am concerned that we are not demonstrating that now.

For years, the Federal Government has cut research and development dollars to meet budget caps, and I am worried that countries like China are outpacing our investment. Our failure to put money into R&D may cost us not only our strategic advantage as the world's leader in technology development, but the global influence that stems from it. What is most alarming, however, is the lack of attention that this administration is giving to this important National security issue. Despite the fact that our intelligence agencies have confirmed that nation-state actors are utilizing the emerging technology for their strategic advantage, the administration annually slashes R&D funding under the false promise that the private sector will make up the difference. Maintaining U.S. leadership in this space will require direction, coordination, and money from the Federal Government. Before I close, I want to address a final issue that is causing concern in my district and others like it: How AI and automation will affect the workforce. Automation has already decreased the availability of jobs in the labor market, and I worry about the National and economic security consequences that could result if we do not adequately plan for this transition. I look forward to our witness' thoughts on this important issue today.

The success of our National and economic security rests on whether the Federal Government can effectively partner with its allies, State and local partners, and the private sector to develop policies that both incentivize investment in emerging technology and manage the risks associated with it when it falls into the hands of our adversaries. I look forward to understanding how this committee can assist in the development of safe, secure, and responsible technologies.

Mr. RICHMOND. I will now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Katko, for an opening statement.

Mr. KATKO. Thank you, Mr. Chairman, and thank you for having me here today, and thank you for the witnesses. I appreciate you coming today.

During my time as a Federal prosecutor over 2 decades I saw first-hand how criminals evolved and adapted to changes. As I have learned about the cyber landscape as Ranking Member of this subcommittee, I have been amazed at the number and diversity of the cyber threats we face today. These threats are always evolving and adapting to new obstacles, new protections, new tactics, and new technologies.

All levels of government, Federal, State and local, as well as our allies around the globe, the private sector, academia, and nonprofits must work together in order to protect against emerging cyber threats.

Today's technologies have a number of vulnerabilities that must be protected from bad actors. In the first 6 months of this year more than 4 million records have been exposed due to data breaches. Ransomware attacks have doubled in 2019 in my district. Syracuse School District, for example, and the Onondaga County Library System both suffered ransomware attacks from unknown threat actors in the last month.

More citizens than ever are falling victim to phishing attacks and malware. Cyber crime made up 61 percent of the attacks that cybersecurity firm CrowdStrike saw between January and June of this year. These are just the attacks and statistics that we are aware of. Many experts believe incidents to be vastly under-reported.

These threats are persistent, complex, and on the rise. Cybersecurity must constantly evolve in order to provide protection. As evi-

denced by the number of incidents this year alone, this is a difficult endeavor that cannot be done without help. As I heard from my constituents in my district, companies and local government entities need assistance and guidance to identify, protect against, and recover from certain current cyber threats.

These are just the threats we see with our current technology. Our cyber landscape is becoming increasingly sophisticated, and new innovations are being introduced every day. These advances have put cybersecurity out of reach for even more small, medium, and large businesses, as well as State and local governments who simply cannot afford it.

It is estimated that 22 million internet of things devices will be on-line by 2025. 5G deployment is just around the corner. Artificial intelligence and machine learning, while making impacts today, are projected to have even more of an enormous effect on our lives in the years ahead. Quantum computing, which is a huge concern, is on the horizon. These emerging technologies will undoubtedly present new and evolving cyber threats. While we are staying vigilant and working to protect against current hazards, we must also be preparing for our future ones.

Our first step is to better understand these new threats, and this hearing is a very good start.

I am also working to educate my colleagues on the challenges and opportunities of the internet of things. I am the co-chair of the Internet of Things Caucus, and have spent time learning from Syracuse University about the quantum research they are working on in partnership with the Air Force Research Lab. I will do more to seek out opportunities to improve our cybersecurity against current and emerging threats.

I want to thank the Chairman for holding this important hearing today, and to our witnesses here to help us understand the emerging threat landscape.

In closing, I would like to note that I view the cyber advancements much differently than I view other products in our commodity market. A lot of products, like in the automobile arena, they consider the safety aspects along with emerging technology in the cars. They are—they don't always do that with cyber technology, and we are constantly playing catch up. That is why it is really important that the Chairman and myself and others on this committee work diligently to get the information we need to try and catch up to the advancements in technology, which always seem a couple of steps ahead.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

OCT. 22, 2019

During my time as a Federal prosecutor, I saw first-hand how criminals evolved and adapted to changes. As I have learned about the cyber landscape as Ranking Member of this subcommittee, I have been amazed at the number and diversity of the cyber threats we face. These threats are always evolving and adapting to new obstacles, new protections, new tactics, and new technologies. All levels of Government—Federal, State, and local, as well as, our allies around the globe—the private sector, academia, and non-profits must work together in order to protect against emerging cyber threats.

Today's technologies have a number of vulnerabilities that must be protected from bad actors. In the first 6 months of this year, more than 4 million records have been exposed due to data breaches. Ransomware attacks have doubled in 2019—in my district, Syracuse City School District and the Onondaga County Library System both suffered ransomware attacks from unknown threat actors last month. More citizens than ever are falling victim to phishing attacks and malware. Cyber crime made up 61 percent of the attacks that cybersecurity firm, Crowdstrike, saw between January and June of this year. These are just the attacks and statistics that we are aware of; many experts believe incidents to be under-reported.

These threats are persistent, complex and on the rise, and cybersecurity must constantly evolve in order to provide protection. As evidenced by the number of incidents in this year alone, this is a difficult endeavor that cannot be done without help. As I heard from constituents in my district, companies and the local government entities need assistance and guidance to identify, protect against, and recover from current cyber threats.

And these are just the threats we see with our current technology. Our cyber landscape is becoming increasingly sophisticated and new innovations are being introduced every day. These advances could put cybersecurity out of reach for even more small, medium, and large businesses as well as State and local governments.

It is estimated that 22 million internet of things devices will be on-line by 2025. 5G deployment is just around the corner. Artificial intelligence and machine learning, while making impacts today, is projected to have even more of an enormous effect on our lives in the years ahead. Quantum computing is on the horizon.

These emerging technologies will undoubtedly present new and evolving cyber threats. While we are staying vigilant and working to protect against current hazards, we must also be preparing for future ones. Our first step is to better understand these new threats and this hearing is a good start. I am also working to educate my colleagues on the challenges and opportunities of the internet of things and the co-chair of the IOT Caucus and have spent time learning from Syracuse University about the quantum research they are working on in partnership with the Air Force Research Lab. And I will do more to seek out opportunities to improve our cybersecurity against current and emerging threats.

I thank the Chairman for holding this important hearing today and to our witnesses here to help us understand the emerging threat landscape. I look forward to our discussion and yield back.

Mr. KATKO. So with that, I yield back, Mr. Chairman.

Mr. RICHMOND. The gentleman yields back. I now recognize the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much. Good afternoon. I would like to thank Chairman Richmond for holding today's hearing on emerging cyber threats.

I have served on the Homeland Security Committee since its inception. Over that period of time I have watched the tactics our adversaries use against us evolve, and the threat landscape grow.

As new network devices and information technologies enter the marketplace, many become so mesmerized by their potential for good that we fail to appreciate and plan for the security consequences. Although I am encouraged that we are having more conversations about the nexus between technology and security today, there is still much to be done. So I commend Chairman Richmond for holding today's hearing.

When this committee was established a decade-and-a-half ago we focused our efforts on defending against physical attacks committed by terrorists who would readily claim responsibility. Now we are faced with cyber threats from state and non-state actors who use cyber tools to carry out attacks in secret, blur attribution, and complicate our ability to impose consequences.

As technology continues to evolve, so too will the tools of our adversaries. Last December DHS, DoD, the State Department, and the Office of the Director of National Intelligence identified inter-

net of things devices, artificial intelligence, and quantum technology as emerging dual-use technologies that pose a threat to our National security.

A month later, then-director of national intelligence, Dan Coats, warned that our adversaries and strategic competitors will increasingly use cyber capabilities, including cyber espionage, attacks, and influence to seek political, economic, and military advantage over the United States and its allies and partners.

Unfortunately, much of what DNI warned us about is, in fact, already happening. We know that Russia has relied on the cyber capabilities to carry out influence campaigns designed to divide Americans and swing elections. Efforts to manipulate Americans on social media platforms are wide-spread, but technologically simple.

I worry about influence campaigns of the future, where Russia uses AI to create deepfakes that make it nearly impossible to discern fact from fiction. We know that China has engaged in intelligence gathering and economic espionage, and has successfully breached OPM, Navy contractors, and non-governmental entities, from hotels to research institutions. We also know that China is investing heavily in developing quantum computing capabilities, which could undermine the security value of encryption within the next decade.

Over the past year the Department of Justice has indicated—indicted 2 Iranians for their role in the ransomware attack against the city of Atlanta. Microsoft recently revealed that Iran had attempted to breach a Presidential campaign. According to the U.N. Security Council, North Korea has used its cyber capabilities to evade sanctions, stealing $670 million in various foreign and cryptocurrencies between 2015 and 2018.

The momentum Russia, China, Iran, and North Korea have demonstrated related to their use of cyber tools shows no sign of slowing. We must prepare ourselves to harness the security, economic, and health care benefits of emerging technologies like AI and quantum computing will yield, while defending ourselves against adversaries who will use technology against us.

But the Government cannot do it alone. The private sector is a critical partner in this effort. I am eager to hear from our witnesses how the Federal Government can ensure the responsible deployment of emerging technologies.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

OCTOBER 22, 2019

I'd like to thank Chairman Richmond for holding today's hearing on emerging cyber threats. I have served on the Homeland Security Committee since its inception. Over that period of time, I have watched the tactics our adversaries use against us evolve and the threat landscape grow. As new networked devices and information technologies entered the market place, many became so mesmerized by their potential for good that we failed to appreciate and plan for the security consequences. Although I am encouraged that we are having more conversations about the nexus between technology and security today, there is still much to be done. So I commend Chairman Richmond for holding today's hearing. When this committee was established a decade-and-a-half ago, we once focused our efforts on defending against physical attacks committed by terrorists who would readily claim responsibility. Now, we are faced with cyber threats from state and non-state actors who use cyber tools to carry out attacks in secret, blur attribution, and complicate our

ability to impose consequences. As technology continues to evolve, so too will the tools of our adversaries.

Last December, DHS, DoD, the State Department, and the Office of the Director of National Intelligence identified internet of things (IOT) devices, artificial intelligence (AI), and quantum technologies as emerging, dual-use technologies that pose a threat to our National security. A month later, then-director of national intelligence Dan Coats warned that our "adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners." Unfortunately, much of what DNI's warning about is in fact already happening.

We know that Russia has relied on its cyber capabilities to carry out influence campaigns designed to divide Americans and swing elections. Its efforts to manipulate Americans on social media platforms were wide-spread, but technologically simple. I worry about the influence campaign of the future, where Russia uses AI to create "deepfakes" that make it nearly impossible to discern fact from fiction. We know that China has engaged in intelligence-gathering and economic espionage, and has successfully breached OPM, navy contractors, and non-government entities from hotels to research institutions. We also know that China is investing heavily in developing quantum computing capabilities, which could undermine the security value of encryption within the next decade.

Over the past year, the Department of Justice has indicted 2 Iranians for their role in the ransomware attack against the city of Atlanta, and Microsoft recently revealed that Iran had attempted to breach a Presidential campaign. And according to the U.N. Security Council, North Korea has used its cyber capabilities to evade sanctions, stealing $670 million in various foreign and crypto-currencies between 2015 and 2018. The momentum Russia, China, Iran, and North Korea have demonstrated related to their use of cyber tools show no signs of slowing. We must prepare ourselves to harness the security, economic, and health care benefits of emerging technologies like AI and quantum computing will yield while defending ourselves against adversaries who would use technology against us. But the Government cannot do it alone. The private sector is a critical partner in this effort. I am eager to hear from our witnesses how the Federal Government can ensure the responsible deployment of emerging technologies.

Mr. THOMPSON. With that I thank the witnesses for being here today, and I look forward to the testimony, and yield back the balance of my time.

Mr. RICHMOND. Thank you, Mr. Chairman. I want to welcome our panel of witnesses.

First I am pleased to welcome Mr. Ken Durbin, senior strategist for global government affairs at Symantec, where he has provided solutions to the public sector for over 30 years.

Next we have Mr. Robert Knake, who is a senior fellow at the Council of Foreign Relations and a senior research scientist at Northwestern University's Global Resilience Institute. Mr. Knake served as director for cybersecurity policy at the National Security Council from 2011 to 2015.

Next Ms.—Niloofar, is that right?—Razi—which is the easy part, Howe is a fellow at New America's Cyber Security Initiative. Ms. Howe has been an investor, executive, and entrepreneur in the technology industry for the past 25 years, with a focus on cybersecurity for the past 10. Most recently Ms. Howe served as chief strategy officer and senior vice president of strategy and operations at RSA, a global cybersecurity company.

Finally, Dr. Ben Buchanan is a senior faculty fellow at Georgetown's Center for Security and Emerging Technology. He has a—he has written journal articles and peer-reviewed papers on artificial intelligence, attributing cyber attacks, deterrence in cyber operations, cryptography, election cybersecurity, and the spread of malicious code between nations and non-state actors.

Without objection, the witnesses' full statements will be inserted into the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with Mr. Durbin.

STATEMENT OF KEN DURBIN, CISSP, SENIOR STRATEGIST, SYMANTEC CORPORATION

Mr. DURBIN. Chairman Richmond, Chairman Thompson, Ranking Member Katko, thank you for the opportunity to testify.

Assessing emerging threats is important, but we can't forget about traditional threats that have been re-purposed; I will address both in my testimony. I will start with a couple key findings from our 2019 Internet Security Threat Report.

Email has been a traditional threat vector cyber criminals constantly re-purpose. The latest exploit is the use of Microsoft Office attachments to deliver malicious payloads. Forty-eight percent of malicious email attachments were, in fact, Microsoft Office documents.

Attacks on endpoints from the web continue to grow. We saw a 56 percent increase in web attacks in 2018. By the end of 2018 Symantec blocked more than 1.3 million unique web attacks on endpoints every day.

As this committee well knows, supply chain attacks remain a persistent and serious threat. There was a 78 percent increase in supply chain attacks which exploit third-party services and software to compromise a target.

Deepfakes, on the other hand, are an emerging threat. Deepfake are audios or videos created by artificial intelligence systems and used to make the public believe they are authentic. Deepfakes are new, and not typically viewed as a threat to enterprise security. Fake videos, photos, or audio recordings represent a serious risk to the enterprise, since, to create convincing deepfakes, you simply need the internet, a gaming PC, and the right software. A deepfake of a CEO announcing a layoff or used to order an employee to transfer funds or intellectual property could hurt their reputation and their stock price. Until we can identify or block deepfakes, organizations will be best served implementing rapid response plans that can be executed as soon as a deepfake is identified.

Twitter bots have emerged as a threat hiding in plain sight. Symantec analyzed content released by Twitter originally posted on their service by the Russian-based Internet Research Agency. The IRA content was used as part of a Twitter bot campaign directed against the 2016 U.S. elections. The operation was carefully planned, with accounts often registered months before they were used. The data set consisted of 3,836 Twitter accounts and nearly 10 million tweets. They attracted almost 6.4 million followers and they, in turn, followed 3.2 million accounts. A core group of 123 main accounts was used to push out new content, while a larger pool of auxiliary accounts amplify messages pushed out by the main accounts. One main account only tweeted 10,794 times, but was retweeted over 6 million times.

Targeted ransomware has been re-purposed to focus on the enterprise. During 2018 attacks against organizations rose by 12 percent, but represented 81 percent of all infections that year. State

and local governments were hit hard. The city of Atlanta was attacked and chose not to pay the ransom. Clean-up is expected to exceed $10 million. The Colorado Department of Transportation spent $1.5 million to clean up after their attack. Two Florida cities took another direction and paid the ransom, which totaled $1 million between them.

Targeted attacks have tools to infect a large number of computers simultaneously, maximizing the number of assets to improve the chances the victim will pay the ransom.

Mobile is an example of a kind of self-inflicted threat. Mobile devices are susceptible to unwanted cyber threats and threats we allow via app permissions. We looked at apps on both the Google and Android platforms and found both requested personal information and access to similar device functions. Many of these requests were reasonable, but many were excessive and questionable.

We looked at a flashlight app which has over 10 million installs that wanted access to the user's location, contacts, and permission to make calls. It is difficult to imagine why a flashlight app needs your contacts, call your friends, or know your exact location. Users are opening themselves up to potential threats, since they grant permission without understanding what the app developer will do with that data.

Finally, stalkerware is a type of malware that is secretly loaded on an unsuspecting victim computing device, giving almost total control of the device to an ex-spouse, ex-boyfriend, or other stalker, who would then know the victim's exact location, be able to read their emails and texts, and even turn on their microphone or camera.

So why is stalkerware commercially available? Publishers of stalkerware typically advertise their product as parental monitoring software to keep kids safe. This can certainly be true when it is used appropriately by a responsible parent. However, the features built into some of these apps give more control than parents would need, which make them ripe for abuse.

In closing, emerging threats that try to influence beliefs or drive behavior need to be assessed along with the re-purpose traditional threats. The focus of this committee is vital for our Nation to understand these threats and ensure resources are allocated to defend against them.

Thank you for the opportunity to testify, and I would be happy to take any questions you may have.

[The prepared statement of Mr. Durbin follows:]

PREPARED STATEMENT OF KEN DURBIN

OCTOBER 22, 2019

Chairman Richmond, Ranking Member Katko, my name is Ken Durbin, CISSP, and I am a senior strategist for Symantec Global Government Affairs and Cybersecurity. I have been providing solutions to the public sector for over 30 years. My focus on compliance and risk management (CRM) and its application in both the public and private sector has allowed me to gain insights into the challenge of balancing compliance with the implementation of Cybersecurity Solutions. Additionally, I focus on the standards, mandates, and best practices from NIST, OMB, DHS, etc. and their application to CRM. I spend a significant amount of my time on the NIST

Cybersecurity Framework (CSF)[1] and the emerging privacy framework, the DHS Continuous Diagnostics and Mitigation (CDM) Program and the EU Global Data Protection Regulation (GDPR.)

Symantec Corporation is the world's leading cybersecurity company, allowing organizations, governments, and people to secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud, and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to help protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. In my testimony I will discuss the current Threat Landscape, to include:

- Key findings from the 2019 Symantec Internet Security Threat Report (ISTR);
- Mobile security privacy;
- Deepfakes risk to the enterprise;
- Twitterbots in the 2016 election;
- Targeted ransomware; and
- Stalkerware.

THE THREAT LANDSCAPE

A review of the current threat landscape shows there are challenging new attacks and threats that need to be addressed. However, it also shows that it would not be wise to ignore the traditional threats we have been dealing with for years. Bad actors are finding new ways to attack using well-established attack vectors. At the same time new technologies and campaigns are emerging to exert influence and drive behavior. I'll address both traditional and emerging threats in the following sections.

The Internet Security Threat Report

The Internet Security Threat Report (ISTR)[2] analyzes data from Symantec's Global Intelligence Network, the largest civilian threat intelligence network in the world, which records events from 123 million attack sensors worldwide, blocks 142 million threats daily, and monitors threat activities in more than 157 countries. The analysis provides insight into a wide variety of threats and identifies trends that help inform the public with the goal of helping them avoid risk. Highlights from the ISTR include:

- One out of 10 URLS are malicious. That is up from one in 16 in 2017. Clicking on a malicious URL continues to be a widely-used attack vector by attackers.
- There was a 56 percent increase in web attacks over 2017. By the end of 2018, we blocked more than 1.3 million unique web attacks on endpoint machines every day.
- On average, 4,800 websites are compromised with formjacking software each month.
- Formjacking is the use of malicious JavaScript code to steal payment card details and other information from payment forms on the checkout web pages of eCommerce sites. We blocked 3.7 million formjacking attempts on endpoint devices in 2018.
- Supply chain attacks increased 78 percent. Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software.
- Forty-eight percent of malicious email attachments were MS Office documents, up from just 5 percent in 2017. Cyber crime groups continued to use macros in Office files as their preferred method to propagate malicious payloads in 2018, but also experimented with malicious XML files and Office files with Dynamic Data Exchange (DDE) payloads.
- The number of attack groups using destructive malware rose 25 percent. Destructive malware is designed to inflict physical damage to an organizations network or facility. While still a niche area, the use of destructive malware continued to grow. Eight percent of groups were known to use destructive tools, up from 6 percent at the end of 2017.

---

[1] NIST Cybersecurity Framework (CSF): Provides guidance to private companies on how best to prevent, detect, and respond to cyber attacks.

[2] *https://www.symantec.com/security-center/threat-report*.

Mobile Security

The average smartphone user these days has between 60 and 90 apps on their device, and most of them request some sort of information about the user and the device. They may want to know your name, your email address, or your real-world address. But because smartphones are so powerful, they can also get quite a bit more than that, such as your exact location. Some apps will even request access to the device's camera or microphone despite having no legitimate need to use them.

In order to find out what kind of data your apps may be looking for, we analyzed the top 100 free apps as listed on the Google Play Store and Apple App Store on May 3, 2018.[3] For each we looked at 2 main things: How much personal information was the user sharing with the app and which smartphone permissions the app accessed.

Email addresses are the most common piece of personally identifiable information (PII) apps were accessing, as 48 percent of the iOS and 44 percent of the Android apps did so. Username was next, which was accessed by 33 percent of iOS and 30 percent of Android apps, followed by phone numbers, which were accessed by 12 percent of iOS and 9 percent of Android apps. Finally, 4 percent of iOS and 5 percent of Android apps accessed the user's physical address.

It is often reasonable and necessary to grant apps permission to access various features on a smartphone. For example, if you want to take a picture using an app, the app will need permission to use your device's camera. However, not all permissions are the same. We took a closer look at permissions that could provide access to data or resources that involve the user's private information or could potentially affect the user's stored data or the operation of other apps.

Camera access was the most requested permission, with 46 percent of Android and 25 percent of iOS apps seeking it. That was followed by location tracking, which was sought by 45 percent of Android and 25 percent of iOS apps. Twenty-five percent of Android apps requested permission to record audio, while 9 percent of iOS apps did so. Last, 15 percent of Android apps sought permission to read SMS messages and 10 percent sought access to phone call logs. Neither of these permissions are available in iOS.

Apps have permissions because the user granted them by hitting an "I Agree" button—usually without considering if certain permissions make sense, and often without pausing to consider the request at all. For example: The Android flashlight app "Brightest Flashlight LED—Super Bright Torch", which has 10 million installs, asks for permissions including precise user location, access to user's contacts, and permission to directly call phone numbers. It is hard to imagine why a flashlight app has a legitimate need to copy all of your contacts, call all of your friends, or know exactly where you are located. Consumers should pause before the agree to permissions—and app developers should be very clear about what permissions their app needs and why it needs them.

Deepfakes

"Deepfakes" are audio or video tracks created or altered by artificial intelligence (AI) systems and used to make the public believe they are authentic. Most of the popular examples of deepfakes show politicians or actors saying or doing things designed to embarrass or harm reputations. As a result, deepfakes are not typically viewed as a threat to Enterprise security.

This is short-sighted. Enterprises do need to pay attention to deepfakes; fake content like videos, photos, audio recordings or emails represent a serious risk to individuals as well as the organization. The technology behind deepfakes has advanced to the point decisions might be made based on a deepfake, or decisions not made because an authentic video is thought to be a deepfake. Deepfakes are particularly dangerous because there is such a low barrier of entry and because they are difficult to detect. Until recently, altering videos was expensive and required significant resources, specialized equipment, and money. Today, if someone has access to the internet, a gaming PC and the right software they can produce convincing deepfakes. Specialized applications have reduced creating deepfakes to a point-and-click exercise, reducing the need for advanced skills.

Deepfakes are created using a process based on Generative Adversarial Networks (GAN). Essentially, a GAN consists of 2 machine-learning networks that work in an on-going feedback loop where 1 network creates the deepfake and the second one tests the output. The networks pass the deepfake back and forth making alterations to make it as realistic as possible. Since the GAN is "learning" throughout the process, the deepfake becomes harder to spot with the naked eye.

---

[3] *https://www.symantec.com/blogs/threat-intelligence/mobile-privacy-apps.*

Given the low barrier of entry and that they are difficult to detect, Enterprises need to understand the risks deepfakes pose to their organization. For example: A deepfake of a CEO announcing a massive layoff could cause their stock price to sink. A deepfake could be used to order an employee to wire funds, or transfer intellectual property out of the company. Until a proven method to identify or block deepfakes is developed organizations will be best served educating employees about the danger of deepfakes and implementing rapid response plans that can be executed as soon as a deepfake is identified.

Twitterbots

In October 2018, Twitter released a massive dataset of content posted on its service by the Internet Research Agency (IRA) beginning in May 2014. The IRA is the Russian company behind the social media propaganda campaign directed against the 2016 U.S. elections. Symantec conducted an in-depth analysis of the dataset to learn more about how the campaign operated.

The dataset consisted of 3,836 Twitter accounts and nearly 10 million tweets. These accounts amassed almost 6.4 million followers and followed 3.2 million accounts. The sheer volume of data was enormous, more than 275 GB.

Our research [4] led to a number of interesting findings:

1. The operation was carefully planned, with accounts often registered months before they were used. The average time between account creation and first tweet was 177 days. The average length of time an account remained active was 429 days.
2. A core group of main accounts was used to push out new content. These were often "fake news" outlets masquerading as regional news outlets or pretending to be political organizations.
3. A much larger pool of auxiliary accounts was used to amplify messages pushed out by the main accounts. These accounts usually pretended to be individuals.
4. Some operatives may have been making money on the side by using monetized URL shorteners to create links. If they did monetize the URLs one account in particular could have generated almost $1 million.

We divided the accounts into two main categories; main accounts and auxiliary accounts. Each category had different characteristics and played a different role. We identified 123 main accounts, each having at least 10,000 followers. Main accounts tended to not be followers of other accounts. They were primarily used to publish new tweets.

We identified 3,713 auxiliary accounts, each having less than 10,000 followers. Auxiliary accounts tended to be followers of thousands of other accounts. Their main purpose was to retweet messages from other accounts. Since auxiliary accounts were used to amplify targeted messages it makes sense they were the larger category.

A particularly effective account in the dataset was called TEN—GOP. Created in November 2015, the account masqueraded as a group of Republicans in Tennessee. It appears to have been manually operated. In less than 2 years TEN—GOP managed to rack up nearly 150,000 followers. Despite only tweeting 10,794 times, the account garnered over 6 million retweets. Only a small fraction (1,850) of those retweets came from other accounts within the dataset. In other words, almost all of its retweets came from accounts outside the dataset, meaning many could have been real Twitter users.

The Twitterbot campaign is often referred to as the work of trolls, but the release of the dataset makes it obvious that it was far more than that—it was highly professional. It was planned months in advance and the operators had the resources to create and manage a vast disinformation network. And aside from the sheer volume of tweets generated over a period of years, its orchestrators developed a streamlined operation that automated the publication of new content and leveraged a network of auxiliary accounts to amplify its impact.

Targeted Ransomware

Ransomware continues to be one of the most dangerous cyber threats facing any organization. The threat has changed significantly over the past 2 years, as criminals are increasingly targeting enterprises. During 2018, while the overall number of ransomware infections was down 20 percent, attacks against organizations (as opposed to against individuals) rose by 12 percent. Alarmingly, Enterprises accounted for 81 percent of all ransomware infections in 2018. Targeted attacks have been particularly hard on State and local government organizations. In March 2018 the city of Atlanta was attacked and ransomware encrypted servers that made over a third

[4] *https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.*

of the 424 city-wide services inaccessible. The clean-up costs for the attack are expected to run to over $10 million. The Colorado Department of Transportation spent $1.5 million to clean up after they were attacked. Two Florida cities that were attacked took another route—they paid the ransom, which totaled $1 million between them.

The number of targeted ransomware attacks has multiplied as new groups move into this sector. Although targeted ransomware attacks account for a small percentage of overall ransomware attacks, they present a far greater risk as a successful targeted ransomware attack can cripple an ill-prepared organization. These attacks also typically involve much higher ransom demands, ranging from $50,000 to over $1 million.

Targeted attacks can result in hundreds of computers encrypted, backups destroyed, and business-critical data removed from the organization. Targeted attacks can shut down an organization, leading to loss of business, reputational damage, and multimillion-dollar clean-up bills. The number of organizations affected by targeted ransomware attacks has grown sharply over the past 2½ years. As recently as January 2017, Symantec observed just 2 organizations a month being attacked. However, recent months have seen that figure grow to above 50 organizations a month.

The SamSam ransomware group was the original targeted ransomware threat, but was joined in 2018 by another highly-active targeted actor called Ryuk. In 2019 several additional groups were linked to a series of highly disruptive attacks in the United States and Europe. Current trends indicate that targeted ransomware is attracting a high degree of interest among cyber criminals, with new groups appearing at an accelerating pace, motivated no doubt by the success of some recent attacks. RobbinHood is another new family, first appearing in May 2019. It was reportedly used in the attack against the U.S. city of Baltimore that shut down several services, including municipal employees' emails, phone lines, and on-line bill payments.

A group known as GoGalocker has used a new breed of targeted ransomware that appeared in early 2019. Traditional ransomware attackers cast a wide net using spam campaigns to improve their chances of finding a victim. GoGalocker selects targets and digs in deep. The attackers behind GoGalocker appear to be highly skilled, capable of breaking into the victim's network and deploying a wide array of tools in order to map the network, harvest credentials, elevate privileges, and turn off security software before deploying the ransomware. This process permits the attackers to identify and access a large number of computers in order to later simultaneously infect them with the ransomware. By maximizing the number of assets, the attacker compromises the better the chances are the victim will pay the ransom.

Stalkerware

Stalkerware is a type of malware that is secretly loaded on an unsuspecting victim computing device giving almost total control of the device to a bad actor. The bad actor—who can be an ex-spouse, ex-boyfriend, or other stalker—would then know the victims exact location, be able to read their emails and texts, and even turn on their microphone or camera. Due to the control Stalkerware gives a bad actor, it is classified as a type of malware—malicious software designed to gain access to or damage your computer, often without your knowledge.

Stalkerware can affect PCs, Macs, and iOS or Android devices. Although Windows operating systems may be more susceptible to attacks, attackers are becoming better at infiltrating Apple's operating systems as well. Stalkerware typically infects a device when the victim accepts a prompt or pop-up without reading it first, downloads software from an unreliable source, opens email attachments from unknown senders, or pirate media such as movies, music, or games

So why is Stalkerware available in app stores? Publishers of Stalkerware typically advertise their product as parental monitoring software to keep kids safe, and this can certainly be true when it is used appropriately by a responsible parent. However, any software surreptitiously loaded onto a device, no matter how well-meaning is malicious. Additionally, the features built into some of these apps give more total control of a device than parents would need and make it ripe for abuse.

CONCLUSION

New threats are emerging every year—but that does not mean existing threats have gone away. We need to be vigilant in our defense against the traditional threats we have battled for years, while understanding emerging threats and planning defenses accordingly. Emails have been a persistent attack vector, yet attackers are finding new ways use the service against us. Ransomware is not new but the attacks are becoming more targeted and disruptive. Mobile security is a

threat we allow by granting excessive permissions. Finally, deepfakes and twitterbots teach us that cyber can be utilized to influence and force actions from a distance. The focus of the Cybersecurity, Infrastructure Protection, and Innovation Committee is vital for our Nation to understand the current threat landscape and ensure resources are allocated to determine how to defend against them. Thank you for the opportunity to testify before this committee, and I would be happy to take any questions you may have.

Mr. RICHMOND. Thank you, Mr. Durbin. Thank you for your testimony.

I now recognize Mr. Knake to summarize his statement for 5 minutes.

STATEMENT OF ROBERT K. KNAKE, SENIOR RESEARCH SCIENTIST, GLOBAL RESILIENCE INSTITUTE, NORTHEASTERN UNIVERSITY, SENIOR FELLOW, THE COUNCIL ON FOREIGN RELATIONS

Mr. KNAKE. Thank you, Mr. Chairman. I want to break down my remarks into 3 categories.

OK, thank you, Mr. Chairman. I want to break down my comments into 3 categories, what I will call the good, the bad, and the ugly.

The good is that I think we are actually making progress in cybersecurity. Ten years ago, when I wrote my first book on cyber warfare, it was a dire prognosis for the patient. We concluded in that that the attacker had an overwhelming advantage, and that private companies could not possibly protect themselves from Russian, Chinese, or other state-based adversaries.

I think the last 10 years have showed us that, in fact, some companies are able to manage the risk from even the most sophisticated adversaries, and they are able to do it day in and day out. In the last decade we have seen the development, not just of new technology, but new doctrine and new strategies and new tactics for defense.

Most notably, I will call out the kill chain. Right? This is the basic concept that an adversary doesn't simply need to compromise a single host, they need to go through a series—anywhere from 7 to 22 steps, depending on how you count—to achieve their objective. So, from that perspective, a defender only needs to detect them at one, and block them at one of those stages.

This kind of thinking has allowed us to reverse the notion that the offense has an overwhelming advantage in this space. We now have tooling around that. Technology like endpoint detection and response, end-point protection program that can automatically identify malware. These technologies have really helped us turn a corner for the most sophisticated of cyber defense programs. That is the good news.

What we need to do now, of course, is create the incentives and the structures and the Government enablement to drive these innovations down into the wider markets so that school districts and local governments and mom-and-pop businesses are able to achieve this level of cybersecurity.

The bad news is, of course, the technology landscape, as you all know, is rapidly changing. This may mean that, by the time we get in place these secure systems, these secure concepts that will help

protect the state of play today, the technical terrain is going to have changed.

We have talked about IOT, we have talked about AI, and we have talked about quantum. Those, I think, are the 3 big changes out there. I would add, with IOT, 5G. Ubiquitous high-speed connectivity is going to enable so many millions of devices to be connected.

What we have seen so far is that, for IOT, it is not really so much a new technology as a trend toward cheaper computers and ubiquitous connectivity that is enabling us to put computers everywhere. What we are not doing is learning the lessons from the past 20 years of enterprise security and applying those lessons into the IOT space.

For artificial intelligence and quantum, the only thing I can say is we have got to make sure that this is a race between the United States of America and the Chinese, not a race between Silicon Valley and the Chinese. The capability that Silicon Valley is bring to this fight is immensely important, but they are acting in their commercial interests, as they should as private businesses. We need to ensure that we have the funding there.

So finally, I would say the ugly of it is Government intervention in this space. We have got to make sure that Government is helping to align market interests in favor of security. That is going to require doing things that we haven't wanted to do in this space, like regulate, in part because we believe that the technology is moving too fast for Government regulation to keep up.

I think, though, that there is an answer here, and I think it is fairly simple. Instead of Government setting requirements that we know adversaries will target to get around, our goal needs to be to require outcomes. We can do this through insurance. We can do this through other financial incentives. But we have models for this in other spaces that we can apply, so that the goal should not be to meet a list of Government requirements for what security looks like, but to achieve an objective that we know current technology can meet, and that the market can reinforce companies meeting that objective.

Thank you very much.

[The prepared statement of Mr. Knake follows:]

PREPARED STATEMENT OF ROBERT K. KNAKE

TUESDAY, OCTOBER 22, 2019

INTRODUCTION

Thank you Chairman Richmond, Ranking Member Katko, and Members of the committee for the opportunity to testify on this important matter. While other witnesses will focus on how the capabilities of specific threat actors may change and evolve, I would like to focus my remarks on how the technology landscape may change in the next 5 years and what that may mean for emerging cyber threats. Before I begin, let me be clear that the views I represent here are my own and do not represent my employers or any supporters of my work.

Looking back over the past decade, there are reasons to be hopeful for a secure cyber future. When my co-author Richard Clarke and I wrote *Cyber War: The Next Threat to National Security and What to Do About It* a decade ago, we predicted a dire future in cyber space. Early trends then indicated to us that our adversaries would develop sophisticated cyber offensive capabilities and would use these capabilities to undermine our dominance of conventional military domains. We predicted correctly that North Korea would emerge, somewhat surprisingly, as a capable ad-

versary in the cyber domain and highlighted China's on-going campaign of economic espionage on behalf of its National champion companies. We of course failed to predict many of the key events that are top of mind today like Russia's use of the internet to interfere in elections and sow dissent; however, in my view, our greatest error was our failure to see the technology trends that have allowed the defensive community to be able to manage the threat posed by even the most determined nation-state adversaries.

In *Cyber War,* we concluded that private companies could not defend themselves against determined adversaries because cyber space as a domain favors the attacker. Conventional wisdom at the time was that an attacker had all the advantages. An attacker only needed to find one vulnerable system to succeed whereas the Chief Information Security Officer (CISO) at a large enterprise had to defend thousands or hundreds of thousands of systems. This asymmetry was often captured as the idea that "the attacker only needs to compromise one vulnerable system; the defender needs to be perfect."

The good news is that technology trends and new doctrine for cybersecurity have dramatically changed the terrain of cyber space. Companies at the leading edge of cybersecurity have been able to manage the threat from even the most sophisticated actors. If these trends continue and if policy is put into place to correctly align incentives, it is possible that in 5 years we may view cybersecurity broadly as a manageable problem. The bad news is that emerging technologies may once again favor the attacker, erasing the defensive gains of the past decade. In my remarks below, I will review the "good news" of the last decade and how these trends can be accelerated and adoption of better cybersecurity practices encouraged by Congress. I then will discuss the "bad news" of how emerging technology trends like artificial intelligence, the internet of things and 5G, and quantum computing could favor the offense. I then provide some thoughts for how Congress can promote wider adoption of cybersecurity practices that are on the cutting edge today and shape the future of technology so that defenders are not left at a disadvantage tomorrow. Finally, I conclude with a brief review of the projects I am working on today that may help us build a more resilient cyber future.

THE GOOD NEWS: CYBERSECURITY IS POSSIBLE

There is an old joke in cybersecurity, attributed to Dmitri Alperovitch, now the Chief Technology Officer (CTO) of the cybersecurity firm Crowdstrike. The joke, retold in many formulations, is always along the lines of "there are two types of companies: Those that have been hacked and know it and those that have been hacked and don't know it." That may have been true a decade ago, but today there are three types of companies: Those that have been hacked and know it, those that have been hacked and don't know it, and those that are actively and successfully managing the risk.

In *The Fifth Domain,* Clarke and I conclude that the greatest advance in cybersecurity over the last decade was not a technology but a white paper. In "Intelligence-Driven Security" a group of researchers and practitioners at Lockheed Martin presented the processes they had developed for detecting and disrupting adversary activity along the "Cyber Kill Chain". Published in 2011, the paper showed how defenders could take the advantage away from adversaries by breaking down the process by which an adversary attempted to achieve an objective on a network and building a security program around each of those steps. Unlike in conventional thinking on cybersecurity where a network compromise is considered a failure, the Kill Chain methodology sees that as only one step in the chain. Before an adversary can exploit an initial host on a network, they must engage in reconnaissance of the target, weaponize what they have learned into a package capable of compromising the target and deliver it. After they have achieved the initial exploitation, they then need to gain administrative rights, move laterally across the network to find their target, and then carry out out their intended action. That action might be to exfiltrate data off the network or to destroy operational systems. Whatever their goal, it is not simply to compromise a single system.

The concept of the kill chain has evolved and expanded since first published. MITRE Corporation has developed the ATT&CK Matrix to further breakdown the steps that happen after initial compromise into 22 discrete steps. However you break down the attackers progression, the key takeaway should be that detecting and stopping them is possible. Whether the adversary needs to go through 7 steps or 22, they have to successfully avoid detection at each stage; defenders only need to detect them at any one stage. Once the adversary is on the defender's system, the defender should have the advantage. Gaining that advantage requires knowing the topology of your system better than the adversary and being able to detect

anomalous behavior within it. This ability to detect and respond rapidly is what Crowdstrike and other companies have specialized in. Endpoint Detection and Response (EDR) has been the technical capability that has enabled "threat hunting" along the kill chain to occur at scale within enterprises. Managed Detection and Response companies are rapidly bringing these capabilities to the middle market.

Beyond detection and response, newer technologies have the potential to remove large swaths of risk. When properly deployed and managed with security in mind, cloud computing, containerization, and software defined networking, to name just three emerging technologies, can provide real advantages to defenders. Virtualization can allow new computing environments to be spun up and down for a specific purpose so rapidly that gaining a foothold in one of these new environments does an adversary no good because the environment itself does not persist. These technologies can also allow for deception campaigns on a massive scale to create new opportunities for detection and to increase the work factor of adversaries.

All this adds up to the potential to make our country, our companies, and ourselves resilient to cyber attacks. Through the adoption of secure-by-default technologies we should be able to make it so that almost all attacks "bounce off" and that we can "bounce back" when attacks do succeed. From a policy perspective, what is needed now are the incentives and requirements to promote the adoption of these techniques and the technologies beyond the small handful of companies that are deploying them in a holistic way today. And of course, this transition needs to occur at a faster rate than adversaries can adopt new technologies that defeat them.

THE BAD NEWS: TECHNOLOGY CHANGES COULD ERASE THESE GAINS

Just as we may be turning a corner on security, the technology landscape may change in ways that are not evolutionary but revolutionary. By that I mean that the technology coming on-line is not about the continuation of current trends or even the acceleration of trends but whole new classes of technology. Artificial intelligence, quantum computing, and 5G and the internet of things may not intrinsically favor attackers over defenders but the offense is likely to adopt technologies that can give them an advantage faster than defenders and their targets are likely to adopt new technologies in ways that open up new swaths of vulnerabilities. I would like to now discuss three such technologies: (1) Artificial intelligence; (2) 5G and the internet of things; and (3) quantum computing.

Artificial Intelligence

Arguably, artificial intelligence up until now has been a technology that has favored the defense. Many of the gains discussed above in the last decade are due to artificial intelligence applications within cybersecurity. For instance, the ability of advanced endpoint protection programs to identify never before seen malware using machine learning has made the work of adversaries much more difficult. The bad news is that as the state-of-the-art in artificial intelligence advances, attackers are likely to use it in ways that will upend the basis of today's security architectures.

Deepfakes have made headlines recently in the political world. For public figures who have thousands of hours of voice and video recordings available on-line, artificial intelligence can now be used to piece together snippets of them talking to literally put words in their mouths. Deepfakes are likely to come into play heavily in the 2020 election and defenses against them are lagging. Use of AI for deepfake detection made news over the summer but in this arms race, adversaries look to have an advantage, tweaking their tools and testing against deepfake detection technology until they can defeat it.

Initially, deepfakes required large libraries of voice and video but as the technology improves, the amount of source data required is rapidly coming down. That will mean that many of the fundamental controls we have in place today to combat cyber crime may no longer be trusted. The cybersecurity community has worked hard to educate companies about the dangers of wire transfer fraud—to train finance departments to be suspicious of emails from the CEO ordering them to wire funds on an emergency basis, for instance. But what if, instead of compromising the email system, adversaries compromise voice and video systems, and your boss in her natural speaking voice that you hear everyday, calls you to confirm that she does in fact need you to wire those funds right now? The ability to create deepfakes from smaller and smaller sets of source material will make that scenario possible for many companies in a short period of time. That will mean that the ultimate root of trust—believing what we see and hear—can no longer be trusted.

5G and the Internet of Things

Internet of things (IOT) technology is rapidly being distributed within critical infrastructure and in homes and businesses in ways that appear to ignore the security

lessons we learned over the last 20 years within enterprise systems. Coding practices are poor in the space, firmware is difficult to update, and systems are widely exposed to the public internet. What's more, with the advent of 5G, massive, ubiquitous wireless connectivity will mean that many of these devices will be directly connected to the public internet with no defense-in-depth built around them. Within the consumer market, we have seen a troubling trend of "set and forget" connected devices that, after being setup, are not monitored for security and do not receive updates to their software after problems are discovered. Unfortunately, this trend does not appear to be confined to the home IOT market. The same problem is occurring even within industrial control systems.

Quantum Computing

Far more than these other two technological shifts, quantum computing is likely to up-end computer security because it will up-end computing. A calculation that might take a classical computer several centuries to complete could be done by a quantum computer in the blink of an eye. Experimental systems today are showing a lot of promised toward achieving this kind of capability. Google may already have achieved what is known as "Quantum Supremacy", using a quantum computer to complete a mathematical equation faster than a conventional system could.

Quantum computing has the potential to be extremely disruptive to security, allowing encryption protocols to be defeated; whether quantum resistant encryption will be deployed ubiquitously and will prove to defeat quantum computing is an open question. The combination of artificial intelligence technology with quantum computing open some scary possibilities. More than anything else, Government needs to ensure that the United States is a leader, not a follower, in the development of quantum computing.

THE UGLY: GOVERNMENT INTERVENTION IN NECESSARY

For most of the last 20 years, U.S. Government policy across administrations has largely been about getting out of the way and hoping that markets would solve cybersecurity problems on their own. Where Government has intervened, intervention has been uneven and light touch. Today, I believe we are starting to recognize that markets alone will not solve our cybersecurity dilemma. I think it is fair to conclude that the industries that are doing the best at actively managing risk in cyber space are also actively regulated: Financial services and the defense industrial base. Many of the approaches to security that are working today were pioneered in these sectors. Driving these innovations to other markets will require creating the right set of incentives and requirements. I have been pleased to see that more so than in any previous administration, the current leadership of the Department of Homeland Security has recognized that regulation, smartly and carefully implemented, is necessary to drive the level of security required for our Nation. The Department's cybersecurity strategy is explicit on this point. In the IOT space, DHS should lead efforts to regulate the security of IOT devices in the sectors that it regulates including chemicals, pipelines, and the maritime industry.

I believe that the Internet of Things Cybersecurity Improvement Act would be a good first step toward improving IOT security. The act would set standards that sellers of IOT technology to the Federal Government would need to meet as well as establish disclosure requirements when manufacturers discover vulnerabilities. The approach uses Government's massive purchasing power to improve security more broadly. Companies that develop technologies on a "build once, sell everywhere" model will likely meet the Government's requirement for all their commercial offerings rather than just for those sold to Government. These requirements, once set, could then be adopted to regulate the use of IOT in critical infrastructure sectors.

Fundamentally, however, I believe that setting requirements is insufficient. We need to make device makers responsible for the full life cycle of security by making them liable for harm caused by their devices. I recognize that this notion is a radical departure from how we have approached liability within the information technology realm thus far but now that these devices are making their way into National security systems and life safety systems, I think it is critical that we create incentive structures that truly value security. In the next section, I discuss one effort we have undertaken at the Global Resilience Institute to create a model for liability for cybersecurity.

Beyond IOT, the leadership of the Cybersecurity and Infrastructure Security Agency (CISA) has made election security the agencies No. 1 priority. CISA will need to build on its current efforts to counter-election interference to play a role in combating the proliferation of deepfakes in the political realm and for enterprise security. Crucial to this effort will be building strong, operational partnerships with

social media companies that go well beyond today's arm length interactions. Steps must be taken to breakdown the reluctance by Facebook, Google, Twitter, and other social media companies to truly partner with Government on this problem.

For quantum computing and artificial intelligence, Government's role should be less about managing the cybersecurity implications and more focused on ensuring that the United States competes and wins in these technologies. I tend to be skeptical of analogies to arms races or calls for Apollo Programs or Manhattan projects, but on the basic science in these fields, those kinds of approaches are warranted. Both China and Russia have made gaining an advantage in AI a National priority. China has also done that on quantum. I believe our market-based approach to technology development comes with real advantages but in the development of these core capabilities, I worry that a race that is the Chinese State vs. Silicon Valley is one that Silicon Valley will lose. We need a National effort to ensure that U.S. technology leadership continues into the next decade.

Each of these lines of effort will take at least half a decade to produce meaningful results—thus it is crucial that the efforts begin now.

WHAT WE ARE DOING AT GRI

The challenges we face are large, but they are not insurmountable. While much work remains to be done, let me take this opportunity to highlight four efforts under way at the Global Resilience Institute that may contribute to improving our National cyber resilience over the next 5 years.

Creating a National Transportation Safety Board for Cyber Incidents

Resilience is a concept that we have talked a lot about in the field of cybersecurity but it's a far better-developed idea in other fields like emergency management and psychology. One of the key components of resilience I have taken away from studying the concept in these other fields is the importance of adapting following a bad outcome. Learning from disasters or even from so-called "near misses" is critical to the development of resilience. To this end, as far back as 1991 practitioners in the field have suggested that Government should develop the equivalent of a National Transportation Safety Board (NTSB) for cybersecurity incidents, a "Cyber NTSB". Given that this idea was first suggested 3 decades ago but has yet to reach fruition, we are planning a workshop, sponsored by the National Science Foundation, to develop a prototype process for how such an organization would operate. We plan to hold the workshop in the spring of 2020.

Building a High Assurance Network for Collaborative Defense

Critical to building resilience is creating a model for Collaborative Defense. The "partnership" that has been the central tenet of our National cybersecurity policy for 2 decades needs to evolve to real-time, operational collaboration. In order for that to happen, we need collaboration platforms where the members of this partnership can trust each other. Government needs to be able to trust that the intelligence it shares will be protected and only shared appropriately and securely. But private companies need the same degree of assurance when they share with Government and with each other. Today, the platforms on which we collaborate, internet-connected, general purpose computers, are not trustworthy. Moreover, we often do not know whether we can trust our partners that are using those computers.

When I testified before this committee 2 years ago, I discussed early thinking about how to develop such a network. Today I am pleased to say that, working with our partners at the Advanced Cybersecurity Center and with a generous grant from a private foundation, we have developed a prototype network. This network takes advantage of the trends in computing that have dramatically lowered cost: Inexpensive computing at endpoints and cloud computing to provide immense computing power for analytics and other services. For about $300 a year, we can provide a high assurance endpoint that can only be accessed by specified users to connect to a secured, private network for threat collaboration. This model provides the basis for addressing the issue of trust in the users and trust in the systems by replicating at far lower costs many of the design criteria of the Classified networks used by Government today.

In my view, the model we have developed should be adopted by the Department of Homeland Security to create what we have dubbed CInet for Critical Infrastructure Network. Using existing authorities, the Secretary of Homeland Security should establish a new safeguarding standard for Confidential information, the existing level below Secret in the classification schema. The standard should be built around the prototype we have developed which eliminates the most common paths to compromise (spear-phishing, credential compromise, and watering hole attacks) and prevents end-users from unintentionally releasing information through a series

of technical controls. Having vetted the concept with a handful of critical infrastructure companies, we believe that this model could fit into the current operating models within critical infrastructure security operating sectors. We also believe that by harnessing current best practices in the private sector for continuous monitoring of insider threats, the Secretary could also promulgate a different standard for granting of clearances at the Confidential level that would be better, faster, and cheaper. Then would come the hard part of convincing the intelligence community to target collection to provide relevant threat intelligence to participating companies and to downgrade it to the Confidential level.

Designing a Darknet for the Electric Grid

Many of the same technology trends that could provide attackers an advantage over the next 5 years can also be harnessed to increase security for critical infrastructure. Advances like software defined network (SDN), increased mobile bandwidth with 5G, and artificial intelligence can enable far higher degrees of assurance for critical infrastructure than can be attained today. This is the idea behind our Darknet project to create a separate network for the electric grid using "dark" or unlit fiber optic cables. GRI initially began work on this concept with a grant from a private foundation and is now partnering on it with Oak Ridge National Laboratory.

Developing an Insurance Regime that Promotes Better Security

Cyber insurance was supposed to help drive down risk. In theory, the insurance sector, in exchange for providing insurance coverage, would require companies to prove that the risk they underwrote was being managed. In practice, as the recent spate of ransomware attacks on city governments has demonstrated, cyber insurance is simply transferring the risk and enriching the criminal groups behind the attacks. Yet, in other sectors, insurance markets have proved remarkable mechanisms for encouraging risk reduction. Dr. Stephen E. Flynn, the director of Northeastern's Global Resilience Institute, and I have been developing a model for insurance that would promote risk reduction rather than just risk transference. Dr. Flynn, a retired Coast Guard officer, has posited that the regime put in place under the Oil Pollution Act of 1990 after the Exxon. Valdez oil spill could be ported over for data security. In other words, we should treat data spills like oil spills. Under that regime, ships entering U.S. waters must provide proof in the form of a Certificate of Financial Responsibility that their owners or their guarantors in the insurance industry have the financial resources to cover the cost of cleaning up an oil spill should containment on their vessel fail. Notionally, owners of data could be required to take out insurance policies to cover the full societal cost should they fail to protect the data that they hold. In this thinking, Congress could establish a dollar figure per record and then require holders of personal data to obtain insurance to cover those loses. From there, market mechanisms would take over to determine how to price risk. This model could also be adapted for critical infrastructure. For instance, if natural gas pipeline owners had to obtain private insurance to cover the costs of a disruption to service caused by malicious cyber activity, markets would likely require a far higher degree of assurance than would be required through a standard regulatory model. In the coming months, we will engage the insurance industry on further developing this concept.

Mr. RICHMOND. Thank you, Mr. Knake.

We will now recognize Ms. Howe to—five minutes to summarize your statement.

STATEMENT OF NILOOFAR RAZI HOWE, SENIOR FELLOW, CYBERSECURITY INITIATIVE, NEW AMERICA

Ms. HOWE. Chairman Richmond, Chairman Thompson, Ranking Member Katko, distinguished committee Members, thank you so much for inviting me to speak today about emerging cyber threats. My name is Niloofar Razi Howe, and for over 2 decades I have worked in the technology sector, including cybersecurity, as an investor, as an entrepreneur, and as an executive.

When I first started working in technology we had a Utopian vision for the internet, and cybersecurity was a dark art that lived in its own silo. But as the internet has matured, and every aspect

of our lives has become operationalized in this domain, the threat it represents has grown in kind and in effect.

From IP theft, to cyber crime, to espionage, hostile social manipulations, radicalization, and cyber war, the activity and malfeasance that takes place affects all of society. It affects all of our businesses, not just critical infrastructure. It affects our Government's ability to provide services. Most importantly, it affects all of us, the people. This same adversary that is infiltrating our defense industrial base is stealing intellectual property from our companies, probing our infrastructure, and manipulating individuals. As Dan Geer famously said, "Every sociopath is now your next door neighbor."

There are no more silos. The problem is only getting bigger as we embrace new waves of technology, innovations such as cloud computing, autonomous vehicle, small low-orbit satellites with advanced sensor platforms, the internet of things, drones, distributed ledger technology, augmented and virtual reality. On the horizon we see the emergence of 5G and microsensor proliferation, autonomous weapons for private and military use, quantum computing, AI, and synthetic biology, to just name a few.

People and businesses will not wait for security laws and regulation to catch up before they embrace these technologies. They don't have a choice. The internet of things, which has the potential to change industries at their core and create over $11 trillion of economic gain, has security issues that are well understood. But these issues will not slow adoption down. Oddly, there is too much at stake to wait for security.

For the first time in human history, the accelerating pace of technology innovation is outstripping our ability as human beings to adapt and adjust our policies in a time line that is relevant. Our adversaries have repeatedly shown that they can move faster than we do. They adapt and exploit technology while we grapple with its implications, emerging social norms, the uneven distribution of authorities and capabilities, and a political process that does not function at the speed of innovation.

While we study the problem, our adversaries have infiltrated our systems, exploited an already polarized society, and undermined the very foundation of our democracy, the belief that there is such a thing as objective truth—because where there is no objective truth, the biggest liar wins.

We need a coordinated and collaborative whole-of-society approach to rise to the challenge of these emboldened adversaries that we are out of position to deal with. It is time for the United States to set a bold cyber agenda capable of restoring trust globally, trust in our technology, trust in our systems, trust in our infrastructure, and, through that, trust in our political system, our political process, and our leaders.

To be effective our Government will have to do this in partnership across the Government and with private sector, and remove any barriers that prevent Government agencies that have relevant information from sharing that information and the context that goes with it with the entities that are most affected. This collaboration must extend to our cities, which are overwhelmed and under-

resourced. Their vulnerabilities are a homeland security issue, especially as we look at our election infrastructure and ransomware.

To have trust in our systems and infrastructure we must commit to regaining our innovation edge, and never again lose our seat at the standard-setting table. As we look to the next waves of technology, especially AI and quantum, falling behind is not about National pride. It is about National security. We must have a strong and consistent cyber deterrence policy, something only the Government can deliver on. Even the strongest walls will eventually succumb to a capable and determined adversary if there is no deterrence.

Technology companies that are co-conspirators with our adversaries, that facilitate communications and propaganda networks enabling destructive and chaotic social manipulation must be regulated. To build resilience in society to social manipulation efforts, funding and incentivizing media literacy programs that teach the difference between fact, opinion, misdirection, and lies, as well as research into deepfakes must become a Homeland Security priority.

Finally, our cybersecurity work force lacks diversity, lagging the technology sector by a significant margin. As we build programs to skill and re-skill individuals to address the massive skill shortage, we must put in place the right incentives for diversity. We need new perspectives and a new mental model for how we approach this threat. Our adversaries are agile, creative, and persistent. Our technology landscape is ever-shifting and our tax surface ever-expanding. Preparing for the future requires a new organizational and operating model focused on persistent cooperation and collaboration at cyber speed.

Thank you.

[The prepared statement of Ms. Howe follows:]

PREPARED STATEMENT OF NILOOFAR RAZI HOWE

OCTOBER 22, 2019

Chairman Richmond, Ranking Member Katko, distinguished committee Members, thank you for inviting me to testify on cybersecurity and emerging technologies. I am a senior fellow in the Cybersecurity Initiative at New America, a DC-based nonpartisan think tank, and have spent close to 3 decades in the technology sector, the last 15 years focused on innovation in the National security and cybersecurity sectors. I have been a venture capitalist, an entrepreneur, and a corporate executive in the cybersecurity industry. I am also a member of a number of corporate and Government advisory boards.

OVERVIEW: WHERE WE STAND TODAY

We must rethink our approach to cybersecurity and cyber defense.

We are at an inflection point as enormous technological and societal shifts are converging to reshape the National security landscape and the underpinnings of our democracy. The world is changing dramatically with the speed, scope, and scale of nothing we have ever experienced. New, highly-advanced technology is being adopted at a blinding pace as we digitize business, economic, defense, and social infrastructures. We are embracing cloud computing, autonomous vehicles, small low-orbit satellites with advanced sensor platforms, the internet of things (IOT), drones, distributed ledger technology, augmented and virtual reality. On the horizon we see the emergence of 5G and microsensor proliferation, autonomous weapons (for both military and private use), quantum computing, artificial intelligence, and synthetic biology, to name a few. It's an exciting time, but there are consequences. Over time almost everything that we have experienced in the physical world—prosperity, democracy, corruption, and warfare—will happen digitally but with a speed and severity that we are just starting to comprehend. This isn't about technology alone or

something that takes place in a dark corner of the internet somewhere. It's happening every moment in our offices, our cars, our family rooms, and in our children's pockets. Every device is a supercomputer, every application an attack vector, and with the internet, "every sociopath is now your next door neighbor." This is a defining moment for our society as we face emboldened groups of adversaries with complex motivations creating new social, political, and economic challenges that we are out of position to deal with and almost out of time.

Good cyber hygiene is no longer sufficient as the path forward in the face of increasing sophistication and the volume of threats our society faces. In cyber space, we are certainly in conflict, and many believe we are at war every day. Our adversaries are committed, well-coordinated, persistent, and agile and they are growing in number, especially as we continue to digitize the world, including some of the world's most fragile societies. They are focused on using digital tactics to exploit weaknesses in our technology infrastructures and in our human nature. They are penetrating the seams that exist in society, sometimes for greed, sometimes for power, and sometimes for their National security imperatives.

For decades, our Nation has played a critical global leadership role, providing vision, diplomacy, and stability to further our interests and our allies' interests, and this role is core to the trust and partnership required for a stable society and effective governance at home and around the world. We must do this in the digital world as well. To move us to a world of trustworthy systems and a resilient society, we must reclaim our technology innovation edge and set the standards for our digital infrastructure, which increasingly underpins every aspect of our existence. We must work together—individuals, businesses, innovators, technologists, educators, policy makers, and our Government and military leaders—to define this new world order in cyber space, or at least mitigate the risks that compound with every moment.

And we must move fast.

It took centuries for Gutenberg's invention, the printing press, to fundamentally change society by transforming information sharing and communication. The internet has transformed society on a fundamentally different, faster time line. Today, time is not on our side. Our starting point is a society that is polarized, a political system that is under attack, and a way of life that feels remarkably uncertain and fragile to many Americans. The accelerating pace of technology innovation for the first time in human history is outstripping our ability as humans to adapt, adjust our policies on a time line that is meaningful, and avoid the inevitable widening of the income divide in society that this acceleration will drive. Automation will diminish the importance of labor over time adding to income disparity between the highest earners and the low-wage labor force, reinforcing a belief for many in our society that the future will not be better for them or their children. In fact, an Oxford University study estimates that 47 percent of total U.S. employment is at risk with automation. It is these seams in society that our adversaries are exploiting. They are using cyber space to undermine the very foundation of our democracy. The amplification of polarization as a result of the structure of our technology platforms as well as exploitation of those platforms by our adversaries to sow discord and chaos in society has undermined the effectiveness, stability, and consistency of our Government leaders and policy makers to address these pressing problems and to find common ground to rally around as a society with shared values and a shared vision for the future. Not surprisingly, people's faith and trust in their leaders—government, business, and religious leaders—continues to decline, especially and most alarmingly, among our youth.

We must also move fast because our people and our businesses will not wait for our policy makers to catch up or security to be designed in before they embrace new waves of technology innovation that can bring with them new disruptions to society. IOT, powered by 5G networks, will be embraced by businesses to take advantages of the $11 trillion of economic gain waiting to be captured. Many of these devices are inexpensive and rely on slim profit margins and with little to no regulation or liability they generally lack even the most basic security features we have come to expect in our connected devices. The result is that most IOT devices have known vulnerabilities, and they have already become a key component of adversary attack tactics such as botnets. IOT devices are proliferating in every corner of society from business-to-business applications in manufacturing, agriculture, health care, and transportation to consumer applications such as home automation. As a result, the vulnerabilities of these systems will also proliferate into every aspect of our corporate and personal lives.

The growing market in low-orbit satellites, which gets little airtime from security and privacy experts, threatens to form the most ubiquitous surveillance platform ever built with no meaningful regulation to control what they are used for or by whom. These platforms can now be easily tasked by individuals at low cost with few

limits, regulatory or technical, on what they can be tasked to track or what information they can obtain and sell. The privacy debate, which is a critical corollary to any discussion about cybersecurity, needs to take into account the implications of the 4,000 satellites that are being launched into orbit.

The consequences of the digitization of fragile societies without thought to security ramifications poses a credible security risk both to those societies and possibly to the broader interconnected world. While over half of the world's population is online, many of the people who are now being brought on-line live in some of the world's most chaotic geographies. As these populations get connected via the internet, with few norms to truly govern their behavior or those who seek to destabilize and manipulate them, we must be prepared for new forms of malfeasance and exploitation.

As more money pours into artificial intelligence from governments and technology firms, the ramifications are poised to be immense and by definition beyond what the human brain can comprehend. We can expect every industry and every aspect of society to be impacted by AI. What this impact will be exactly is yet to be fully understood and must be carefully researched and studied at every stage of development.

Our adversaries have repeatedly shown in the past that they can move faster than we do in the United States. We have witnessed how quickly they can adapt and exploit technology while we grapple with emerging technologies, emerging social norms, and a political process that does not function at cyber speed. While we have been studying the problem of cybersecurity, cyber criminals have innovated and adapted. Cyber crime is now an industry, often protected by the governments of the geographies in which the cyber criminals operate, and has quickly grown to be the most lucrative form of crime, overshadowing the global illegal drug trade. The Hacker-Industrial Complex—networks of cyber criminal who crowdsource their tools and share their services—continues to operate with little fear of prosecution or retribution.

Just in the past few years, ransomware, which started out as a troublesome cyber crime issue for petty criminals to extract value from locking down access to data, has grown to represent a National and homeland security issue threatening the very ability of our Government to provide services to its citizens. This past year multiple jurisdictions in the United States were hit with ransomware attacks that crippled municipal services for prolonged periods of time. If this was a testing ground for a new attack vector, these incidents proved the vulnerability of our under-resourced State and local municipalities to ransomware attacks and the potentially disastrous effect on the communities they serve.

Our adversaries over the past 3 years have developed a better understanding of, and therefore improved their use of, social manipulation through the internet. The growth and reliance on social media in the United States has enabled our adversaries, especially Russia and China, to engage in state on individual activities (manipulation) exploit vulnerabilities in our society, amplify polarization, radicalize our youth, and undermine any sense of objective truth in society. By definition, polarized societies are ineffective at governance as there is no common ground to build consensus to enact bipartisan policies, laws, and regulations that benefit all of society. As our ability to govern erodes, so does people's faith in the government leaders and their political system. A recent Pew Research study found that Republicans and Democrats are more divided along ideological lines—and partisan antipathy is deeper and more extensive—than at any point in the last 2 decades. The "middle" has literally disappeared.

Underpinning all of these issues is the fact that human beings have a flawed operating system (OS) that relies on outdated mental models and cognitive biases that perhaps were useful when we lived in caves, surviving attacks from the wild, but do little to help us in the age of technology acceleration or protect us against our increasingly vulnerable digital existence. This flawed human OS sits at the intersection of our networks and devices and continues to be the weak link in our security programs and architecture. For example, 91 percent of all cyber attacks start with a phishing email, which still drives a better response rate than most marketing programs. This flawed human OS is also responsible for developing the policies, laws, and regulations to protect our people and our businesses from harm. The pace at which we have historically developed societal and Government solutions, adapted to new technologies, and built consensus with respect to our most pressing problems is too slow for the age of technology acceleration. It is time to change our perspective and mental model with respect to the time lines we must operate on, the agility with which we take action, and the collaborative model we employ. Our adversaries have.

WHERE WE NEED TO GO

It is critical to put in place the right policies to address our most existential threats in real time. It is time for the United States to set a bold cyber agenda capable of restoring trust globally trust in our technology, trust in our systems, trust in our infrastructure, and through that trust in our political system, our political process, and our leaders. To be effective, our Government will have to do this in partnership across the Government and with the private sector. There is no time for silos or provincialism as we turn into solving an existential crisis for our homeland, for the people, and for the world.

A bold new cyber agenda should include the following elements:

1. Speed and transparency.—The U.S. Government must remove any barriers that prevent Government agencies that have threat and adversary information from sharing that information real-time and with context with the entities that are most affected. Sustained and real-time cooperation and collaboration between all relevant Government agencies and the private sector is the only way to rebuild trust and have a real impact on our adversaries. We now have multiple agencies with unique capabilities to help the private sector, including the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Protection Agency (CISA), United States Cyber Command, the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and sector-specific agencies such as United States Treasury and Department and Energy (DOE) to name a few. Each plays a unique role in the Nation's cybersecurity mission, but only if they are working together and without barriers and provincial turf wars, can we actually change the landscape of cybersecurity for the country. The Russia Small Group, with a clear mandate to protect the 2018 elections, was a tremendous example of what happens when we bring the full power of multiple Government agencies to solve a problem, hand-in-hand with the private sector. We need to rethink our U.S. Government operating model to empower consistent and real-time coordination and collaboration. Many of the authorities for securing our systems were written long before there was a commercial internet. We need take a holistic look at these authorities through the lens of how we can most effectively defend the Nation, our enterprises, and our people, with the goal of enabling effective real-time consistent collaboration and coordination.

2. A relentless focus on unique value drivers and outcomes.—

a. Government's unique role.—Government must do what only the Government can do—deter malfeasance in cyber space, especially by nation-state adversaries, by using our tools of National power against those adversaries who are harming us. The private sector cannot defend itself alone against nation-state adversaries and criminals who are agile, persistent, and creative. Even the strongest walls will eventually succumb to a capable well-funded adversary if there is no deterrence. This is uniquely the Government's role. Peter Singer, a senior fellow at New America, wrote last year about the collapse of cyber deterrence: "Less generously, these trends have created the opposite of deterrence: Incentives. The failure to clearly respond has taught not just Russia, but any other would-be attacker, that such operations are relatively no pain on the cost side, and all gain on the benefits side. Until this calculus is altered, the United States should expect to see not just Russia continue to target its citizens and institutions but also other nations and non-state groups looking for similar gains." Strong deterrence is the cornerstone of any security framework and the U.S. Government must take up this challenge in a decisive way, with a consistent policy and framework for imposing cost on those who do us harm.

b. Private sector's unique expertise.—The private sector has developed deep technical expertise in certain domains and the U.S. Government must leverage the private sector better and not duplicate effort in areas where private-sector capabilities now surpass Government capabilities. In the threat intelligence market, while U.S. intelligence agencies can bring the full power of their capabilities to bear on a selected basis producing unique insights into foreign adversaries, the private sector has advanced capabilities across a broad group of actors (foreign and domestic), including insight into attacker behavior, tactics techniques and procedures (TTPs), and campaigns. Coordinating intelligence between private and public sector to understand adversary behavior and create a coordinated response to defend and defeat the adversary is critical. As we build and invest in Government capabilities, we must be careful not to duplicate or compete with private-sector capabilities.

3. Resilience to ransomware.—Ransomware is no longer just a cyber crime issue. Ransomware at the State and municipal level is a National security and homeland security issue. The single purpose of Government is to provide services (including protection) to its citizens. Ransomware at scale keeps that from happening as we saw in Baltimore, Atlanta, and the State of Texas. A ransomware attack during an election would have devastating affect not just on the election itself, but on people's trust in Government and the validity of our political process. State and municipal administrations need Federal help in the form of standards, grants, developing response plans, and tax incentives to invest in infrastructure that can be resilient to ransomware attacks and making Government systems resilient to ransomware attacks should be a high priority for Congress. It will take a coordinated effort across the whole of Government, but especially DHS CISA, NIST, FBI, and NSA's Cybersecurity Directorate, working hand-in-hand with State and local agencies, to make progress against this real threat and to stay ahead of the adversary.

4. Support secure smart cities.—As a corollary to the ransomware issue, Congress should provide more support to sub-Federal entities to collaborate on smart city modernization projects. Our cities do not have the expertise to defend themselves on their own nor the resources to do it. As our cities become smarter, they must do so with security in mind or these modernizations could unwittingly enable disruption of the Government's core function of providing services and security to its citizens, and given the criticality of municipal services, actually lead to loss of life. As Natasha Cohen and Brian Nussbaum write in their New America report *Smart is not Enough,* "Despite increasing concern from the information security community, it is far from clear that even the smartest of U.S. cities are in a position to deal with the full range of new risks that the technology may bring. The required financial, social, security, operational, legal, and policy innovations needed for smart cities to deliver on their aforementioned promises do not appear to be moving at the pace of innovation of the technology."

5. Commit to regaining our innovation edge.—Government funding of innovation so that the United States can regain its edge in next generation technologies will be critical to ensuring that those technologies and the infrastructure that supports them is secure by design. While venture capitalists invest over $5 billion per year conservatively in cybersecurity companies and technologies, with a myriad of Innovation competitions such as the RSA Conference Innovation Sandbox and Launchpad Competitions held each year during the RSA Conference, which now boasts close to 45,000 attendees each year, private-sector investment is focused on building businesses based on proven technologies and established market demand. That is not where the funding gap exists. The United States must significantly increase (to the tune of multiple of current Federal R&D budgets) its funding in basic and applied research in the areas identified by the U.S. intelligence community such as artificial intelligence, 5G, and quantum computing in order to meet its declared National technology priorities. It is time for the Government to fund a bold innovation agenda that will carry us forward to 2030 and beyond, and commit to regaining our innovation edge in these critical next generation technologies.

6. Fund media literacy programs.—We live in a polarized, hyperconnected world of impatient digital citizens who are being continuously and creatively targeted with misinformation. Developing and funding a media literacy program that teaches individuals how to discern the difference between fact, opinion, misdirection and lies, is critical to a well-functioning society and should be a homeland security priority. IREX, a global development and education organization, developed a *Learn to Discern* education program for the Ukrainian Ministry of Education to combat Russian disinformation campaigns. Their program integrated information consumption skills into existing secondary school curricula and teacher training programs at pre- and in-service teacher training institutes. Working with the non-profit community as well as the private sector, the U.S. Government should fund the development of similar programs and curricula in the United States for our elementary, middle, and high-school students as well as for teacher training. With a broad media literacy campaign, we can build resilience to state-sponsored disinformation campaigns, help individuals recognize divisive narratives and hate speech, and improve our youth's ability to navigate increasingly polluted on-line spaces in a safe and responsible way. As we do this, we must pay close attention to misinformation innovations such as deepfakes, which present a unique challenge, and fund research aimed at identifying and mitigating the threat they pose to the very concept of objective truth.

7. Commit to building a diverse workforce in cybersecurity.—The Government is in a unique position to contribute and commit to purposefully reducing the skills shortage in the cybersecurity industry. While there are some great programs in place, including DHS's CyberPatriot competition, CyberCorps Scholarship for Service initiative, and the April 2019 Executive Order focused on reskilling and upskilling Federal employees, more needs to be done to recruit individuals from outside our typical skill sets (IT, law enforcement, and military) with a clear mandate of solving the diversity gap in the industry. The cybersecurity workforce today significantly lags behind the broader technology industry in terms of diversity and to solve our skills shortage we need all of society to be inspired by the mission to reclaim cyber space for good. Elizebeth Friedman, one of the most prolific codebreakers in U.S. history had no background or training in mathematics or linguistics and yet was able to break any code in any language during and after World War II. We need to inspire a new generation of Elizebeth Friedmans to consider a career in cyber. There are a number of good examples of reskilling efforts in both the public and private sector. The U.K. Cyber Retraining Academy is an effort by the U.K. government in partnership with the SANS Institute to reskill individuals with high natural aptitude, but no formal cyber background, to enroll in an intensive 10-week program preparing them for a career in cybersecurity. Google launched Google IT Support Professional Certification under its Grow with Google initiative through Coursera, offering a way for anyone from any educational background to get a start in the IT field where the average starting salary for IT support is $52,000 per year. The Homeland Security Act of 2002 envisioned the creation of a National Emergency Tech Guard program, a corps of volunteers whose training is funded by the Government and who can be deployed during periods of crisis to restore critical systems and services to their communities. Policy makers should support, fund, expand, and incentivize similar initiatives with a mandate of driving diversity in the industry. This commitment would not only help solve the industry's skills shortage, bolster our resilience during times of crisis, but would help address the "digital divide" of the haves and the have nots in our society. As we look to the future we will have to ultimately commit to completely rebuilding our digital infrastructure, cities, and nations to face the digital and social challenges of 2030 and beyond. Investment in building the talent base in the right way to tackle this challenge is a necessity for success.

8. Judicious implementation of regulation.—Regulation must be pursued in a focused and purposeful manner with a willingness to adjust and adapt as we evolve, as technology evolves and as our adversaries evolve. With those guiding principles, we should enact regulation targeted at very specific areas where we can have measurable impact.

a. Setting minimum Security Standards for IOT is critical.—Congress should enact basic regulation with respect to IOT. The U.S. Government can help protect the 5G ecosystem of billions of connected devices by setting basic security standards, requiring features such as auto update, and importantly providing the right incentives, including tax incentives for vendors to implement these standards and corporations (including critical infrastructure) to deploy secure products and the financial headroom and reason to make changes.

b. It is time to enact regulations on big data and social platforms.—The aim is not to regulate "Big Tech" but rather those technology platforms that facilitate communications and propaganda networks, exploit human weakness for profit, are addictive by design, reward virality, not veracity, thereby enabling destructive and chaotic social manipulation by our adversaries, without providing clear benefits to their users that outweighs these costs. These social platforms have demonstrated an unwillingness to self-regulate or put the interests of their consumers or society at large ahead of their profit motivation. The scope of harm they have caused society includes not only the amplification of polarization, but also psychological harm as the amount of stress, anxiety, and depression caused by their platforms is on the rise in society and especially with our youth. They are out of time.

CONCLUSION

All of the recommendations outlined above are intended to support empowering a society that is resilient to the unintended consequences of technology innovation and the inevitable exploitation and use of those technologies by adversaries to gain some form of advantage. This may only be a starting point of a long journey. If our ultimate goal is defending our Nation by defeating our adversaries in cyber space

rather than accommodating them, then, in addition to establishing acceptable norms of behavior, developing and committing to a consistent policy of engagement, escalation and deterrence, we must have a working model for successful public-private collaboration and engagement. Defeating our adversaries presupposes our ability to harness the vast technical expertise and resources as well as the unique authorities of the Federal Government, the vast technical expertise and agility of the private sector, a collaborative intelligence gathering and sharing framework, and coordinated response planning. It presupposes a society where trust exists between the private sector and the public sector, where transparency and fact-based substantive conversation, discussion, and communication are the norm.

We have a long way to go, time is not on our side, but we have not yet run out of time.

Mr. RICHMOND. Thank you, Ms. Howe, for your testimony.

I now recognize Dr. Buchanan to summarize his opening statement for 5 minutes. Thank you.

STATEMENT OF BEN BUCHANAN, PH D, SENIOR FACULTY FELLOW, CENTER FOR SECURITY AND EMERGING TECHNOLOGY, MORTARA CENTER, ASSISTANT TEACHING PROFESSOR, GEORGETOWN UNIVERSITY

Mr. BUCHANAN. Thank you, Chairman Richmond, Chairman Thompson, and Ranking Member Katko, for holding this important hearing and for inviting me to testify.

My name is Ben Buchanan. I am an assistant teaching professor at the School of Foreign Service, and the senior faculty fellow at the Center for Security and Emerging Technology, both at Georgetown University. I am also a global fellow at the Woodrow Wilson Center for Scholars, where I teach introductory classes on artificial intelligence and cybersecurity for Congressional staff. My research specialty is examining how cybersecurity and AI shape international security. In this vein I co-authored recently a paper entitled, "Machine Learning for Policymakers."

I will confine my opening remarks to the impact of AI on cybersecurity, since I think it is the emerging technology poised to have the most significant effect in this area. While there is an enormous amount of hype and debate around AI in general, the intersection of AI and cybersecurity is understudied and underappreciated. At least 3 dimensions of this problem deserve our analysis.

First and most significant is the cybersecurity of AI systems themselves. AI systems are just as likely to be susceptible to the kinds of software vulnerabilities that are present in other kinds of computer code. As we have seen for decades, hackers can exploit these vulnerabilities for their own ends. There is no reason to think that hackers will not try to do the same to AI systems, and there is no reason to think that they will not, at times, succeed. This possibility is particularly worrying, given the high stakes of some AI applications. This is not a reason to avoid using AI, but vigilance is imperative in order to improve cyber and National security.

Yet to stop our analysis at just the traditional kinds of software vulnerabilities is to miss a great deal of the cybersecurity risk that AI systems pose. The neural network architecture that underpins a lot of modern AI is immensely powerful, but presents new classes of cybersecurity risk that we are only beginning to uncover and understand. We call this field adversarial learning.

Using adversarial learning hackers can cause neural networks to make bizarre errors, causing systems that rely on those networks

to fail or reveal confidential information. This is a field that requires a great deal more attention. A tiny fraction of the research in AI today goes to studying AI security and the risks of adversarial learning.

Our second area of analysis is that AI can change traditional offensive cyber attacks against regular computer systems. Modern hackers in many cases do not need AI to achieve their ends. That said, I think it is noteworthy that some of the most potent cyber attacks we have seen, including last decade's Stuxnet, the 2006 black—2016 blackout in Ukraine, and the 2017 attack now is NotPetya, which caused $10 billion in damage, feature some forms of automation within them.

I can imagine a world in which future cyber operations will use more sophisticated automated capabilities to achieve particular tasks such as vulnerability discovery, target selection, command and control, and attack execution. Mr. Knake mentioned the kill chain earlier, and suffice it to say that I think almost every aspect of the kill chain could be transformed by more powerful automated capabilities.

I suspect that such automation could offer significant upsides to sophisticated hackers faced with complex targets and complex missions. In some respects, the possible upside to automation in attack is higher in the area of cyber operations than in physical warfare, since whether a plane is operated by a human or a machine, the laws of physics still apply. But it is likely that automated cyber capabilities, if sophisticated enough, could operate much faster than their human-directed counterparts. I stress, however, we have not seen this come to fruition yet.

This leads to the third area of analysis, the possibility that AI might help on cyber defense. This idea is also the subject of a lot of hype and a lot of investment. There seems to be discreet ways in which AI can indeed help secure computer systems, both in discovering vulnerabilities before hackers do, and also in detecting the presence of malicious code.

However, we must be careful not to let the hype outrun the reality on this front. In evaluating cybersecurity advances in this area, we should compare them to the baseline of technologies we already use, many of which already involve automation, and understand how, if at all, automation in our modern paradigm of machine learning actually improves our defenses. I do believe that AI-enabled tools are likely to be a fundamental part of modern and future cyber offense and defense. The scale, size, and speed of cyber operations will make this inevitable. It is imperative that we keep up with changing times.

That said, we must not forget that cyber operations, no matter how sophisticated, are still fundamentally human operations. For as much as we will talk about technology today, we must remember that the people in our organizations, including Government, are key to addressing these threats.

I look forward to your questions.

[The prepared statement of Mr. Buchanan follows:]

PREPARED STATEMENT OF BEN BUCHANAN

Thank you, Chairman Richmond and Ranking Member Katko, for holding this important hearing and for inviting me to testify.

My name is Ben Buchanan. I am an assistant teaching professor at the School of Foreign Service and a senior faculty fellow at the Center for Security and Emerging Technology, both at Georgetown University. I am also a global fellow at the Woodrow Wilson International Center for Scholars, where I teach introductory classes on artificial intelligence and cybersecurity for Congressional staff. My research specialty is examining how cybersecurity and AI shape international security.—I coauthored a paper entitled "Machine Learning for Policymakers."[1]

I will confine my opening remarks to the impact of artificial intelligence on cybersecurity, since I think it is the emerging technology poised to have the most significant effect in this area. While there is an enormous amount of hype and debate around AI in general, the intersection of AI and cybersecurity is understudied and underappreciated.

At least 3 dimensions of this problem deserve analysis:

First and most significant is the cybersecurity of AI systems themselves. AI systems are just as likely to be susceptible to the kinds of software vulnerabilities that are present in other kinds of computer code. As we have seen for decades, hackers can exploit these vulnerabilities for their own ends. There is no reason to think that hackers will not try to do the same to AI systems, and there is no reason to think that they will not at times succeed. This possibility is particularly worrying given the high stakes of some AI applications; it is not a reason to avoid using AI, but vigilance is imperative to preserve cybersecurity.

But to stop our analysis at just the traditional kinds of software vulnerabilities is to miss a great deal of the cybersecurity risk that AI systems pose. The neural network architecture that underpins a lot of modern AI is immensely powerful but presents a new class of cybersecurity risks that we are only beginning to uncover. We call this field adversarial learning.

Using adversarial learning, hackers can cause neural networks to make bizarre errors, causing systems that rely on those networks to fail or to reveal confidential information. This is a field that requires a great deal more attention.

Second, AI can also change traditional offensive cyber attacks against regular computer systems. Modern hackers in many cases do not need artificial intelligence to achieve their ends. That said, I think it is noteworthy that some of the most potent cyber attacks we have seen—including Stuxnet, the 2016 blackout in Ukraine, and the 2017 attack known as NotPetya that caused at least $10 billion in damage—feature some forms of automated propagation and attack capability. I can imagine a world in which future cyber operations will use more sophisticated automated capabilities to achieve particular tasks, such as vulnerability discovery, target selection, command and control, and attack execution.

I suspect that such automation could offer significant upsides to sophisticated hackers faced with complex targets. In some respects, the possible upside to automation is higher in this area than in physical warfare; whether a plane is operated by a person or a human, the laws of physics still apply, but it is likely that automated cyber capabilities—if sophisticated enough—could operate much faster than their human-directed counterparts. I stress, however, that we have not seen this come to fruition yet.

This leads to the third area of analysis: The possibility that AI might help on cyber defense. This idea is also the subject of a lot of hype and a lot of venture capital investment. There seem to be discrete ways in which AI can indeed help secure computer systems, both in discovering vulnerabilities before hackers do and also in detecting the presence of malicious code. However, we must be careful not to let the hype outrun the reality on this front. In evaluating cybersecurity advances in this area, we should be careful to compare them to the baseline of technologies we already use—many of which already involve automation—and understand how, if at all, artificial intelligence improves our defenses.

I do believe that AI-enabled tools are likely to be a fundamental part of modern and future cyber defense; the scale, size, and speed of cyber operations will make this inevitable, and it is imperative that we develop these tools. That said, we must not forget that cyber operations, no matter how sophisticated, are still fundamentally human operations. For as much as we will talk about technology today, we

[1] Buchanan, Ben and Taylor Miller. "Machine Learning for Policymakers." *Belfer Center for Science and International Affairs* (2017), *https://www.belfercenter.org/sites/default/files/files/publication/MachineLearningforPolicymakers.pdf.*

must remember that the people in our organizations are key to addressing these threats.

I look forward to your questions.

Mr. RICHMOND. Thank you. Thank you for your testimony. I will now recognize myself for 5 minutes to ask questions.

Let me just start with some of the things that you all talked about. Mr. Knake, you mentioned that there are examples where governments set the objectives or goals. Can you give me some of those, and your train of thought on how governments should do it, or what the goals should be?

Mr. KNAKE. Yes, Mr. Chairman. The analogy that I like to use in this space is how we handle oil spills.

We all remember the *Exxon Valdez* oil spill in 1989. In 1990, Congress passed bipartisan legislation, the Oil Pollution Act. What that act said was that, if you are going to bring oil into U.S. waters, you need to have insurance that would cover the full cost of cleaning up a loss of containment from that vessel. So the important thing that that act did is, it didn't say, "Here are the requirements for safety of your vessels, here is what you must do," it said you will own the cost. The polluter will pay.

Well, I think we can adapt that model very easily to areas like data spills. Treat data spills like oil spills. If you want to hold 140 million records of U.S. citizen data, then you probably should have to have an insurance bond that would pay out on the order of—back of the envelope math would suggest about a $1,000 per record. That would require the insurance industry to be able to measure risk in a way that they cannot measure today, and to measure security in a way they cannot measure today.

But I am quite confident that, from that point on, markets would be able to adopt new strategies to be able to price that risk and enforce it, so they wouldn't have to pay out that kind of insurance payment.

Mr. RICHMOND. Part of my thinking—and you mentioned Atlanta in your testimony, and other places—part of my concern—and I will pick a fictional place so that I don't offend any community, but let's think of Mayberry, North Carolina, where Barney Fife was the sheriff's deputy.

[Laughter.]

Mr. RICHMOND. It is made up.

So how do we ensure that they are up with the times in terms of protecting their data, and their cyber hygiene, and all of those things? How do we get them to where they need to be?

Mr. KNAKE. This is a very unpopular opinion, Mr. Chairman. The first thing I would do is I would ban ransomware payments.

What we are doing at this point is handing hundreds of millions of dollars over to our adversaries. They are taking that money. They are spending some of it on Lamborghinis and leather jackets. The rest of the money they are reinvesting to up their capabilities. They are growing more sophisticated. They are building larger teams. They started out doing ransomware against individuals. They are now doing hospital systems and local governments. It is only a matter of time before they do the power grid. So from that perspective, we have got to stop funding them.

Mr. RICHMOND. Let me stop asking you questions.

[Laughter.]

Mr. RICHMOND. Ms. Howe, you mentioned autonomous weapons. What is out there when you speak of that?

Ms. HOWE. Today the technology exists to have completely autonomous weapons. They are available, both for the military and also for private use, where you can set up sniper rifles to take down targets from great distances with very little human intervention. That exists out there, and when they are networked it creates an interesting dilemma, from a security perspective.

Mr. RICHMOND. Thank you. Mr. Durbin, you mentioned stalker apps, or stalker—tell me how they—how it will get on a Member's phone or one of the panelists' phone.

Mr. DURBIN. Stalkerware is considered malicious software. Like most threats and malicious software packages, there are—there is no difference in how they would end up on a device.

So, like a phishing exercise, where you get an email and you are asked to click on a link that could execute a program to load it in, or even—you could do it via text. If since stalkerware in—sometimes involves somebody that the stalker knows, if they have physical access to the phone, then they would be able to, obviously, grab it and loaded it on. So it is like typical threats. You can be tricked into having that, the software load.

Mr. RICHMOND. OK. I would imagine that you all sell software to detect it.

Mr. DURBIN. Yes, we do.

Mr. RICHMOND. OK. With that I will recognize the Ranking Member of the subcommittee, Mr. Katko, for 5 minutes.

Mr. KATKO. Thank you, Mr. Chairman. Ms. Howe, during your testimony—well, all of you talked about the various threats that are out there, and I really, truly believe we are constantly playing catch-up, and that is a concern.

But Ms. Howe, you mentioned that we need to study—we, being the Government—need to set a bold cyber agenda. Could you just drill down a little more and tell me what you envision would be good for us to do?

Ms. HOWE. Well, certainly, sir. Thank you for the question.

From the outset, I think the Government—there are things only the Government can do that would have a tremendous impact on the threat landscape.

Having a consistent cyber deterrence policy that imposes costs on the adversary is a great starting point. It is unfair to expect companies to be able to defend themselves against nation-state adversaries who are committed. We have done that in the past. We certainly wouldn't do that in the kinetic world, but we are doing that in the cyber world, where we expect companies to defend themselves.

We also have to—some of the authorities that were written for defending our most critical systems were written before there was a commercial internet. As we take a holistic look and see what is happening in the dynamics of the market, we have to be willing to re-examine how we operate as a Government, the authorities and capabilities mismatch that we all talk about, and how we organize and how we collaborate at cyber speed.

Mr. KATKO. All right, thank you very much.

Mr. BUCHANAN. You talked about a human element factor. You know, one common theme that I believe in is that, with emerging technologies and threats the way they are, the human element remains critical to the functionality of the attacks. So how do we make the human element of attacks less effective with emergent technologies? Or can we?

Mr. BUCHANAN. Well, I think, again, as much as we talk about technology, it is important to recognize that, both on offense and defense, there are humans involved. One of the things I worry about quite a bit, as someone who teaches students who often go into Government, is the capacity to educate future policy makers and policy advisers to have Government-hiring authorities to bring people into Government so they can serve in this mission set on offense and on defense.

As you can imagine, relating to compensation and other factors, often times many of these individuals go to the private sector and don't end up in Government working on these important missions.

Mr. KATKO. Thank you. Here is a question for everyone here.

Mr. Durbin, we can start with you. It is about quantum computing. In my home town, Syracuse, New York, they have a robust quantum computing research operation under way. But it is, of course, not the only one in the country. I am vitally concerned about quantum computing in that—one of you said that if China gets it, basically, we are in big trouble. It should be something that we prioritize better than we are right now.

I just want to, should we—just—it is a softball question, but it is—I want to hear what your answers are.

Should we be making more of a concerted effort to develop our quantum capabilities on the Government level, given how much of an advantage fully-functional quantum computing can provide?

Mr. DURBIN. Yes, it is a serious threat. It is coming. The time frames are very debatable, but the time to come up with defenses are now, not when somebody does have the first functional working quantum computer.

The algorithms that are used right—or the encryption rhythms for protecting data right now will not be sufficient with quantum, so we need to come up with the new problem that is hard for a quantum computer to solve.

I am encouraged with the attention that NIST has been giving this topic, and so I encourage them to keep going with the research that they are doing.

But yes, it is coming, and focus needs to be brought to bear.

Mr. KATKO. Yes, it seems to me that there is a bit—it is a bit diffused, the projects, and there is not, like, a centralization, if you will, of the—their overall goal. I mean, I view this as a modern-day moonshot, because if we—if the Chinese get it before us, then we really—our encryption data is—or our encryption capabilities are going to be severely hampered. We are already vulnerable, as it is.

So Mr.—as you say, Knake—is that how you say it, or Knake? Yes. Well, what can we do, as a Government, from a prioritization standpoint?

To me, it seems to me that we need to do more to make this a high priority within Government. It is not something that people

can see and feel like the moonshot, if you will. But it is something that is critically important to us, going forward. How do we get the Government to prioritize this more?

Mr. KNAKE. So I think the way that I would approach this problem is to say that we need to focus on it with the same energy and, really, the same level of resources as we would maybe a Manhattan project or a moonshot, but we need to harness the capabilities within our private sector. So instead of having one large Manhattan Project out in the Southwest desert, in this case we need to have dozens, if not hundreds, of companies working on various aspects of it. There are models for how we have done this in the past. I would call on SpaceX as a good example of a commercial-supported endeavor.

But I think the key here is more research going to more teams to compete globally, and hope that one of those teams that is going to win is going to be a U.S.-based team. I think we can't really put all our eggs either in the hope that Silicon Valley is going to solve this problem for us, or that a Government research team singly funded and focused is going to beat the Chinese, who I view as the major adversary in this space.

Mr. KATKO. Thank you all. I wish I had more time to ask you a ton of questions, but I have to—I am out of time. I yield back.

Mr. RICHMOND. The gentleman yields back. The Chairman of the full committee, Mr. Thompson, is recognized for 5 minutes.

Mr. THOMPSON. Thank you very much, Mr. Richmond. As I heard the witnesses' testimony today, I became very suspect of something I can't do without. But the challenge for this committee and Members of Congress is how do we not overreact to a problem, so that Government, all of a sudden, is stifling innovation and a lot of other things with regulation.

So—and one of the reasons hearings like this are held is to try to get the benefit of the talent that is out here, especially in the private sector. Some of us believe that there is a role for Government, but it is to encourage the development of the technologies and things that we need, while understanding that it is really the private sector and its talents that ultimately will get us to where we need to be.

So—but a couple of things I heard. One is right now we are kind-of reacting to the problem, rather than getting ahead of it. Can you suggest a way forward for us to wait until the next attack occurs, in anticipation of whatever that is, that we could do, as Members of Congress, to get us to that point?

Mr. Durbin, if you can, get us started with some idea.

Mr. DURBIN. It is tempting to react to the buzz word, what people are talking about in the press, like the deepfakes. I encourage that we also have to keep our eye on the threats that have been plaguing us for a long time.

Email, for example, still tends to be the No. 1 threat vector out there that attackers use to do their malicious things. As soon as a bad guy figures out a way to utilize email, then companies like ourselves, we counter it. Then they come up with a new clever way. So we can always be prepared for what is coming by focusing on what is tried and true, and what we know that the adversaries aren't going to back away from.

Ransomware. Today I talked about targeted ransomware. This is the first time since we have been tracking it where the shift has moved to the enterprise versus the individual. Why are they doing that? They are doing that because, when you target somebody and you really understand their network, you can get in there, get in there deep, compromise as many assets as possible, launch it at the same time, and it puts pressure on that company: "We better pay the ransom, because we are tied up."

So solving ransomware will help you to solve the next iteration, the next usage of it, and it is a way to kind-of stay ahead of the curve.

Mr. THOMPSON. Mr. Knake.

Mr. KNAKE. Thank you, Mr. Chairman. I would focus on 3 brief ideas.

No. 1, I think we need to have a much higher degree of disclosure of cyber incidents. We really don't have a clear picture of how badly we are owned by Chinese or Russian or other adversaries. Companies tend to try and avoid disclosing publicly what has happened. So, on the one hand, we have the number that General Alexander has put out, which I believe to be accurate, of possibly as high as $400 billion in loss from economic espionage by the Chinese, but we have very few cases where we actually know of public incidents where that loss has happened. That puts investors at a disadvantage, it puts stakeholders at a disadvantage, and it keeps markets from inflicting pain on companies that don't have good security.

With that, I would highly recommend the idea of creating one or more National Transportation Safety Board-like mechanisms to dig in and understand why these incidents happen once they are disclosed, so those lessons learned can get pushed out to the broader ecosystem.

Finally, I think this is all about creating collaboration, defensive collaboration with Government and with the private sector. Today we don't have the system that we need to be able to do that to trust the end-users and to trust the systems over which information is shared. So that is why I have advocated for extending Classified connectivity out to critical infrastructure companies beyond the defense industrial base. I think that is essential.

Mr. THOMPSON. Thank you.

Ms. Howe.

Ms. HOWE. Chairman Thompson, you are exactly right that the attack surface is ever-shifting, the landscape moves on us, and the most important thing we can do is put in place a collaborative process that can be as agile as the threat landscape and as our adversaries are.

We have had great examples of this. The Russia Small Group, which was—had a very specific goal of protecting the 2018 midterm elections, did their job. They did it. It was Cyber Command, NSA, FBI, DHS, working together with private sector. The Enduring Security framework was another example of this collaboration working.

If we could systematize that kind of collaboration so that, no matter how our adversary adapts, no matter how our technology evolves, we can be as agile as they are—I don't think we can pre-

dict with precision how these attacks will take place in the future, but if we organize the right way, we can make a difference.

The other thing I would put out there is today we want to have resilience and protect ourselves. The boldest thing we can do is to decide to defeat the adversary in cyber space, and to organize to actually defeat the adversary. That is something we are absolutely capable of doing. It takes a lot of resolve to do. But again, working society, Government, hand-in-hand with trust between the two, we can accomplish that.

Mr. THOMPSON. Dr. Buchanan.

Mr. BUCHANAN. Just in terms of concrete ideas, I think we need to do a lot more study of the cybersecurity vulnerabilities of emerging systems, ideally, before we employ them. This is something we, in many cases, did not do with old cyber systems. The good news, I think, is that the Government does have some capacity to do this that we could use as a foundation. I am thinking in particular of NIST, National Institute of Standards and Technology, which has very small effort, but a promising one, to study weaknesses in artificial intelligence systems.

It seems to me that would be something that is ripe for expansion, where we could study the problems that many in the private sector, because of market interests, are not studying, but that will be quite impactful for broader society if they were to be targeted by adversaries.

Mr. THOMPSON. Thank you very much. I ask the Chair—I have some follow-up questions we will submit to the witnesses in writing along this line. But I thank you very much.

Mr. RICHMOND. The gentleman yields back. The gentleman from North Carolina, Mr. Walker, is recognized for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman.

Dr. Buchanan, I would like to stay with you, if I could, please. In August, President Trump announced a rule restricting Government agencies from doing business with the Chinese telecommunications company Huawei due to National security threats. What was our exposure to Huawei when the decision was reached?

Mr. BUCHANAN. Congressman, I don't know that I am in a position to judge U.S. Government's exposure to Huawei.

I would imagine that what would concern me most would be exposure in Classified networks, and I am in no position to have visibility into that.

Mr. WALKER. So you don't necessarily have anything that is confirmed, but you do have some concerns. Is that fair to say, without having to get into detail?

Mr. BUCHANAN. Sure. I think it is fair to say that telecommunications systems provide enormous access to the information and broader networks of which they are a part. In general, I worry about that as a significant threat, and——

Mr. WALKER. Yes. Not everybody on the panel—technology still is an issue for, I am realizing, but that is a different story.

[Laughter.]

Mr. WALKER. What has changed in the agency's contract acquisition since the ban, such as the type of contract signed, or how contractors are chosen?

Mr. BUCHANAN. Again, I am not sure I have visibility into the contracting processes.

Mr. WALKER. OK, all right. So maybe my final question for you, then, may be the same thing. Are there alternatives to the covered ban telecom companies such as Huawei routers and other companies' data networks, or have agencies been struggling to fill their tasks because of the ban? Can you address that?

Mr. BUCHANAN. Yes. Speaking generally, there is—there are other players in the telecommunications market. I think it is a smaller market than we would like. Huawei has a price advantage, why they are attractive, but they are not the only supplier in the world.

Mr. WALKER. OK. Do you see that changing in the foreseeable future, as far as these smaller companies having a little bit more access, or a little bit more stronger foothold?

Mr. BUCHANAN. I think it is fair to say that I worry generally about competition in this space, because there are not that many players.

Mr. WALKER. OK.

Mr. BUCHANAN. Yes. So, in general, I think there is reason why we would want more competition than we have right now, and particularly we might want more U.S. companies involved than is currently the case.

Mr. WALKER. Thanks. I appreciate you going there.

Mr.—I believe it is Knake, is that correct? In your testimony you mentioned that in a race—and this struck me a little bit—in a race between Silicon Valley and China, I believe you said Silicon Valley would lose in respect to these emerging technologies. Is that correct? I am going to come back with a question. I just want to make sure I heard that correct. Right? Is that fair?

Mr. KNAKE. Yes, I think it is fair.

Mr. WALKER. All right. There is no question that Huawei, in circumventing—is circumventing the U.S. export ban and experiencing success in becoming self-sufficient.

So my question is this. If China becomes totally self-reliant in these technologies, such as the production of their own advanced chips, what impact do you think that is going to have on the U.S. economy 5, 10, 50 years down the road?

Mr. KNAKE. So I am in a minority within the international relations community on this topic. But what I think is going to happen is we are largely going to see a split of the internet into 1, 2, or 3 parts, and with it a split of the underlying technologies, so that we are unlikely to see a situation barring massive political change in China, in which U.S. companies are able to compete there for that market.

Therefore, I don't think we are going to continue to allow China to compete in our market. So I think we are going to have very different technology development and very different paths.

Mr. WALKER. Well, you just—you answered the second question, as far as, if there have—if they have the largest R&D funding in the sector, how would we expect companies in the United States to compete with the Chinese government-backed company from dominating the telecom market? You just answered that. It looks like it is going to be two independent sectors here.

Mr. KNAKE. Yes, sir. I would say that I think that there is a—it is almost a dirty word within policy communities in Washington, but it is time that we re-look at the concept of industrial policy.

How are we going to assure that 6G, however we decide to define that, is something that the United States can compete in, and isn't going to fall behind these other actors?

Choices were made by leading telecommunications firms in the United States not to compete in this space. That clearly was not in our National security interest. So we have got to find ways to make sure they choose to compete in the next generation.

Mr. WALKER. A lot of my questions, a lot of the focus in the media and National security is on Huawei, but there are other companies that should cause major concern, as well, for the U.S. National security. Do you agree with that?

Mr. KNAKE. Absolutely.

Mr. WALKER. Especially in the emerging technologies.

In my closing few seconds, what should be done, in your opinion, to prevent these companies from posing a security risk, specifically, obviously, in our country?

Mr. KNAKE. So I think one of the things that we need to look at, which is, again, a very unpopular opinion, is can we maintain global supply chains, or do we need to have trusted supply chains by trusting companies that are either manufactured in the United States or by our allies?

Can we trust chips and devices and components that are manufactured abroad for critical systems?

Mr. WALKER. Thank you for your testimony. I yield back, Mr. Chairman.

Mr. RICHMOND. The gentleman from North Carolina yields back. The gentleman from Rhode Island, Mr. Langevin, is recognized for 5 minutes.

Mr. LANGEVIN. Thank you.

[Pause.]

Mr. LANGEVIN. Is that better? OK. Here we go.

I just want to thank our panel of witnesses for your testimony today, and your contributions to raising our National security awareness, and providing steps forward to how we better protect the country in cyber.

Mr. Knake, I would—first of all, I am not going to get into this question, but on the issue of—be able to discuss industrial policy, I couldn't agree with you more. We need to make sure that we can do that, and take the politics out of it, and really focus on the issue at hand. So I agree on that point.

So this is a question, and it actually—one other point I want to make is how I completely would agree with you on what you talked about in terms of critical thinking. You know, this issue of our adversaries using our values and our commitment of free speech and using these social media platforms as weapons against us and undermining our democracy is something that I have worried about for a long time.

Being able to think critically when you talk about media and issues that are raised, if the public can't do that, we are already losing. We need to build that resilience into our democracy, and

that starts with our kids, and teaching civics in class, and also doing things like critical thinking.

But this question is for all witnesses, and I would like to start with Mr. Knake. In your collective testimony you all focused on—significant attention on new tactics and techniques to achieve malign cyber goals. You do not, though, to a large extent focus on threat actors.

So do you believe that the cyber threat actor environment is likely to remain largely static in the coming years, with major challenges coming from China, Russia, North Korea, and Iran, and lesser problems from organized crime and other non-state actors? Or are we likely to see major shifts?

Mr. KNAKE. Thank you, Congressman. I would say that, from a nation-state perspective, the threats are largely determined by the geopolitics and the ability for any nation-state to rapidly acquire offensive cyber capability. It means that any of our adversaries are likely to confront us in cyber space if they deem it in their interests.

You touched on organized crime. I think we are at the point where organized crime in cyber space really represents a danger, and a National security danger, a National security threat. The capabilities are only growing. Their interests in generating financial revenue are moving them out of purely the cyber realm and into the physical realm. So we have hybrid threats emerging from these criminal groups. They are operating out of safe havens. I think that they are, like the drug cartels in the 1990's, ever much a National security threat as certain nation-states.

Mr. LANGEVIN. How about in terms of mitigating our risk? How much would you focus on responding to threat actors vice (sic) technological steps that we can take to protect ourselves from emerging threats?

Mr. KNAKE. What I have advocated is that there is a limited amount we can do to threat actors.

I certainly agree with Ms. Howe that we want to engage them everywhere we can and in every way that we can. But really, our National strategy needs to be about building resilience. We need to be able to have most attacks bounce off of our infrastructure, and we need to be able to bounce back rapidly, should those protections fail. That kind of strategy, I think, is really in our National interest. That is where we want to focus on incentives and aligning technology around those incentives.

Mr. LANGEVIN. Thank you, Mr. Durbin, in your written testimony you make reference to something that we have been focusing a great deal on right now, and that is risk posed to ever-expanding supply chains, and the various accesses that they provide to networks. Can you expound upon the growth that you have seen in this type of threat?

To our other witnesses, do you believe that intrusions through the supply chain will continue to rise in the future?

Given that malicious actors often use software update mechanisms when attacking through supply chain, are you concerned that an uptick in supply chain attacks could actually undermine faith in this important hygiene measure?

Mr. DURBIN. So the supply chain is attractive because, if your main target has a sufficient enough cybersecurity budget, and has taken the—done the due diligence to protect themselves, instead of spending your resources trying to penetrate them, let's go down the supply chain and look for someone who is less diligent, attack there, and try to feed the attack back upstream into the main target. So that is always going to be an attractive vector that we are going to have to stay diligent with.

I think the—using the supply chain and compromising software download sites and software patching sites is also going to be very attractive, because you are able to reach a large number of people, and you are doing it in a way where the victim thinks that they are interacting with a trusted site. So you are not going to be as cognizant, or you are not could be as concerned or suspicious. So it can be a very powerful threat vector.

Mr. LANGEVIN. Thank you. I know my time has expired. Thank you, Mr. Chairman. I yield back.

Mr. RICHMOND. The gentleman from Rhode Island yields back. The gentleman, Mr. Taylor, is recognized for 5 minutes.

Mr. TAYLOR. Thank you, Mr. Chairman. I appreciate this hearing.

In 2017 I carried the cybersecurity package for the State of Texas, for the Texas legislature. In that package the attorney general of Texas asked for a limited defense of prosecution in the event that he wanted to take down a human trafficking website. So he would take down a human trafficking gang. The website with the victims' pictures would still be left on the internet. He wanted the ability to conduct a denial-of-service attack against that site to take it down and to eliminate that site on the internet.

So that takes me to my question, my line of questioning, which is around offensive operations against cyber predators. Right?

So we have got people out there that are conducting cyber attacks in the United States, whether it is denial-of-service, whether it is ransomware, et cetera. This is thorny legal ground.

But I was just wondering, since we have some really smart people in the room, what are your thoughts on conducting offensive operations against those that are actually conducting attacks on us when—retaliating, in effect, doing a ransomware attack on people that are doing ransomware attacks on us? I will let you go in order.

Mr. Durbin, do you want to——

Mr. DURBIN. So there are a few issues.

First is attribution. The attacker can hide who they really are. So it may appear as that they are coming from a hospital overseas, and then you are going to go attack this hospital that was innocent. If you do identify the correct attacker, and you attack them, you risk escalation, because they may come back at us again.

But I think one thing that we often overlook, traditional warfare, if you throw a hand grenade at somebody, it blows up. They can't pick it up and throw it back at you. If we launch an attack, we are basically giving them that software that they can re-engineer and use against us, or use against others.

I think there is a way to use a deterrence, maybe the threat of it, or to demonstrate what we could do. But I think hack attacks, or attack-backs are delicate.

Mr. TAYLOR. Mr. Knake.

Mr. KNAKE. Thank you, Congressman. I would say that I am all in favor of Cyber Command taking a more active role in defense of private industry and State and local government. I think that the idea of other entities than Cyber Command carrying out that offensive operation is scary and could put us into situations that we don't want to be in.

But I do think, if we had the kind of capability where, for instance, a critical infrastructure company that was involved in a threat from a overseas actor was able to communicate that in real time with high assurance, with trust among the parties over a Classified network, that then Cyber Command could essentially be tipped off to that activity and target to shut it down.

So we really just need tighter collaboration, rather than kind-of a go-it-alone approach by private companies. I think that is possible.

Mr. TAYLOR. While I have got you, just one quick thing. You said you want to see greater clarity in cyber attacks. The problem that we have grappled with on this subcommittee is that, if we tell people where the attacks are, or what the effect—we are basically saying, hey, there is a vulnerability here.

So, I mean, I appreciate the desire for transparency. I am for that. But then—but in this particular instance, if I give you transparency, I am basically telling you where you can attack me.

Do you want to just quickly respond on that, and I will go back to the offensive question here with Ms. Howe?

Mr. KNAKE. Yes, I think there is two pieces to it. I think, No. 1, the adversary has already exploited the vulnerability if they have created the incident. So, from that point of view, you are not going to be sharing information, assuming that you have patched that specific vulnerability and built protections around that specific threat. So I think that that can be addressed.

I also think that, if we can build the kind of collaborative defense that we have been talking about, and the trust between partners, you don't necessarily need to share that information publicly or with the world. That disclosure could be made with partner, private-sector companies, and agencies.

Mr. TAYLOR. Ms. Howe, going back to the offensive question——

Ms. HOWE. I often tell my children I have escalation dominance so they should never take me on.

[Laughter.]

Ms. HOWE. I think, when it comes to offensive cyber operations, you have to make sure you have escalation dominance, which means it is only the purview of the U.S. Government to conduct offensive cyber activity.

I agree with Mr. Knake, that we have seen Cyber Command do that effectively. We need to have a very consistent policy of engagement if we are going to engage in offensive cyber. If we do, it essentially becomes part of the cyber deterrence policy.

When it comes to attribution, I would say our Government is the best in the world at attribution. We haven't gotten it wrong. In fact, even last week, the NSA put out an advisory showing that the Russians were using Iranian tools and infrastructure, and hiding as Iranians when they were conducting their attacks.

So this is one place where the U.S. Government is fantastic, knows what it is doing, and we have got the capabilities to launch offensive cyber the right way.

We have to have the policies, and we need to be able to communicate them. I do not think this is something the private sector should do.

Mr. TAYLOR. All right. I see my time has expired. Thank you, Mr. Chairman. I yield back.

Mr. RICHMOND. The gentleman from Texas has yielded. I now recognize the gentlewoman from Illinois, Ms. Underwood.

Ms. UNDERWOOD. Thank you, Chairman Richmond. Last week Members of this committee traveled to my district, the Illinois 14th district, to hold a hearing examining what steps the State of Illinois has taken, in coordination with the Federal Government, to prepare for the 2020 election.

In Illinois foreign adversaries were able to exploit a vulnerability in our State's voter database to access the records of 76,000 Illinoisans. Since then Illinois has used Federal and State dollars to increase its cybersecurity posture by executing the Cyber Navigator Program. This model continues to be a valuable tool for election officials around the State who now have access to a sure internet system, and highly-trained cybersecurity personnel.

We know that social media is an important source of information in communities like mine. A majority of Americans check social media at least once daily. So, Mr. Durbin, what advice can you offer to social media users about how to recognize the difference between a post from our neighbor and a post from a bot campaign?

Mr. DURBIN. That is a challenging ask. The people that are coming up with these posts, that are trying to deceive you, they are very good at them.

So I think the platforms themselves are going to have to be involved in looking at the metadata of where these posts are coming from to help identify is this really a person, or is this a bot. But if it is not from somebody that you—you don't know, or that you are just hearing from, and it is on something that is topical, that could be—or topical to the election, that would be a flag for me.

Ms. UNDERWOOD. What we often see is that, you know, people are in groups, and that they don't—they are not friends with the people in the group. So it just pops up on their feed.

So if I am a mom in the 14th, what should I be looking for? Right? Because I don't have access to that metadata.

Mr. DURBIN. Again, I think if it is from someone that you don't know, and it seems awfully topical, it is a pretty good coincidence that around this election we are—which is—this is a hot topic for us—I am getting some—a social post from somebody I don't know, that would be, certainly, a red flag for me.

Ms. UNDERWOOD. OK. But if they—"they," being the social media users—want to report a potential bot campaign, do social media companies currently have a timely and effective way for people to do that?

Mr. DURBIN. I don't know for sure what processes the social media companies have in place.

Ms. UNDERWOOD. Anybody else can—can anybody else answer that?

Mr. DURBIN. I will speak from personal experience. The only way I was able to report a fake LinkedIn profile that had connected with me was to tweet at LinkedIn. That was the only way they responded. They did not respond to the abuse report I filed.

Ms. UNDERWOOD. Interesting.

Following the 2016 election, Symantec conducted extensive research on the use of Twitter bot campaigns to promote disinformation leading up to and during the 2016 election. Mr. Durbin, can you share any lessons or key findings from that research as we prepare for the 2020 election?

Mr. DURBIN. It was very well-planned. There is this impression that it was a bunch of trolls out there that were behind this. We found that not to be the case.

They took their time in planning. They set accounts up months before they started using them. They were set up so that—it was kind of a main group that was responsible for the key content. Then there was a much larger group of the bots that were designed to get that fake messaging out. It was very effective with this kind of generate and amplify.

The response to one of the accounts, which was in my testimony, only 10,000 tweets, but was retweeted over 6 million times. That is a clear indicator that that those 6 million were not bots. Those were actual people that were choosing to read a message that was generated from a fake account——

Ms. UNDERWOOD. Right.

Mr. DURBIN [continuing]. Believe it, and then re-tweet it out to other people.

Ms. UNDERWOOD. Right. For years now, social media companies have been on record saying that they are working to combat the use of their platforms to spread disinformation, specifically during election times. But new reports emerge every day. Just yesterday we heard about 4 new disinformation campaigns backed by foreign states on Facebook.

Do you believe that these companies are prepared today for the 2020 elections, Mr. Durbin?

Mr. DURBIN. They claim that they are. I believe that they have the tools and the resources inside that they—they could take action. Whether or not they are, I am not an expert, I am not inside those organizations.

Ms. UNDERWOOD. OK. Thank you.

We have done a lot to secure our elections, but there is a lot of work that needs to be done to secure our Nation's election infrastructure. As technology continues to advance, so must our resources and policies to combat foreign adversaries who would seek to exploit new technologies to do us harm. Moving forward, this is going to take a whole-of-Government approach to preserve the integrity of our democratic institutions.

I look forward to working with all my colleagues on this committee and the House to address election security from all angles. I yield back.

Mr. RICHMOND. The gentlelady from Illinois yields back.

I want to thank the witnesses for their valuable testimony, and the Members for their questions.

The Members of the committee may have additional questions for the witnesses, and we ask that you respond expeditiously in writing to those questions.

Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 3:28 p.m., the subcommittee was adjourned.]

○