RED ALERT: COUNTERING THE CYBERTHREAT FROM CHINA

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MAY 15, 2024

Serial No. 118–108

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
55–708 PDF WASHINGTON : 2024

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
MIKE WALTZ, Florida

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida
RASHIDA TLAIB, Michigan
AYANNA PRESSLEY, Massachesetts

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
PETER WARREN, Senior Advisor
LAUREN LOMBARDO, Senior Policy Analyst
RAJ BHARWANI, Senior Professional Staff Member
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
Vacancy
Vacancy

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JARED MOSKOWITZ, Florida
AYANNA PRESSLEY, Massachesetts
Vacancy

C O N T E N T S

WITNESSES

INDEX OF DOCUMENTS

RED ALERT:
COUNTERING THE CYBERTHREAT FROM CHINA

Wednesday, May 15, 2024

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
Washington, D.C.

The Subcommittee met, pursuant to notice, at 4:01 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, and Connolly.

Also present: Representative Moylan.

Ms. MACE. Good afternoon, you all. I am pleased to introduce our witnesses for today's hearing.

Before we do that, I want to ask unanimous consent for Representative Moylan from Guam to be waived onto the Subcommittee for today's hearing for the purposes of asking questions. So, without objection, so ordered.

Our first witness today is Mr. William Evanina, Chief Executive Officer of the Evanina Group and former Director of the National Counterintelligence and Security Center. Our second witness is Mr. Rob Joyce, owner of Joyce Cyber, LLC, and former Special Assistant to the President and White House Cybersecurity Coordinator.

Our third witness is Mr. Charles Carmakal, Chief Technology Officer at Mandiant, and our fourth witness today is Mr. Steven Kelly, Chief Trust Officer at the Institute for Security and Technology.

I would now like to recognize myself for 5 minutes for my opening statement.

Earlier this year, top intelligence and cybersecurity officials testified before the Select Committee on China about a vast, long-term, and ongoing campaign by the Chinese Communist Party, or CCP, to hack into the computer systems that operate America's critical infrastructure—our dams, power plants, transportation hubs, and other essential operations. We do not know the full extent of this campaign. Why? First, the hacks are done in a manner designed to avoid detection. Second, the perpetrators are not trying to steal data or cause systems to immediately go haywire. It is worse. This

campaign, labeled Volt Typhoon, has been underway for several years, at a minimum.

The Chinese Government and its state-sponsored actors are using an infiltration tactic called Living Off the Land. The hackers' aim is to blend in with normal Windows system and network activities and remain undetected, according to one cybersecurity expert. Using malicious software, Volt Typhoon finds vulnerabilities to penetrate internet-connected systems to take control of devices like routers and security cameras, for example.

The goal here is not smash-and-grab-type theft or immediate system disruption. It is a lot more disturbing because China is playing the long game. It is silently pre-positioning itself for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States. That is according to an advisory jointly issued this year by the National Security Agency, the FBI, and other Federal agencies. In other words, the CCP is biding its time until it has reason to awaken these cyber sleeper cells. At the critical moment, they will trigger them to create confusion and disarray across America by disrupting our power supply, our transportation, our communication networks, our water and our food supply. This is a terrifying but realistic scenario. It also illustrates how China's cyber warfare against the United States has matured. It is now part and parcel of its military strategy and its plan to achieve its broader ambitions on the world stage.

Earlier this year, General Paul Nakasone, former head of the NSA and U.S. Cyber Command, testified the People's Republic of China poses a challenge unlike any our Nation allies have faced before, competing fiercely in the information domain. Today's hearing is a forum to discuss the challenge posed by China's cyber warfare and how we must, as a Nation, meet that challenge.

We know China is throwing massive money and manpower into its efforts. FBI Director Wray recently testified the PRC has a bigger hacking program than that of every major nation combined. In fact, if you took every single one of the FBI's cyber agents and intelligence analysts and focused them exclusively on the China threat, China's hackers would still outnumber FBI cyber personnel by at least 50 to 1. Fifty to 1, what a massive, massive number.

This speaks to the necessity of the U.S. maintaining its technological edge over China, including in cutting-edge fields like artificial intelligence and quantum computing. AI is increasingly being harnessed as both an offensive and defensive tool in cyber warfare, and post-quantum cryptography will be key to safeguarding critical data in the future. We also need to bolster cybersecurity partnerships between the Federal Government, the private sector, and international allies. These are vital pathways for sharing threat information. Finally, we need to widen our talent pipeline to help fill the hundreds of thousands of cybersecurity job vacancies that currently exist in the public and private sector of the United States.

To facilitate today's dialog, we are thrilled to have testifying today individuals who recently served at the highest levels of the Federal intelligence community. Before I—well, I already introduced them. I skipped the order, so you are here, so we will now recognize you for 5 minutes.

Mr. CONNOLLY. Thank you, Madam Chairwoman. Forgive me for being a little late, but we have too many hearings. I have two markups, two hearings, two briefings, and two sets of votes today, so maybe we should cut back on some hearings.

This past March, the Office of Director of National Intelligence released the Annual Threat Assessment of the U.S. Intelligence community. An excerpt from the report reads, "China remains the most active and persistent cyberthreat to U.S. Government, private sector, and critical infrastructure networks." The Chinese Communist Party poses a significant threat to the safety and economic prosperity of the United States. Through a multipronged strategy that includes the Belt and Road Initiative, economic coercion, and military buildup, the CCP has sought to challenge the American-led, rules-based international order. As part of its larger campaign to conduct asymmetric attacks on the United States, Beijing has turned to cyberattacks to steal American companies' intellectual property, undermine our civil society, and disrupt civilian and military infrastructure.

Just 2 months ago, the Cybersecurity and Infrastructure Security Agency, or CISA, confirmed that CCP-sponsored groups, like Volt Typhoon, have successfully infiltrated the Federal Government's civilian and military systems. What is more, some of those groups have been on our networks for up to 5 years and lay in wait until the opportune moment to disrupt a military response or to disable our water and power infrastructure. Unfortunately, when it comes to cyber warfare, the threat extends beyond China. In fact, experts have identified that not just China, but also Iran and North Korea, are using Russia's well-known disinformation playbook to disrupt elections, infiltrate American companies, and generally cause malign behavior.

Although disinformation campaigns and cyberattacks are not identical, they are two halves of the same chaotic coin. They similarly seek to inject uncertainty into daily operations and undermine the foundation of businesses, communities, and democratic values and tenets. Last November, Meta released its Third Quarter Adversarial Report, which outlined the removal of nearly 5,000 fake accounts all based in China. Meta removed those accounts for impersonating U.S. citizens and posting divisive rhetoric on deeply sensitive internal political issues with the intent to have an impact on the upcoming 2024 Presidential election.

It is not just America at risk. Earlier this year, the CCP again employed Moscow's tactics of online disinformation to cast doubt upon Taiwan's Government and to influence its recent elections. China has made a concerted effort to extend its power and influence across the world, especially in the global south. As roughly half of the world's population heads to the polls in 2024, China will take this opportunity, no question, to expand its influence and disrupt democratic processes using all tactics at hand.

Fortunately, the Biden-Harris Administration has taken unprecedented steps to counter these threats, both direct cyberattacks and disinformation campaigns. The White House released the first-ever National Cybersecurity Strategy in October 2022, directing both public and private stakeholders to coordinate efforts to address new ambitious plans called the International Cyber Space and Digital

Policy Strategy, seeking to work with allies to counter both Russia and China's global election interference efforts. I am also proud to have partnered with this Administration to safeguard networks against harmful nation-state actors.

Historically, this Subcommittee has held hearings to conduct meaningful oversight of Federal IT programs and worked alongside the Government Accountability Office to produce a Biannual Scorecard on compliance with FITARA. Agencies then receive grades based on compliance with the law and other statutory-based IT priorities. The scorecard assesses compliance with the Federal Information Security Modernization Act—FISMA—evaluating all 24 CFO Act agency cybersecurity postures. For further transparency and after years of congressional advocacy for metrics to replace the expiring Trump-era cross-agency priority data, OMB finally began publishing quarterly Federal cybersecurity progress reports on performance on Performance.gov website. These reports measure agencies' progress in achieving milestones in implementing key cybersecurity measures articulated in President Biden's executive order on improving the Nation's cybersecurity. The executive order encouraged adoption of Zero Trust architecture, and I encourage the Administration to revolve the Performance.gov data and provide public metrics in order to assess agencies' implementation.

To successfully stop our foreign adversaries, we need a whole-of-government approach with bipartisan congressional support to bolster our Federal work force and its IT infrastructure, and we need a whole-of-Nation approach to combat the disinformation and misinformation coming out of Russia and China. A report from the Center for Security and Emerging Technology found that, "By 2025, Chinese universities will produce more than 77,000 STEM Ph.D. graduates per year," compared to approximately 40,000, almost half that, here in the United States. If international students are excluded from that number of the United States, Chinese STEM Ph.D. graduates would outnumber their U.S. counterparts by more than 3-to–1. Three-to-one.

For our country to compete effectively with China, we need to implement the Office of the National Cyber Director's National Cyber Workforce and Education Strategies' recommendations and bolster our cyber work force and cyber faculty pipelines. We will soon introduce legislation that would enhance the already highly successful CyberCorps Program, which boasts an impressive 97 percent successful job placement rate. When passed, I hope that legislation will extend the scholarship cap of this program from 3 to 5 years and provide a pathway for more STEM-trained Ph.Ds.

We must properly fund the cyber defenses and basic government IT by reauthorizing and properly funding the TMF. In 2021, Democrats fought to secure $1 billion investment for that program, although the President had requested $6 billion. Today, the TMF has funded 11 Zero Trust efforts, as well as numerous other cyber projects, to protect our military and sensitive information while retiring vulnerable legacy systems. Congress usually sees IT as an easy thing to cut, but in most cases, IT modernization is a critical investment with a critical return on it with respect to the future. The pandemic exposed the cracks in the Federal Government's aging IT infrastructure and how it impeded mission-driven pro-

grams. Upgrading those systems is not just a national security priority. It is essential to making sure government stays effective and serves the people.

State-sponsored cybersecurity and disinformation campaigns seek to undermine the very fabric of our society. Cyberattacks wreak chaos and prove costly. Disinformation campaigns obscure the truth and threaten democratic principles. We must work to resist and oppose both. I look forward to the hearing, and I look forward to hearing from our witnesses. Thank you, Madam Chairman. I yield back.

Ms. MACE. Pursuant to Committee Rule 9(g), the witnesses, if you will please stand and raise your right hands.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[A chorus of ayes.]

Ms. MACE. Let the record show the witnesses all answered in the affirmative. We appreciate all of you being here today and look forward to your testimony.

Let me remind the witnesses that we have read your written statements, and they will appear in full in the hearing record. Please limit your oral arguments to 5 minutes, and as a reminder, please press the button on the microphone in front of you so that it is on and we can hear you up here. And when you begin to speak, the light in front of you will turn green. After 4 minutes, the light turns yellow, and then when the red light comes on, your 5 minutes has expired, and I will very kindly smile and wave this thing and ask you to wrap it up.

So, you all can be seated, and I will recognize Mr. Evanina to please begin your opening statement, 5 minutes.

STATEMENT OF WILLIAM EVANINA
CHIEF EXECUTIVE OFFICER, THE EVANINA GROUP, LLC
FORMER DIRECTOR, NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Mr. EVANINA. Chairwoman Mace, Ranking Member Connolly, Members of the Committee, it is an honor to appear before you today with my esteemed colleagues at the table.

Our Nation faces an array of diverse, complex, sophisticated, and unprecedented threats by nation-state actors, cyber criminals, and terrorist organizations. Each of them in their own distinct manner pose a serious threat to our Nation, our systems, and our citizens. However and unequivocally, the existential threat to our Nation emanates from the Communist Party of China. This comprehensive threat is the most complex, pernicious, strategic, and aggressive threat our Nation has ever faced. It is an existential threat to every fabric of our great Nation, our capitalism, and our democracy.

Xi Jinping drives a comprehensive and whole-of-country approach to the CCP's efforts to invest, leverage, infiltrate, influence, and steal from every corner of the United States. Naivete by those who hope to otherwise believe the opposite will only accelerate Xi's intentions and progress. Additionally, the United States' private sector, critical infrastructure, academia, and research and develop-

ment entities have all become the new battle space for the CCP's nefarious activities. As this Committee is aware, it is currently estimated that the economic loss from the theft of intellectual property from the Communist Party of China is nearing $600 billion per year. To make it more relevant and personal, that equates to approximately $6,000 per American families of four after taxes.

China's ability to strategically obtain our intellectual property and trade secrets via legal, illegal, and sophisticated cyber and hybrid methods is like nothing we have ever witnessed before. It is said by many to be the largest theft of intellectual property in the history of the world. Technology, from ideation to manufacturing, is frequently the intended target of these efforts. Additionally, it is estimated that 80 percent of American adults have had all of their data stolen by the Communist Party of China. The other 20 percent, just most of their data. Data and technology have become two of the most valuable commodities in the world, and acquiring them has been a high priority for the CCP.

I believe we must approach this existential threat with the same sense of urgency, leadership, spending, and strategy as we have done for the past 2 decades in successfully preventing and deterring terrorism. I would offer to this Committee that we are in a terrorism event—a slow, methodical, strategic, persistent, and enduring event—which requires a degree of urgency of government action and corporate awareness. It is clear that under Xi Jinping, the CCP's economic war with the United States, combined with his intent to be the military leader of the world, has manifested itself into a terrorism-like framework.

Let me be more specific. The CCP's capabilities and intent are second to none as an adversary. Countless cyber breaches, insider threats, and nefarious penetrations into our critical infrastructure are ubiquitous and have been widely reported. Add in the CCP's crippling stranglehold to so many critical aspects of our supply chain, and what results is domestic vulnerability we have not seen in generations, if ever. Now we must confront and defend against these CCP efforts with all the known and unknown artificial intelligence accelerators which will come along.

As we continue to drive forward with AI development for the good, we must also ensure security safeguards are implemented to protect from the bad. For all the progress we make, we must equally think of the potential of a zero day exploit utilizing sophisticated AI. When we incorporate China's recent actions, to include, as referenced by the Chairwoman and Ranking Member, Volt Typhoon; sophisticated surveillance balloons across our sovereign land; technical surveillance stations just 90 miles away in Cuba; maritime port threats; Huawei; strategic land purchases near military installations; fentanyl; TikTok; malign influence, et cetera, the collage begins to paint a bleak picture that is beyond blinking red. I am not even addressing space, deep fakes, or 5G genomics.

The inability or unwillingness to look behind China, the curtain they provide, and deal with the existential threat is no longer an option for the Congress, for the Administration, academic institutions, and the private sector. There is no more curtain to look behind. It has been removed. There must be consequences leveled for China's actions. Otherwise, there will be continued to be no deter-

rent. Volt Typhoon should be the straw of the proverbial camel's back. Unfortunately, I believe more is to come.

Thank you for the opportunity to join my esteemed fellow witnesses, and I look forward to answering your questions.

Ms. MACE. Thank you. I will now recognize Mr. Joyce for 5 minutes.

STATEMENT OF ROB JOYCE
OWNER, JOYCE CYBER LLC
FORMER SPECIAL ASSISTANT TO THE PRESIDENT
AND WHITE HOUSE CYBERSECURITY COORDINATOR

Mr. JOYCE. Chairwoman Mace, Ranking Member Connolly, Members of the Subcommittee, it is an honor to appear before you today. Thank you for this chance to discuss what I believe is the most significant cybersecurity issue faced by the U.S. That is the threat from cyberattack from the People's Republic of China and the threat it poses to our critical infrastructure. I am Rob Joyce. I served over 34 years at the National Security Agency, retiring as the Director of Cybersecurity, and I hope in our conversation today, I get to provide you some insight into the sophistication and strategic implications of these PRC cyberthreats and, really, how the PRC competes fiercely in the cyber domain.

It has been widely understood that for years, PRC hackers have stolen intellectual property, they have performed traditional espionage through cyber, but now they are preparing attacks against our critical infrastructure through cyberspace. So that first segment, they stole intellectual property. This is to aid their domestic industry. Chinese state-sponsored hacking groups, like APT 41, have systematically conducted cyberespionage campaigns to steal trillions of dollars' worth of intellectual property and trade secrets from U.S. companies. It has been across critical sectors like aerospace, pharmaceuticals, energy, manufacturing, and more.

For example, a multiyear campaign uncovered in 2022 showed APT 41 had infiltrated over 30 multinational firms and exfiltrated hundreds of gigabytes of proprietary data, including designs for fighter jets, missiles, drugs, solar panels, and other cutting-edge technologies not yet patented. The brazen thefts rob American companies of their R&D investment and competitive advantages, undermining U.S. economic interests. The annual cost to the U.S. economy from IP theft is hundreds of billions of dollars, and that does not include the long-term impact where China closes technology gaps and brings competing products to markets using stolen information.

And the second area I would highlight is the hacking for traditional espionage. A good example of that cyberespionage is the intrusion last year into the U.S. State Department in which the U.S. State Department discovered the compromise of its email system. The attackers accessed the inboxes of the U.S. Secretary of Commerce, the U.S. Ambassador to China, Congressman Don Bacon, and key State Department employees. All of this was before a sensitive visit by the Secretary of State to China. Microsoft assesses the intrusion was a Chinese threat actor they call Storm 0558. According to the Cyber Safety Review Board study of this event, of which I was a panel member, the activity was so stealthy, Micro-

soft still cannot say with certainty how the credentials used in the attack were stolen from them.

The issues of espionage and intellectual property theft have persisted for years, but now I want to highlight an even more troubling set of intrusions into critical infrastructure. In 2023, the U.S. cybersecurity community developed increased understanding that a set of PRC hackers, called Volt Typhoon, was pre-positioning on U.S. critical infrastructure. They were not there to steal our information but, instead, prepared to disrupt vital critical infrastructure systems. They want to slow the U.S. military's ability to mobilize and deploy in time of crisis, and they want to sow societal panic at the time of their choosing. They hope we would turn inward and focus on serious critical infrastructure problems at home rather than supporting any crisis on the other side of the globe. My colleague, the Honorable Evanina, talked about a simple description for their intent: domestic terrorism. They want to inspire panic inside our society. That is serious and disturbing.

So, this activity was discovered and validated through unique collaboration of government and industry, and I sit here today with some of my industry partners. Foreign intelligence was used in conjunction with the tremendous insight of industry where NSA, along with multiple government agencies, both domestic and international, described the intrusions in a public advisory, and 11 of the biggest internet and telecommunication companies added their names to the publication as participating in the investigation. Subsequent work by FBI, CISA, and industry confirmed the compromise of IT systems in diverse infrastructure sectors, including communications, energy, transportation, water, and wastewater systems. They found prepositioning in the continental U.S. as well as the U.S. territory of Guam. Guam is significant because the island hosts the Anderson Air Force base and Naval Base Guam, which play a crucial role in any potential conflict with China over Taiwan.

The intrusions have gone on for quite some time but have generally escaped notice. It is increasingly important that we understand the siege, that we work against it, and that we get our systems prepared to not only get them out but keep them out. These activities by the Chinese Government warrant your full attention and support, ensuring the PRC cannot undermine our national security. And I look forward to answering your questions alongside this knowledgeable panel.

Ms. MACE. Thank you, and, Mr. Carmakal, you are recognized for 5 minutes.

STATEMENT OF CHARLES CARMAKAL
CHIEF TECHNOLOGY OFFICER
MANDIANT

Mr. CARMAKAL. Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to share my observations and experiences regarding this very important topic, as well as for your leadership on cybersecurity issues. My name is Charles Carmakal, and I am the Chief Technology Officer at Mandiant

In my role at Mandiant, I oversee a team of security consultants and incident responders that help organizations both respond to security events and prepare for and mitigate the risk and impact of those security events. I led the teams that are responsible for discovering and identifying the SolarWinds software supply chain attack in December 2020, the Colonial pipeline cyber destructive attack in 2021, and the discovery of several novel and sophisticated cyber campaigns carried out by China-nexus threat actors. I am here to talk about Mandiant and my personal experiences in defending against and responding to cyberthreats emanating from the People's Republic of China. I will share my firsthand observations and the observations of the team that I lead.

Before we discuss today's threats, it is important to review what has happened over the past decade. On September 25, 2015, the United States and China agreed that neither government would conduct or knowingly support cyber-enabled theft of intellectual property for economic advantage. The following year, in 2016, Mandiant analyzed our incident response cases to assess the impact of the agreement. We actually observed a reduction in cyber intrusions by China-nexus threat actors that began a year prior to the agreement. The relatively lower volume of intrusion activity continued until approximately 2020. Government-backed China-nexus threat actors operated notably differently prior to the agreement than they do in modern days.

In my written testimony I talk about specific ways in which China-nexus threat actors operated prior to the agreement. These actors operate very differently today. They are more coordinated, resourced, sophisticated, and clandestine. I want to talk about a few of the capabilities that we see them demonstrating as they effectively break into organizations across the globe but, specifically, in the United States.

We see them leveraging zero-day vulnerabilities, which essentially are vulnerabilities that are known by threat actors and exploited by threat actors before the vulnerability is known by the vendor. The tools and the know-how to exploit these vulnerabilities are shared amongst multiple discrete groups that conduct cyber operations for the benefit of the PRC. Over the past few years, we have observed targeted zero-day exploitation of vulnerabilities in VPN, firewall, email security gateway, hypervisors, and other technologies that do not commonly support endpoint detection and response solutions. Endpoint detection and response solutions have gotten more effective over the years and have enabled organizations to detect compromises in Windows environments. Therefore, we see China-nexus threat actors targeting those systems that do not traditionally support EDR solutions, which essentially makes it more difficult for organizations to detect compromises.

To further exacerbate the problem, we see threat actors leveraging vulnerabilities in closed-box appliances, which are essentially systems that provide routing functionality, firewall functionality, or other security functionality to organizations. Because these appliances are closed box, it makes it very difficult for organizations to actually determine if they are compromised. If an organization wants to forensically examine a compromised device, they often need to reach out to the vendor in order to be able to

analyze it. Not all vendors will actually give permission to the victim organization to analyze the device.

We also see China-nexus threat actors leveraging residential IP addresses to conduct their intrusion operations. Over the years, they have built a very large botnet or series of computers that essentially enable them to access victim environments such that they look like an employee of the organization by accessing the network in a close proximity to the employees or to the companies that they want to log into. So, for example, if they were targeting a company in Virginia and they wanted to emulate an employee that lived in Virginia, we would see them leveraging compromised home infrastructure that allows them to log into the VPN of that Virginia-based organization and look like an employee there. We also see them living off the land, which is essentially leveraging tools and technologies that are native to operating systems so that they can move laterally within environments and not get detected by the organizations.

Given the advanced tradecraft leveraged by China-nexus threat actors, it is incredibly difficult for organizations to tell when they have been compromised. In fact, when we work with organizations and discover compromises, we often see that those compromises very often have lasted for weeks, months, and sometimes years. Over the years, I have personally observed multiple China-nexus threat actors with significant access and privileges to U.S.-based technology, defense, government, energy, construction, chemical, financial services, and healthcare organizations. Fortunately, I have not yet personally observed any actions taken by these actors that I consider to be overtly and intentionally destructive that could directly lead to negative kinetic outcomes or physically harm people. That could certainly change over time, but I wanted to share my personal experiences.

On behalf of Mandiant, I thank you for this opportunity to testify before the Subcommittee.

Ms. MACE. Thank you, and, Mr. Kelly, you are now recognized for your 5 minutes.

STATEMENT OF STEVEN M. KELLY
CHIEF TRUST OFFICER
INSTITUTE FOR SECURITY AND TECHNOLOGY

Mr. KELLY. Chairman Mace, Ranking Member Connolly, and Members of the Subcommittee, my name is Steve Kelly. I am the Chief Trust Officer at the Institute for Security and Technology, a think tank that unites technology and policy leaders to create actionable solutions to emerging security threats. I came to IST almost a year ago after retiring from the FBI as a special agent working cyber issues, and during my tenure, I was honored to twice serve on the NSC staff. Bonnie and I have since moved back to Indiana, but I am glad to be here in the Nation's Capital to discuss this pressing topic with you.

I am gravely concerned by both the PRC's illiberal global agenda and the means by which it seeks to realize it. For at least 2 decades, the PRC has carried out a rob, replicate, and replace strategy, which allows Chinese firms to benefit from stolen American innovation, begin manufacturing identical products at a lower cost,

and put the victimized firm out of business. Over time and across numerous research and development areas, this strategy, enabled by large-scale economic espionage, has allowed the PRC's technology industry to rapidly catch up and, in some cases, surpass the United States and allied nations.

Chinese technology products, both inside the PRC and for export, prioritize state-level interests over users' security and privacy, exposing users to government surveillance, acting as a vector for cyber operations, and potentially enabling denial and disruption operations. This has been a challenge here at home, leading Congress to fund ripping and replacing Huawei and CTE equipment from U.S. telecom networks, but the challenge is even greater in developing nations that often find the immediate need of economic development more pressing than the potential foreign intelligence risk. I am encouraged by a recent surge of interest in trusted technology within the investor community. For example, a group of leading investors recently announced their voluntary trusted capital investment principles and commitments. Another leading venture capital firm announced its American dynamism effort, and an array of investors and founders are driving a new defense tech-focused movement.

While it has been a long time coming, many throughout the world have come to recognize the risks that often accompany lower-cost Chinese products and are seeking more trustworthy sources even at a price premium. I played a small part in planning and launching the U.S. Cyber Trust Mark, a voluntary security labeling program for consumer internet of things devices, like smart home appliances, and I am pleased by the enthusiasm shown by consumer technology manufacturers in this program. While the FCC is moving the program forward, I encourage Congress to ensure the program's future stability by specifically authorizing and funding it.

The threat described by my fellow witnesses should inspire a new sense of urgency to remove the PRC's leverage by consistently counteracting and publicly exposing their cyber operations and hardening U.S. critical infrastructure. Given numerous cyberattacks impacting critical infrastructure over the past several years, including the ransomware attacks on Colonial Pipeline, JBS Foods, and many hospitals, we are clearly not doing enough. While ransomware is not the focus of this hearing, it is instructive of the real-world impact cyber operations can deliver. If Russian criminal gangs can achieve these effects, the People's Liberation Army most certainly can, too.

President Biden's National Cybersecurity Strategy calls for establishing minimum cybersecurity requirements for critical infrastructure through regulation or, where such authority does not exist, to seek it. While Federal regulations are not appropriate or desired in all circumstances, I believe that safeguarding functions essential to national security, economic security, or public health and safety warrants a regulatory approach. If establishing baseline requirements is to be achieved, Congress will need to create or clarify regulatory authorities for certain sectors, and each sector risk management agency and regulator must be resourced to carry out the task.

The infrastructure in need of protection is scattered throughout the Nation, and it is difficult to meet their needs from Washington, DC. Fortunately, there are a variety of players across the Federal enterprise who are able to engage at the local level. CISA's Cybersecurity Advisor Program, which places personnel across the country, is still quite new, and often an entire region may have only one such advisor. While I encourage Congress to fund sufficient advisors to cover the ground, what remains clear is the need for expanded and enhanced partnerships as force enablers. Fortunately, CISA cyber advisors are not alone as the FBI and Secret Service have task forces across the country.

Emulating the successful Joint Terrorism Task Force Program, there exist incredible opportunity to team Federal, state, and local cyber personnel to undertake both proactive and reactive cybersecurity efforts. National Guard units acting under their state authorities might also plug into this model. And, given the topic of this hearing, I think it is worth considering what authorities might exist or be needed for active duty cyber personnel under Title IX to provide assistance or even protection to civilian entities essential to the operation of key military installations, also referred to as defense critical infrastructure. While this approach may not scale, I believe there are scenarios under which that would make sense and should be explored.

I want to thank the Subcommittee for inviting me to participate in today's hearing and look forward to your questions.

Ms. MACE. Thank you. I will now recognize myself for 5 minutes of questioning. I do have several questions, so if I could just ask if we could be brief and direct and straightforward in our responses because I would like to try to get through all of them today.

General Nakasone has stated that, "If a nation-state decided to attack our critical infrastructure, I would say that is above the threshold level of war," and in the testimoneys that were prepared, it refers to China's cyber warfare against the U.S. as a form of terrorism, and, Mr. Evanina, you said today it was an existential threat, in your words. So, in the face of this terrorism, Mr. Evanina notes there is little deterrence also. So, my first question to you, Mr. Evanina, if these CCP-driven hacking campaigns are a form of war or terrorism, are we deterring China from conducting them?

Mr. EVANINA. Thanks for the question, Chairwoman Mace. If we are deterring, I am not aware of that from an intel perspective and a law enforcement perspective and a cyber perspective. What they are doing to us is on the border of——

Ms. MACE. Why not? Why aren't we deterring?

Mr. EVANINA. You would have to ask the policymakers in that space, but I do believe as they are preparing for battle, as we heard, and our critical infrastructure, I do not think it is reasonable for the minimum standards to ask companies to defend against nation-state threat actors and their proxies. I think it is a big task for them to do, and I think U.S. Government should take more of a hand in defeating and deterring the Chinese Communist Party and their infrastructure.

Ms. MACE. Is it safe to say this Administration does not have a strategy for deterrence?

Mr. EVANINA. I am not aware what the current strategy is.

Ms. MACE. OK. OK. So, my next questions will be for Mr. Evanina and Mr. Joyce. Do we know how many of America's critical computer systems have been infiltrated via the Volt Typhoon hacking campaign? Do we know?

Mr. EVANINA. I am not aware.

Ms. MACE. Mr. Joyce?

Mr. JOYCE. I do not have that information, no.

Ms. MACE. OK. So, if it is achieving its goal of gaining undetected system access, how would we know?

Mr. JOYCE. So, Madam Chairwoman, I believe the combination of intelligence that revealed this campaign as well as the capabilities of the U.S. cybersecurity industry has the ability to find and defeat some of these activities. But it is going to take a combination of both the public efforts, the private efforts, as well as the targeted entities have to remove some of their outdated and legacy IT to be safe

Ms. MACE. A debate that has been going on for the better part of 30 years probably. Mr. Joyce, do we know how much money the CCP invests in cyber warfare?

Mr. JOYCE. I do not.

Ms. MACE. Mr. Evanina, do you know?

Mr. EVANINA. I do not.

Ms. MACE. Do we know what kind of manpower they throw into these efforts? We heard what FBI Director Wray said recently, 50 to 1 in terms of comparing it to FBI analysts, but do we know what kind of manpower they have?

Mr. EVANINA. I think that is a conservative estimate by Director Wray, but I also would include in that the cybercriminal actors and their proxies that are supported by the MSS and the PLA should be included in that number as well.

Ms. MACE. OK. AI and quantum computing are powerful new tools in the arsenal of both hackers and defenders in cyberspace. How much does defense of critical U.S. computer systems hinge on our ability to maintain and buildupon our edge in AI over China? Either of you.

Mr. JOYCE. So, I believe that AI is actually going to advantage the defense much more than the offense, especially in the near term. The ability to look at large scales of data to understand the trade craft that might go undetected by human analysts is rapidly increasing by some of the innovations. So, I do believe that is our advantage today.

Ms. MACE. Mr. Carmakal, I have a minute left. Your testimony states that Mandiant, you helped identify SolarWinds and the Colonial Pipeline disruption in 2021. Would you say China's Volt Typhoon campaign is designed to make even these major hacks pale in comparison?

Mr. CARMAKAL. So far, we have only seen intrusion operations that were very hard to detect that were orchestrated by Volt Typhoon, plus many other threat actors emanating from China. We do not yet know what they might do, but we could tell you the capability and the access that they have is very significant, and they could certainly do anything similar to what happened to Colonial Pipeline or even much worse with the access that we know that they have.

Ms. MACE. And how could we respond to a slew of disruptions to critical operators if all this is happening all at once, if they did something all at once?

Mr. CARMAKAL. It would be very difficult to respond to. There is a finite amount of security talent and investigators and incident responders that could help respond to security events. And so if there were a cascading set of security attacks against organizations, it would be incredibly difficult to respond to it.

Ms. MACE. All right. Thank you, and I will now yield.

Mr. CONNOLLY. Madam Chair, if you want to take another 5 minutes?

Ms. MACE. No, I will wait.

Mr. CONNOLLY. OK.

Ms. MACE. Yes.

Mr. CONNOLLY. All right.

Ms. MACE. OK. And I will now yield to Mr. Connolly for 5 minutes.

Mr. CONNOLLY. Thank you. Mr. Evanina, you were ringing the alarm bell some time ago. You served in the Trump Administration. What was your position?

Mr. EVANINA. Yes. I started as the head of counterintelligence for the United States in 2014 under President Obama, and I stayed there until January 2021.

Mr. CONNOLLY. OK. And you, among other things, led efforts to protect security and integrity of the 2020 election from foreign threats. Is that correct?

Mr. EVANINA. That is correct, sir.

Mr. CONNOLLY. Last month, the *New York Times* published an article, "China's Advancing Efforts to Influence the U.S. Election Raise Alarms," and it highlighted that during the 2022 midterm elections, the cybersecurity firm, Mandiant, reported that an influence campaign linked to China tried to discourage Americans from voting while highlighting political polarization. The finding illustrates how China has been using Russia's disinformation to "influence American politics with more of a willingness to target specific candidates and parties, including now-President Biden." I ask that we insert this article into the record.

Ms. MACE. Without objection.

Mr. CONNOLLY. I thank the Chair.

Mr. CONNOLLY. Mr. Evanina, during the Trump Administration, is it true you were already ringing the alarm that both CCP and Russia were trying to influence that 2020 election?

Mr. EVANINA. Yes, sir.

Mr. CONNOLLY. And in August of that year, you issued an official press release warning, "We assess that Russia is using a range of measures to primarily denigrate former Vice President Biden and what it sees as an anti-Russian establishment." Your statement added, "For example, pro-Russian Ukrainian parliamentarian, Andrei Derkach, is spreading claims about corruption, including through publicizing leaked phone calls, to undermine President Biden and his candidacy and the Democratic Party." I ask unanimous consent to insert that press release into the record.

Ms. MACE. Without objection.

Mr. CONNOLLY. Mr. Evanina, is that the same Andre Derkach who, according to reports, "gained access to Trump's inner circle through Rudy Giuliani, the President's personal lawyer?"

Mr. EVANINA. Yes, sir.

[Chart]

Mr. CONNOLLY. Is that the gentleman in question?

Mr. EVANINA. Yes, sir.

Mr. CONNOLLY. And is he sitting with Rudy Giuliani?

Mr. EVANINA. Yes, sir.

Mr. CONNOLLY. Aha. In fact, just a month after you issued your statement, the Trump Administration sanctioned him, to their credit, for being an "active Russian agent for over a decade." Is that correct?

Mr. EVANINA. I believe that is correct.

Mr. CONNOLLY. Even though experts, including you and others, have repeatedly warned us about Russian efforts to smear Joe Biden with false information about corruption in Ukraine. And by the way, one of those informants who was the key witness of the oversight impeachment hearing is now in jail for lying to the FBI. Is that correct, Mr. Kelly? Are you familiar with that?

Mr. KELLY. I do not have firsthand knowledge of that.

Mr. CONNOLLY. Well, do you have any thoughts, given your new role and your previous role, about the dangers that can ensue? Mr. Evanina warned us, correctly, about Russian disinformation inserting itself into our politics? And it sure did get into a very high level both here in Congress and in targeting the President of the United States with absolutely false information. What could go wrong with that, Mr. Kelly? What should we worry about with that?

Mr. KELLY. Malign foreign influence operations coming from Russia, China, or anywhere else is incredibly problematic and, in particular, in the context of elections, so, I agree with that statement.

Mr. CONNOLLY. So, in some cases, credulous people might take at face value information coming from social media bots, false sources who create false identities as Americans when they are, in fact, not. In fact, recently, one of the big media companies just took down 5,000 accounts, I think I mentioned in my opening statement, all from China, pretending to be Americans. But the other is that political figures might use that information, knowing or not knowing it is false, for political gain that could, in fact, be harmful to our system, especially given the fact it is based on false information and a foreign actor with an agenda. Would that be a fair statement, do you think?

Mr. KELLY. Yes. That can absolutely happen.

Mr. CONNOLLY. Thank you. I yield back.

Ms. MACE. Thank you. I would like to say for the record, most Republicans in Congress are actually banned from Russia. And when we are talking about false sources, false information, we could look no further in 2020 than mainstream media that covered up the laptop, and the FBI and all those national security advisors that signed that letter. That was absolutely misinformation, disinformation right before an election. So, when we talk about foreign actors with an agenda, there are domestic actors with an agenda.

So, I would now like to recognize Mr. Moylan for 5 minutes.

Mr. MOYLAN. Thank you, Chairwoman Mace and Ranking Member Connolly, for allowing me to waive onto the hearing and speak on an issue that has plagued my district and the United States at large.

The problem is clear. The People's Republic of China has unabashedly conducted cyber warfare against the United States for over a decade. The PRC uses proxy groups, like Volt Typhoon, to sidestep attribution for these cyberattacks. As a veteran, I can personally say that divesting cyberattacks on the Office of Personal Management in 2015 was a cyber wakeup call. While many cyberattacks target our Federal Government, Chinese hackers' indifference toward targeting civilians is apparent. Chinese leadership or their proxies has continued to demonstrate a lack of concern toward attacking civilian infrastructures. Regardless of source, the blatant disregard, even to the extent of launching cyberattacks during an active Category 5 typhoon on Guam, shutting down Guam's communications while extreme weather destroys billions of dollars' worth of homes, businesses, and community facilities, is simply inexcusable.

So, my question, Mr. Evanina. Cyber represents a facet of Chinese gray zone warfare that the U.S. has struggled to contend with. Part of this problem stems from using cyber contractors to circumvent the Chinese Communist Party attributions for these attacks. With those companies in mind, could you recommend steps that the U.S. should take to properly distinguish who attacks us?

Mr. EVANINA. Congressman Moylan, I thank you for the question, and thank you for your support and efforts in Guam and the Pacific for us competing with our major adversary there. To answer your question, sir, I think the first thing has to happen, we have to be more aggressive as a country, as an Administration, working in partnership with Mandiant and others, to attribute these criminal entities as what they are. They are proxies for a state-sponsored organization that we know is the Communist Party of China.

China actors who are in the administrative state security or the People's Liberation Army oftentimes work part-time jobs in these cyber organizations and do the bidding of the Communist Party of China, and oftentimes are utilized to do zero days and other cyber activities to obfuscate attribution by the Communist Party of China. I think we have to get more aggressive as a country in attributing those entities as what they are: long arms of the Communist Party of China.

Mr. MOYLAN. Thank you. Mr. Joyce, with the limited cyber personnel already, Guam cyberinfrastructure suffers from deterioration and lack of funding, leaving civilian and military assets vulnerable to cyberattacks with Guam being one of the closest U.S. territories to China. What policy advice would you give the President, the Governor, or even myself to solve Guam's cyber insecurity?

Mr. JOYCE. Thank you, Congressman, for your question. I think the most important thing is we have to have the awareness and the priority on this crisis to give them the resources to get rid of old, outdated, and insecure hardware. A lot of the tactics used in the attacks are finding flaws that could have and should have been patched in old and obsolete equipment. So, if you can get the budg-

ets for the infrastructure so they will have cyber-capable training, so that they will get rid of their old and antiquated technology, and that they have the resources to get the support of the private industry with the expertise, I think we can make a lot of headway on this problem.

Mr. MOYLAN. Perfect. Final question—we have got about a minute—for both of you, please. China is using national cyber power to harass districts and state-level actors. Could the panel briefly explain the necessity of developing Federal, state, or local cyber defense and responses?

Mr. EVANINA. Thank you, Congressman. I will start. I think the state and local and tribal cyber capabilities are the weakest point for our Nation. I think the Chinese Communist Party exploits that, especially at the county level. We see that throughout not only ransomware attacks, but also, as we will start to see, in election infrastructure, it is the weakest level. And oftentimes states throughout the United States do not have the money to invest and to replace the legacy hardware that Mr. Joyce talked about. I think that is going to be the first thing to do is to pay for that legacy information utilities to be removed.

Mr. MOYLAN. Mr. Joyce?

Mr. JOYCE. I think it has got to be a close collaboration between the private sector and the state, local, and tribal entities. They are often resource and expertise poor. Someone going to school with a cybersecurity degree, they are not excited to go into the local water utility and be their CISO. So, we have got to then augment them with private industry and technology so that they can have top-notch security.

Mr. MOYLAN. Thank you very much. Thank you to the panel. Thank you, Chairwoman Mace. Thank you.

Ms. MACE. Thank you, Mr. Moylan, and we are going to go for a few extra minutes until votes, which could be in a minute, could be in 10 minutes, so I would like to recognize myself for 5 minutes. I had a few extra followup questions I wanted to ask.

Mr. Carmakal, rapid incident reporting by hack victims enables the identification of specific threats and limits the harm that they can inflict, but critical infrastructure operators vary widely in their knowledge of incident reporting protocols and in their compliance with them. So, what can be done to improve incident reporting by non-Federal entities?

Mr. CARMAKAL. Yes. Thank you very much for the question, Chairwoman. Incident reporting is a very difficult topic because there are a number of equities that need to be balanced. You cannot disclose a security incident too early, especially if the threat actor still has access to the environment. They may do something more damaging, or they might escalate their attack, or they might steal more data. Obviously, you also do not want organizations to wait too long to disclose that there was a security event. And so, there is definitely a very tough balance in terms of how long it actually should take for an organization to disclose, but at a minimum, we do want organizations to disclose so that the whole of community has the opportunity to learn from it.

Ms. MACE. Does the government provide clear guidance about these protocols?

Mr. CARMAKAL. There are a number of regulations and requirements for disclosure, so it is confusing to certain organizations to understand who do they need to report to, when do they need to report it, and they typically have to engage legal counsels to help understand the reporting complexities.

Ms. MACE. And if you are engaging legal counsels, probably pretty expensive for a business in some cases.

Mr. CARMAKAL. It certainly could be expensive. Yes.

Ms. MACE. Do companies ever get punished if they have been hacked by the government? Do they get sued? Is there that kind of thing going on, too, when these things happen?

Mr. CARMAKAL. A lot of victims of cybercrime or cyberespionage feel like they are victimized multiple times. So, they are first victimized by the threat actor, then they might be victimized by the media, by their customers, by their partners. And so, yes, it is certainly complicated, and they do feel like they are victimized often.

Ms. MACE. Is the government effectively sharing information it has about threat actors with the private sector?

Mr. CARMAKAL. There is a lot of information sharing that is occurring from a government perspective. Obviously there could always be more information sharing, better information sharing, more timely sharing, but there is a lot of great things that are happening.

Ms. MACE. That is good to hear. So, talk to me—in your testimony earlier, you talked about legacy systems for a little bit. Talk to me about that and what dire straits we are in right now with regards to our vulnerabilities.

Mr. CARMAKAL. Yes. We very often find organizations that have antiquated technologies still deployed within their environment. Sometimes we see very old operating systems that are deployed that have not yet been retired but are still used for business-critical capabilities and functionality.

Ms. MACE. What is the oldest one you have heard of? What has been around the longest?

Mr. CARMAKAL. We still see Windows XP, which has been long end of light for quite some time.

Ms. MACE. How long?

Mr. CARMAKAL. I cannot remember how long it has been, but it is probably been more than a decade, if I am not mistaken. That is in the IT environments. When you look at OT environments or operations——

Ms. MACE. Is that government specifically or are you just are saying private industry?

Mr. CARMAKAL. Across the globe.

Ms. MACE. Across.

Mr. CARMAKAL. When you look at the systems that are controlling safety at nuclear power plants or manufacturing facilities or pipelines, what we tend to find is that there is very old technology that exists out there that you cannot actually apply software patches to. And so, in the IT world, you expect that you would have to apply a critical security patch in hours or days or maybe a month. In the operational technology world, sometimes the patch timing takes months, maybe a year, or maybe it never happens at all. Generally speaking, there are other compensating controls that

help mitigate the risk of a compromise of an OT environment. But essentially, if a threat actor could get into an operational technology environment, it could be a pretty bad day for that organization because there are generally very little controls in those OT environments with very old technology.

Ms. MACE. How do we incentivize technology updates, private and public sector?

Mr. CARMAKAL. I defer to my colleagues on this panel for a proper response.

Ms. MACE. All right. Mr. Joyce and Mr. Evanina?

Mr. JOYCE. I think one of the things you have to do is you have to look at regulation, right? We would not have antilock brakes and seat belts in our cars if it were just up to the industry. I am not a huge fan of regulation, but I am increasingly convinced that the bare cyber minimums need to be regulated.

Ms. MACE. Mr. Evanina?

Mr. EVANINA. I would add out to that that I think it is about leadership, and it starts with the government. I think if the government earmarked significant dollars, moonshot, to update our own legacy systems would obviously prevent our adversaries from getting our government systems, and I think that would be a leading role to stimulate private sector to do the same.

Ms. MACE. Yes. We have had a lot of hearings up here and the amount that is wasted even in tech. I mean, we had a hearing last year, and DoD had wasted $300 million on a software program. I can only imagine what we could have done with $300 million in the cybersecurity space, either hiring workers or updating and upgrading software packages and technology to keep them safer. So, I appreciate your time today and thank you for being here. Do you want to be recognized for 5 minutes, Mr. Connolly?

Mr. CONNOLLY. I thank the Chair. I want to go back to the danger of relying on Russian and China sources because they have an active agenda of insinuating. We have established one that you are familiar with, Mr. Evanina, and that was a key source for Rudy Giuliani and his false claims about corruption involving Ukraine, Burisma, and then-Vice President Biden, and it is very dangerous to rely on sources like that.

I want to point out three key sources for the impeachment inquiry on my other committee, the Oversight Committee, the full Committee, and on the Weaponization Committee: one, a man on the lam who has been charged by the U.S. Government for being a Chinese spy outright; second, a man who is in Federal prison today for having been convicted of fraud; third, a man named Alexei Smirnov, an FBI informant, in jail, charged by the FBI for lying to the FBI. He lied specifically about witnessing a cash bribe being given to President Biden, then-Vice President, or out of office, actually, and his son, Hunter. Neither was true. In fact, it has been established Mr. Smirnov did not even meet anyone from Burisma until 2 or 3 years after the alleged exchange. And furthermore, Mr. Smirnov has admitted that his sources were Russian agents. Other than that, these are reliable witnesses upon which one of the most solemn constitutional duties that falls upon Congress has occurred, the impeachment of a President. We relied on Russian and Chinese agents. That is an established fact.

Mr. Evanina, what are the risks when political leaders assert that claims of Russian or Chinese interference are just a hoax? Could something go wrong when we do not take it seriously?

Mr. EVANINA. Ranking Member Connolly, I think it is important to note that we should fully expect the Communist Party of China, Russia, Iran, and others to participate in the same type of disinformation, misinformation in the upcoming election. And I think we have to be postured to be able to identify that quickly and notify the American public as fast and as furious as we can, and then take action to notify individuals who are either a part, wittingly or unwittingly, or being used by those nation-states to promulgate their information. So, I think that is really critical that we do that moving forward.

Mr. CONNOLLY. So, I do not want to put words in your mouth, but I am hearing you say, look, before we politically decide to dismiss something as an inconvenient fact, we need to have some skepticism about sourcing because of what Russia and China are doing.

Mr. EVANINA. Well, I think part of the playbook for Russia and China and others is to be able to sow doubt in all the reporting, and I think that is important. I think we should also take time to rely on the intelligence community, law enforcement, and the FBI to be able to most effectively weed out some of this information, to be able to be in the best posture to provide that to decisionmakers.

Mr. CONNOLLY. And that is what you did during the Trump Administration.

Mr. EVANINA. I think that is what the United States government——

Mr. CONNOLLY. Right. It is not a Democrat, or it should not be a Democrat or a Republican issue. Mr. Kelly, in your time in the FBI, does it echo what Mr. Evanina has cautioned us?

Mr. KELLY. Yes, there was——

Mr. CONNOLLY. I cannot hear you.

Mr. KELLY. Yes. In the last Administration, the Justice Department actually came out with a policy on this topic, which I think was actually a very wise approach, which is to flag the source of information. And so, to the extent that they have information that a malicious foreign actor has set up a false persona on social media, they cannotify the social media platform so that they can take action under their terms of use, but to not get into the business of fact-checking because that gets very, very tricky.

So, I think where the facts are that we have identifiable bad foreign actors that are doing things, that is an opportunity then to notify the affected people, to notify technology platforms. And then when it relates to, specifically, the functions of an election, misinformation around that polls have closed or the polls are open, or the voting day moved, or whatever else is happening, those are the kinds of things that public officials need to come out and absolutely correct the factual record on.

Mr. CONNOLLY. Thank you, and I appreciate it. Thank you, Madam Chair.

Ms. MACE. Thank you. And going back, just to clarify with Alexei Smirnov, this Committee was actually told by the FBI—we did not know his name when we got the access to the FBI 1020 form—but

the FBI told this Oversight Committee "that the witness was trustworthy and credible," also repeated by Democrat colleagues here on the Oversight Committee because that is what the FBI told us. And that witness actually was paid six figures by the FBI, over half a million dollars. So, I do not know if the FBI just was incompetent in paying a witness that was not trustworthy and credible, or if they were lying to Congress and this Committee when they said the witness was trustworthy and credible.

And just a reminder, this hearing is about China. It is not about Russia, and we are talking about skepticism about sourcing. We should be very skeptical of mainstream media here today who has fed the American people lies, hook, line and sinker. And, in fact, the whole Russia hoax thing, Trump was not assisted by Russia. The Russia hoax was actually Joe Biden getting paid off with his family members by Russian oligarchies and then lying about it, and we saw that in the testimony of Hunter Biden and his deposition, and we have seen these lies told over and over again by my colleagues across the aisle. Every time it is an accusation, it is really a projection. So, with that, I will recognize Mr. Timmons for 5 minutes.

Mr. TIMMONS. Thank you, Madam Chair. Back to China. I am going to talk about Huawei briefly, Mr. Evanina and Mr. Joyce. I am going to ask you some questions at the end of it.

So, China was using Huawei to give next-generation wireless technology to developing countries and to developed countries, many of which were allies, and they were doing that at a rate that was beyond competitive. It was essentially subsidized, and the FBI was able to reach out to our allies and essentially say, hey, this is a really bad idea. They have a backdoor in security. Their servers are not secure. You are essentially letting the Chinese have all your data.

And so what happened? Well, all of our allies said they either took steps to ban Huawei, or they changed their course and are now using more secure next-generation wireless technology. And that was done, basically, because the United States took a leadership role in informing our allies that China was not being a good actor, and it has caused Huawei to have to completely adjust their approach to the global economy. Is that fair, Mr. Joyce?

Mr. JOYCE. Absolutely.

Mr. TIMMONS. OK. So, I think this is a great model. It is a great model of how we can address larger concerns. So, obviously, we are talking about cyberattacks, and there is no amount of money that the private or publicly held companies can spend to secure their networks from a government as big as China. There is just nothing they can do. It is not a question of if they are going to get a breach. It is a question of when. But what we can do is we can use the U.S. Government and use our allies to create a consequence.

So, I do not see why the United States and like-minded countries cannot create a system—the biggest issue is attribution in this proposal. If a company is breached and receives damages and it is from a nation-state, I think that company should be able to go to the government and say, look, we do all of these things right to try to protect our data, but China came after us. We had a breach. It cost us this amount of money. Obviously, there is going to be a civil

suit. They are going to have to settle that civil suit with all of the individuals who had data breached. And so, let us just say it is, I do not know, a hundred million dollars. So, then the United States says, all right, attribution is good. China did this. The government did this. Here is your hundred million dollars, and then go and use trade tariffs to essentially make the United States whole. If we create a system like that, it can create a deterrent threat to nation-states that are using cyberattacks as a tool. What do you all think? Is that something that we should consider doing, Mr. Evanina?

Mr. EVANINA. Congressman Timmons, yes, but I will caution the Subcommittee here that I think the back end of this is the concern I have looking at Huawei for 15 years. We were able to get the threat relayed to the Congress who acted and had rip-and-replace legislation. The problem we have is Huawei is a legitimate business entity that functions fairly well with an intelligence collection apparatus tied to it. If we rip it, we need to replace it with something different. And the trouble we have had, because we do not have the innovation and technology based in the United States to replace Huawei, we are still stuck with Huawei across our country in our telecommunication systems. So, to your point, I agree with, but we also have to have something to replace Huawei with when we rip it out.

Mr. TIMMONS. Mr. Joyce, do you think that the international community could create this deterrent threat that would hold China accountable? It is not just China. It is China, North Korea, Iran, Russia, anybody that is using cyberattacks as basically a state tool. Is that something that we could do?

Mr. JOYCE. I do, Congressman, believe we have got to use all the elements of our national power, whether it is military, cyber, but increasingly commercial and tariff-related activities have proven pretty forceful, and we have seen the reactions to it. Unfortunately, a lot of these cyber criminals get to remain in places like North Korea, Russia out of the reach of law enforcement cooperation, and so we have got to have other tools beyond law enforcement.

Mr. TIMMONS. So, I think that we can resolve that by saying that any individual that is attacking the United States, I mean, it is no different than the Taliban. I mean, we sent hundreds of thousands of U.S. soldiers and waged war for decades in Afghanistan because the Taliban allowed Al-Qaeda to use it as base of operations to attack the Twin Towers. So, I mean, there is no difference if Al-Qaeda was using a computer in Afghanistan and using code to crash an energy grid in a hot area in the summer or a cold area in the winter. I mean, it could legitimately kill thousands and thousands of people if we are unable to provide heat in the Northeast during a winter storm. And it would be very easy to do that, and we would have to hold that individual accountable, but we would have to hold the country that gave them safe harbor accountable. I mean, do we agree on this?

Mr. EVANINA. I completely agree, and I think your analogy is right with the terrorism because if Al-Qaeda had pre-deployed explosives or electrical magnetic capability in New York City, is that different than Volt Typhoon and what they are doing here to potentially cause harm to our critical infrastructure? We have to look at that as a simple model.

Mr. TIMMONS. And if there was a cyberattack on Goldman Sachs resulting in a half a billion dollars in damages, are we not going to then make them whole when they did nothing wrong versus if Hamas bombs their building? I mean, we are going to make them whole, so I do not think that we should view a terrorist cyberattack any differently than we would view a missile because there is no difference, effectively.

OK. I am over time. Sorry. Thank you for your——

Ms. MACE. I agree. Cybersecurity is national security. Thank you, Mr. Timmons.

In closing, I want to thank our panelists who are here this afternoon, once again, for your testimony today.

With that, and without objection, all Members will have 5 legislative days within which to submit materials and to submit additional written questions for the witnesses, which will then be forwarded to the witnesses for their response.

So, if there is no further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 5:10 p.m., the Subcommittee was adjourned.]