Prepared Statement of Jamil N. Jaffer*
on
Foreign Cyber Threats: Small Business, Big Target
before the
House Small Business Committee

July 6, 2016

I. Introduction

Chairman Chabot, Ranking Member Velazquez, and Members of the Committee: thank you for inviting me to discuss foreign cyber threats and the particular challenge they pose for American small businesses. I hope that we will have the opportunity to talk candidly about these topics and to discuss what we might do, as a nation, to confront these very real and serious threats.

I also want to note your leadership, Mr. Chairman, here in the House of Representatives on these important issues, and to highlight your successful amendment in the House Foreign Affairs Committee to the State Department authorization bill requiring the Comptroller General to report on the State Department's possible use of equipment and services purchased from suppliers linked to key cyber threat nations. The potential use of such equipment and services by the U.S. government is a key issue for congressional oversight, particularly given the threat environment that our nation—in both the public and private sectors—faces from nation-state actors and their proxies.

And, as we know from FBI Director Jim Comey's statement yesterday, the FBI has recently "developed evidence that the security culture of the State Department in general, and with respect to use of unclassified e-mail systems in particular, was generally lacking in the kind of care for classified information found elsewhere in the government."[1] This is troubling news indeed, given the important role that the State Department plays in our relations with other nations, the type of sensitive information it receives from our allies, and the critical nature of the negotiations it conducts on behalf our people. It is even more troubling because it comes in the aftermath of the November 2014 and March 2015 public disclosures of breaches at the State Department that prompted multiple shutdowns of the State Department's unclassified email systems and may have exposed sensitive data.[2] These incidents, taken

---

* Jamil N. Jaffer currently serves as an Adjunct Professor of Law and Director, Homeland & National Security Law Program at the Antonin Scalia Law School at George Mason University and is affiliated with Stanford University's Center for International Security and Cooperation. Mr. Jaffer also serves as Vice President for Strategy & Business Development for IronNet Cybersecurity, a startup technology company headquartered in the Washington, DC metropolitan area. Among other things, Mr. Jaffer previously served as Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee, as an Associate Counsel to President George W. Bush, and as Counsel to the Assistant Attorney General for National Security in the U.S. Department of Justice.

[1] *See* Federal Bureau of Investigation, *Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System*, Federal Bureau of Investigation (July 5, 2016), available online at <https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b.-comey-on-the-investigation-of-secretary-hillary-clintons-use-of-a-personal-e-mail-system>.

[2] *See, e.g.*, Office of the Inspector General of the State Department and the Broadcasting Board of Governors, *Semiannual Report to the Congress – April 1, 2015 to Sept. 30, 2015*, available online at <https://oig.state.gov/system/files/oig_fall_2015_sar.pdf> ("The Department spent approximately $1.4 billion on information technology (IT) in FY 2015. The same year, a number of cybersecurity incidents illustrated deficiencies in the Department's

together, simply highlight the need to ensure that the Chairman's amendment—or language to the same effect, perhaps even expanded further—makes it through the House and Senate floors and to the President's desk at part of the State Department Authorization legislation.

Stepping back, for the moment, from the challenges of internal government cybersecurity, however, may provide the members of this Committee the opportunity to examine the myriad and growing ways in which our nation—and the innovative small businesses that are key engines of job growth and investment in our economy—must confront the very real threats we face in cyberspace.

II. Cyber Opportunities

As members of this Committee well know, technology is rapidly changing. The amount of information circulating the globe via IP networks will reach 2.3 zettabytes by 2020.[3] This means that by the end of the decade, "the gigabyte (GB) equivalent of all the movies ever made will cross the global Internet every 2 minutes."[4] This growth in technology and IP traffic will be accompanied by rapid growth in the quantity of devices connected to IP networks, particularly as we move towards the so-called Internet of Things (IoT) environment. Indeed, Cisco estimates that by 2020 there will be 26.3 billion networked devices, or more than three IP-connected devices per person around the world, up from 16.3 billion such devices in 2015.[5] Traffic from wireless and mobile devices will also account for 2/3 of all IP traffic by 2020,[6] and the Internet Society forecasts that worldwide mobile Internet penetration will reach 71% by 2019.[7]

This growth in technology and connectivity offers huge opportunities and benefits for individuals and business around the globe. It will provide information access to oppressed populations and political movements worldwide. And it will also provide broad access to global markets and production capacity to businessmen and women who were once limited by geography or their national infrastructure. Indeed, Cisco estimates that IP traffic will grow fastest in the Middle East and Africa, coming in at a compound

---

efforts to protect its computer networks. Malicious actors exploited vulnerabilities, potentially compromising sensitive information and significant downtime to normal business operations."); *see also* Russell Berman, *The U.S. Government Is Under (Cyber) Attack*, The Atlantic (Nov. 17, 2014) ("The State Department on Monday joined the White House and two other federal agencies in confirming that it had been the victim of a recent and successful cyberattack. Spokesman Jeff Rathke told reporters at Foggy Bottom that officials 'detected activity of concern' several weeks ago targeting its unclassified email system and that it used a 'scheduled outage' to address the problem this past weekend."); Justin Fishel & Lee Ferran, *State Dept. Shuts Down Email After Cyber Attack*, ABC News (Mar. 13, 2015) ("The State Department shut down large parts of its unclassified email system today in a final attempt to rid it of malware believed to have been inserted by Russian hackers in what has become one of the most serious cyber intrusions in the department's history, U.S. officials told ABC News. 'The Department is implementing improvements to the security of its main unclassified network during a short, planned outage of some internet-linked systems,' State Department spokeswoman Jen Psaki said in a statement to ABC News.")

[3] *See* Cisco, *The Zettabyte Era—Trends and Analysis* (June 2016) at 1, *available online at* <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf>

[4] *See Zettabyte Era*, n. 3 *supra* at 4.

[5] *See Zettabyte Era*, n. 3 *supra* at 2.

[6] *See Zettabyte Era*, n. 3 *supra* at 2.

[7] *See* Internet Society, *Global Internet Report 2015*, at 9, *available online at* <http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf>.

annual growth rate (CAGR) of 41% between 2015 and 2020, with Central and Eastern Europe next at 27%, and as compared with a CAGR of 19% for North America over the same period.[8] And in the developing world, smartphones shipments are up, exceeding 50% of all mobile handsets shipments as of late 2014.[9] Not surprisingly then, regions like Latin America and the Middle East and Africa also saw the fastest growth in consumer mobile location based services worldwide between 2014 and 2015 at 62% and 52%, respectively, year-over-year. Similarly, mobile banking and commerce grew fastest in Latin America at a 49% year-over-year rate and the Middle East and Africa led mobile video growth at a 43% over the same period.

And it is not just developing economies that can benefit from these opportunities. Modern, developed economies will also increasingly rely on technology to innovate, to improve productivity, and to protect the fruit of such innovation and capitalize on productivity gains. Indeed, as the United States continues to evolve its core economic base towards a technology-driven industrial and services economy, protecting the core intellectual property that lies at the heart of such an economy will be all the more important.

Small businesses will almost certainly be at the forefront of this ongoing revolution. This is because, more than any other part of the economy, small businesses have the flexibility to create new products and to capitalize on advances in technology through rapid innovation and by bring products to market quickly. Indeed, it is this very feature of technology startups—which nearly always begin their lives as small businesses—that has turned the Silicon Valley and other technology centers like Silicon Hills (Austin, TX), Silicon Alley (New York, NY), Silicon Beach (West Los Angeles, CA), the Dulles Technology Corridor (Northern VA), Silicon Harbor (Charleston, SC), and the Gig City (Chattanooga, TN) into major hubs of productivity and technological innovation.

III. Cyber Vulnerabilities

At the same time, this reliance on high-velocity technological innovation and the creation of new intellectual property underlying the products these small, rapidly growing businesses are bringing to market, means that such companies, perhaps more than other parts of the economy, will be increasingly vulnerable to cyber threats. In particular, such companies are vulnerable to having the core of their business stolen out from under them: the particular innovations and associated intellectual property that they have developed to give them an edge in the global marketplace. Indeed, given that the primary focus of small business startups is often developing and bringing new, innovative products to market as fast as possible, it would not be surprising if, perhaps more than other companies, small business startups are likely to make security a secondary or tertiary focus.

This is not to suggest that major U.S. companies do not likewise face major cyber threats. To the contrary, the daily drumbeat of news stories about data breaches targeting major American companies across a wide range of sectors, from financial and information services to healthcare and retail, makes clear that a wide range of global threat actors are aggressively targeting our companies. One report estimates that 707.5 million records were lost worldwide, including accidental losses and malicious data

[8] *See Zettabyte Era*, n. 3 *supra* at 3.

[9] *See Global Internet Report 2015*, n. 7 *supra* at 30.

breaches, in 2015 alone.[10] Of these 707.5 million records, more than 60% were compromised by threat actors, including malicious outsiders (37%), malicious insiders (7%), hacktivists (4%), and state-sponsored actors (15%).[11] And while the overall number represents something of a downtick from the more than one billion records compromised in 2014, it is estimated that the total number of records compromised since 2013 exceeds 3.6 billion.[12] In 2015, the vast majority of the breaches—nearly 75%—took place in the United States.[13] And two of the top five breaches on the Breach Level Index, were American private sector companies in the healthcare and information services sectors, with a third being the massive U.S. government data breach at the Office of Personnel Management.[14]

According to Verizon's 2016 Data Breach Investigation's Report, which examined 2,260 breaches across 82 countries, in 93% of cases, it took attackers minutes or less to compromise systems,[15] a troubling static given the fact Verizon reports that in 83% of cases, victims took weeks or more to find out they had been breached.[16] Even worse, Mandiant reports that for organizations it investigated in 2015, the median time between compromise and breach discovery was 146 days (albeit substantially down from 205 days the prior year and 412 days in 2012).[17] Mandiant also indicated that on average, its "Red Team" was able to gain access to administrative credentials—essentially super-user access—within three days of initially gaining access to a given organization.[18]

Of the 64,000+ incidents and 2000+ breaches that Verizon examined, 16.3% involved insider and privilege misuse, 15% involved denial of service attacks, 12.4% involved crimeware (including ransomware), 8.3% used web app attacks (*e.g.*, e-commerce systems) typically for financial crimes, 1% involved point-of-sale or payment card skimmers, and only 0.4% involved cyber-espionage.[19] Most troubling for small businesses, 70% of the breaches involving insider misuse took months or years to discover.[20] And, while only a small percentage of the incidents and breaches involved cyberespionage, in the manufacturing sector in particular, nearly half of the confirmed breaches (47%) could be classified as cyber espionage.[21]

One of the key challenges facing corporate America today—and perhaps small businesses more than others—is simply making sure their IT infrastructure is up-to-date and that known vulnerabilities are

---

[10] *See* Gemalto, *2015: The Year Data Breaches Got Personal* (2016) at 3, *available online at* <http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf>.

[11] *See id*. at 6.

[12] *See id*. at 3-4.

[13] *See id*. at 2, 12.

[14] *See id.* at 5.

[15] *See* Verizon, *2016 Data Breach Investigations Report: Executive Summary* at 2 (2016), *available online at* <http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf>

[16] *Id*. at 10.

[17] *See* Mandiant Consulting, *M-Trends 2016*, at 4 (Feb. 2016), available online at <>.

[18] *Id*.

[19] *See Verizon 2016 DBIR*, n. 15 *supra* at 4.

[20] *Id*. at 6.

[21] *Id*. at 9.

patched. In a 2016 report, Cisco reported that a one-day scan identified 115,000 of its own devices running on the Internet, 92% of which (106,000 devices) had known vulnerabilities in the software they were running.[22] Cisco further determined that these devices were running software that had, on average, 26 vulnerabilities and, in some cases, Cisco found that its customers in the financial, healthcare, and retail sectors using software more than six years old.[23]

And in troubling news for matters under this Committee's jurisdiction, Cisco's 2015 Security Capabilities Benchmark Study found that small and midsize businesses worldwide "show signs that their defenses against attackers are weaker than their challenges demand."[24] Specifically, the Cisco survey found that as compared to 2014, fewer and fewer small and midsize businesses are using web security, mobile security, vulnerability scanning, and patching and configuration tools, and that of the small to midsized businesses without "an executive responsible for security, nearly one-quarter do not believe their businesses are high-value targets for online criminals."[25] Cisco also found, perhaps unsurprisingly, that small and midsize businesses are less likely to have incident response and threat intelligence teams and that such enterprises "use fewer processes [than large enterprises] to analyze compromises, eliminate the causes of an incident, and restore systems to pre-incident levels."[26] Cisco's main point about why all of this matters is also spot on: not only do businesses of all sizes need to take action to protect their own networks, they must be wary of risks they pose to other, sometimes larger, enterprises.[27]

And while the quantity of records estimated to have been lost to nation-state actors may appear relatively small when compared to other malicious outsiders, these numbers do not fully account for the massive scale and scope of intellectual property theft targeting American private sector businesses by nation-state actors or their proxies, principally China. While such theft has been taking place for many years, it has only been openly discussed in the last five years or so. For example, in 2011, former House Intelligence Committee Chairman Mike Rogers famously noted

> There is an economic cyber war going on today against U.S. companies. There are two types of companies in this country, those who know they've been hacked, and those who don't know they've been hacked. Economic predators, including nation-states, are blatantly stealing business secrets and innovation from private companies.[28]

---

[22] *See* Cisco, *Cisco 2016 Annual Security Report* at 35, *available online at* <http://www.cisco.com/c/dam/assets/offers/pdfs/cisco-asr-2016.pdf>.

[23] *Id*.

[24] *Id*. at 37.

[25] *Id*. at 37-38.

[26] *Id*. at 38.

[27] *Id*. at 39 ("In a security environment where attackers are developing more sophisticated tactics for entering networks and remaining undetected, no business can afford to leave its networks unprotected, or to put off using processes that might offer insights on how a compromise occurred so it can be avoided in the future. In addition, SMBs may not realize that their own vulnerability translates to risks for larger enterprise customers and their networks. Today's criminals often gain entry into one network as a means to find an entry point into another, more lucrative network—and the SMB may be the starting point for such an attack.").

[28] *See* House Permanent Select Committee on Intelligence, *Rogers & Ruppersberger Introduce Cybersecurity Bill to Protect American Businesses from "Economic Predators,"* Press Release (Nov. 30, 2011), *available online at* <http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/113011CyberSecurityLegislation.pdf >.

And in July 2012, then-NSA Director Gen. Keith B. Alexander (now retired),[29] referred to the theft of American private sector intellectual property as "the single greatest transfer of wealth in history."[30]

More recently, in September 2015, James Clapper, the Director of National Intelligence, highlighted the ongoing threat posed capable cyber actors, noting that "cyber threats to the U.S. national and economic security are increasing in frequency, scale, sophistication[,] and severity of impact. Although we must be prepared for large Armageddon-scaled strike that would debilitate the entire U.S. infrastructure, that is not, we believe, the most likely scenario."[31] To the contrary, DNI Clapper noted that the intelligence community's primary concerns are the "low to moderate-level cyber-attacks from a variety of sources which will continue and probably expand….[and which] impose[] increasing costs to our business[es], to U.S. economic competiveness[,] and to national security."[32] Deputy Secretary of Defense Bob Work likewise noted that

> [C]yber intrusions and attacks by both state and non-state actors have increased dramatically in recent years, and particularly troubling are the increased frequency and scale of state-sponsored cyber actors breaching U.S. government and business networks. These adversaries continually adapt and evolve in response to our cyber countermeasures, threatening our networks and systems of the Department of Defense, our nation's critical infrastructure[,] and U.S. companies and interests globally.[33]

DNI Clapper also starkly highlighted the risk posed by our increasing reliance on technology and networked devices. In his September 2015 testimony, DNI Clapper noted that "[b]ecause of our heavy dependence on the Internet, nearly all information communication technologies and I.T. networks and systems will be perpetually at risk."[34] DNI Clapper further expanded on this risk in his more recent testimony in February 2016, where he raised concerns about the increasing use of networked devices that are "designed and fielded with minimal security requirements and testing," and noted that reliance on such devices, combined with the "ever-increasing complexity of networks[,] could lead to widespread vulnerabilities in civilian infrastructures and US Government systems."[35]

---

[29] Gen. Alexander currently serves as the President and CEO of IronNet Cybersecurity, the same company employing the author of this testimony.

[30] *See, e.g.*, Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History,"* Foreign Policy: The Cable (July 9, 2012), *available online at* <http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/>; *see also* Gen. (ret.) Keith B. Alexander, *Prepared Statement of Gen. (Ret) Keith B. Alexander on the Future of Warfare before the Senate Armed Services Committee* (Nov. 3, 2015) at 3, *available online at* <http://www.armed-services.senate.gov/download/alexander_11-03-15>.

[31] *See* Federal News Service, *Transcript: Hearing Before the Senate Armed Services Committee on Cybersecurity Policy and Threats* at 4 *(Sept. 29, 2015).*

[32] *Id.*

[33] *Id*. at 5-6.

[34] *Id.* at 4.

[35] *See* Director of National Intelligence James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community 2016* at 1, House Permanent Select Committee on Intelligence (Feb. 25, 2016), *available online at* <https://www.dni.gov/files/documents/Newsroom/Testimonies/HPSCI_Unclassified_2016_ATA_SFR-25Feb16.pdf>.

DNI Clapper also highlighted "the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other sensitive areas" calling this effort—again principally driven by China—a "persistent threat to US interests" and noted that "[t]he sophistication and availability of information technology that can be used for nefarious purposes exacerbate this threat both in terms of speed and scope of impact."[36]

Key to protecting our nation in cyberspace, therefore, is ensuring the confidentiality, integrity and availability of the information that flows amongst our networked devices. As the DNI noted, this effort to protect our personal and corporate information is under attack from all sides with "cyber espionage [and] criminal and terrorist entities, [] undermin[ing] data confidentiality," with "[d]enial of service operations and data deletion attacks undermin[ing] availability," and an ongoing plague of "cyber operations that [aim to] change or manipulate electronic information [] compromis[ing] its integrity."[37] And, perhaps most concerning of all, we have seen an emergence of actual destructive cyber attacks, that is cyberattacks where cyber or real-world systems, data, or capabilities are permanently destroyed. From the attacks on Saudi Aramco and Qatari Ras Gas in 2012[38] to the attacks on the Las Vegas Sands Corporation and Sony Pictures in 2014,[39] such attacks represent a particularly troubling trend.

Before we turn to how we might work to mitigate the impact of foreign cyber threats on American small businesses, it is worth briefly examining the key foreign threat actors in cyberspace.

IV. Nation-State Threats

The DNI noted in 2015 that "cyber threats come from a range of actors including nation states….with highly sophisticated cyber programs, [such as] Russia and China...And those with lesser technical capabilities but more nefarious intent, such as Iran and North Korea…who are also much more aggressive and unpredictable."[40] And in 2016, the DNI assessed that while both Russia and China "seek

---

[36] *Id*. at 10.

[37] *See Transcript: Cybersecurity Policy and Threats* at 4; *see also Clapper SFR: Worldwide Threat Assessment 2016*, n. 35 *supra* at 2 ("Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decisionmaking, reduce trust in systems, or cause adverse physical effects.")

[38] *See* Director of National Intelligence James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community 2013* at 1, Senate Select Committee on Intelligence (Mar. 12, 2013), *available online at* <https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf>; Kim Zetter, *Qatari Gas Company Hit With Virus in Wave of Attacks on Energy Companies* (Aug. 30, 2012), *available online at* <https://www.wired.com/2012/08/hack-attack-strikes-rasgas/>.

[39] *See* Director of National Intelligence James R. Clapper, *Opening Statement to Worldwide Threat Assessment Hearing*, Senate Armed Services Committee (Feb. 26, 2015), *available online at* <https://www.dni.gov/files/documents/2015%20WWTA%20As%20Delivered%20DNI%20Oral%20Statement.pdf> ("2014 saw, for the first-time, destructive cyber attacks carried out on U.S. soil by nation state entities, marked first by the Iranian attack on the Las Vegas Sands Casino a year ago this month and the North Korean attack against Sony in November. Although both of these nations have lesser technical capabilities in comparison to Russia and China, these destructive attacks demonstrate that Iran and North Korea are motivated and unpredictable cyber actors.")

[40] *See Transcript: Cybersecurity Policy and Threats*, n. 37 *supra* at 4.

greater influence over their respective neighboring regions and want the United States to refrain from actions they perceive as interfering with their interests" they will also "eschew direct military conflict with the United States in favor of contests at lower levels of competition—to include the use of…cyber intrusions, proxies, and other indirect applications of military power—that intentionally blur the distinction between peace and wartime operations."[41]

Specifically, with respect to Russia, the DNI testified that "Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny."[42] According the DNI, Russian cyber operations are likely to focus on "intelligence gathering to support [their] decision-making in the Ukraine and Syrian crises, influence operations to support military and political objectives, and continuing preparation of the cyber environment for future contingencies."[43] This latter aspect, Russia's ongoing effort to put in place capabilities to be employed in the event of a larger future conflict, should be a major concern for officials in the executive and legislative branches. In particular, this Russian effort to prepare the cyber battlespace ahead of time is particularly concerning given that NSA Director Adm. Mike Rogers has indicated that the Russians are the most "capable" of the nation-state cyber actors targeting the United States.[44]

With respect to China specifically, NSA Director Adm. Mike Rogers has indicated that by the sheer "volume" of data taken, China is the largest cyber actor targeting the United States[45] and the DNI made clear that China "continues to have success in cyber espionage against the US Government, our allies, and US companies."[46] Deputy Secretary of Defense Robert Work has testified that "we believe that Chinese actions in the cyber sphere are totally unacceptable as a nation-state," and has noted that "we know that they have stolen information from our defense contractors."[47] And it goes without saying at this point, that China is the single largest source of data exfiltration—particularly of private sector intellectual property—from the United States.[48] And, it is likewise fair to say that the bulk of this theft is

---

[41] *See* DNI Clapper, *SFR: World Wide Threat Assessment 2016*, n. 35 *supra* at 16.

[42] *Id*. at 3.

[43] *Id*.

[44] See *Transcript: Cybersecurity Policy and Threats*, n. 37 *supra* at 4 ("Unknown: Which country, do you believe, is the most committed, successful hacker of the U.S.? Rogers: If you look at volume and nation-state wise -- nation- state wise, I would -- China, the PRC, has been the one that we've been the most vocal about. They're not the only one by any the stretch of the imagination. Unknown: I thought the last time you were here, I recall you saying that you had more concerns over Russia, having more of the ability or expertise to do us damage. Rogers: I thought your question was really focused more on volume. If the perspective is capability if you will, then we've been very public about saying -- I would probably put the Russians. Unknown: Russians? Rogers: In a higher capability. Unknown: But it seems like that China is more committed and determined to do it. Rogers: They certainly do it at a volume level.")

[45] *Id*.

[46] *Id*. at 3.

[47] *Id*. at 14.

[48] *See* House Permanent Select Committee on Intelligence, *H. Rept. 112-445* (2012) at 5, *available online at* <https://www.congress.gov/112/crpt/hrpt445/CRPT-112hrpt445.pdf> ("Perhaps most troubling, these efforts are targeted not only at sensitive national security and infrastructure information, but are also often aimed at stealing the corporate research and development information that forms the very lifeblood of the American economy. China, in particular, is engaged in an extensive, day-in, day-out effort to pillage American corporate and government information. There can be no question that in today's modern world, economic security is national security, and the government must help the private sector protect itself.");

undertaken by government actors or their proxies, with an eye towards gaining an edge for China in the global marketplace.[49] And, notwithstanding the September 2015 joint commitment between the United States and China to not "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors,"[50] the DNI made clear within days of the deal that he was not optimistic about its prospects.[51]

Moreover, in Feb. 2016, Director Clapper testified that while "[w]e have seen some reduction" in Chinese industrial espionage, in his view, the United States is not "in a position to say at this point whether [China is] in strict compliance."[52] CIA Director John Brennan recently testified that Chinese cyber espionage against American businesses has not ended and that while he "see[s] some effort by the Chinese government to follow through on some of the commitments they've provided in political channels" he "continue[s] to be concerned about the cyber capabilities that reside within China, as well as the actions that some continue to undertake."[53] And while a recent report from FireEye iSight Intelligence indicates a sustained drop-off in the quantity of active network compromises by 72 China-based groups since mid-2014,[54] the report also highlights 13 China-based groups that have actively compromised corporate networks in the U.S., Europe, and Japan between late 2015—after the September 2015 agreement was signed—and early 2016.[55] Indeed, the number of network compromises per month between October 2015 and May 2016, albeit lower than any time in the past two years, has stayed fairly

---

see also House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Oct. 8, 2012), *available online at* <https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf> ("Chinese actors are also the world's most active and persistent perpetrators of economic espionage.")

[49] *See id*.

[50] *See* White House, *Fact Sheet: President Xi Jinping's State Visit to the United States* (Sept. 25, 2015), available online at <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

[51] *See Transcript: Cybersecurity Policy and Threats*, n. 37 *supra* at 8 ("McCain: As a result of the Chinese leader in Washington there was some agreement announced between the United States and China. Do you believe that that will result in an elimination of Chinese cyber attacks? Clapper: Well, hope springs eternal. I think we will have to watch what they're behavior is and it will be incumbent on the intelligence community I think to depict, portray to policymakers what behavioral changes if any, result from this agreement. McCain: Are you optimistic? Clapper: No.")

[52] *See* Federal News Service, *Transcript: Hearing Before the House Permanent Select Committee on Intelligence* at 15 (Feb. 25, 2016) ("Himes: I wonder if you could characterize whether those agreements have been effective in reducing the amount of cyber espionage and cyber activity that we've seen out of China. Clapper: We did probably go into that in more detail on a closed session. As I indicated in my oral remarks, I think the jury's out. We have seen some reduction but I don't think we're in a position to say at this point whether they're in strict compliance. And we can go into that in more detail in a closed session.").

[53] *See* Federal News Service, *Transcript of Hearing Before the Senate Select Committee on Intelligence on CIA Intelligence Activities* at 14 (June 16, 2016) ("Blunt: Let me ask one additional question about China and cyber attacks. Last year, the president announced a common understanding with China's leadership that neither country would conduct, or knowingly support cyber-enabled threat of intellectual property for commercial advantage. In your view, does that mean that cyber-enabled theft of intellectual property by people from china has ended? Brennan: No.").

[54] *See* FireEye iSight Intelligence, *Redline Drawn: China Recalculates Its Use of Cyber Espionage* at 10-11 (June 2016), *available online at* <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>.

[55] *Id*. at 4, 13

constant.[56] That is, while such compromises by China-based actors may have been on a downward trend, ascribing the trend to the September 2015 agreement seems questionable, at best. To the contrary, given that rates have stayed relatively stable since the agreement, one must assume the agreement had limited effect, if any, on China's cyber behavior. As such, while the overall reduction may be laudable, it is unclear whether this truly represents a positive change in behavior or simply evinces a more focused set of cyber activities by China aimed at higher value Western targets.

Another key threat posed by China in the cyber realm, beyond its extremely aggressive policy of cyber theft, is its ostensible effort to obtain access to key U.S. and allied infrastructure. The House Permanent Select Committee on Intelligence, in a report issued in October 2012 after a nearly year long investigation, warned that "[t]he United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies."[57] Specifically, the report recommended that "the Committee on Foreign Investment in the United States (CFIUS) [] block acquisitions, takeovers, or mergers involving [Chinese telecommunications companies] Huawei and ZTE given the threat [these companies pose] to U.S. national security interests."[58] The report further recommended that "U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts" and that U.S. "government contractors—particularly those working on contracts for sensitive U.S. programs—should exclude ZTE or Huawei equipment in their systems."[59] Finally, as relevant here, the report recommended that "[p]rivate-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services," and stated that, in particular, "U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects" because "[b]ased on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems."[60] Given the warnings provided in the HPSCI report, in addition to taking steps to protect themselves against external intrusions, it is important that U.S. businesses—large and small alike—and particularly those in the infrastructure services area, take seriously the potential security threat posed by such companies and take appropriate steps to minimize or otherwise mitigate such risk.

With respect to both Iran and North Korea, the DNI made clear that both are prepared to use cyber to support their political objectives. In the case of Iran, the DNI noted that Iran "used cyber espionage, propaganda, and attacks in 2015 to support its security priorities, influence events, and counter threats—including against US allies in the region."[61] And in the case of North Korea, the DNI made clear his assessment that "North Korea probably remains capable and willing to launch disruptive or destructive cyberattacks to support its political objectives" and specifically noted that South Korea had determined that "North Korea was probably responsible for the compromise and disclosure of data from a South Korean nuclear plant."[62]

---

[56] *Id*. at 11.

[57] *See HPSCI Huawei-ZTE Report*, n. 48 *supra* at vi.

[58] *Id.*

[59] *Id*.

[60] *Id.* at vi-vii.

[61] *See* DNI Clapper, *SFR: World Wide Threat Assessment 2016*, n. 35 *supra* at 3.

[62] *Id*.

V. Non-State Actors

Non-nation state entities also use cyberspace extensively. From organized criminal groups motivated by financial gain and terrorist groups seeking to recruit assets, plan operations, or conduct information operations[63] to hacktivists motivated by ideology and individual criminals or extremists with capable skills, there is no shortage of non-state actors looking to target Americans and their businesses online. In addition to the noting the now run-of-the-mill online marketplaces on the deep- or dark-web where illicit goods and information may be transferred, the DNI recently identified an increasing effort by terrorist groups to experiment as they seek to develop more advanced capabilities.[64] Moreover, the increasing use by criminals of "ransomware" to "block user access to their own data, sometimes by encrypting it, is becoming a particularly effective and popular tool for extortion for which few options for recovery are available" is a significant problem for individuals and businesses alike.[65]

VI. Opportunities to Help Small Business to Protect Themselves

What can small businesses—and the government—do to help address these problems?

First, like large businesses, small businesses must get buy-in for the need for cybersecurity at all levels of the company from the Board of Directors, to the C-suite, and down from there. Such buy-in will help drive appropriate resource allocation decisions that may not otherwise be prioritized. Indeed, Cisco's survey of cybersecurity professionals determined that, regardless the sophistication or cybersecurity maturity of the organization, the single biggest set of obstacles to adopting advanced security processes and technologies were budget constraints, identified as challenges by 38-48% of such professionals.[66]

Second, small businesses must consider working together—for example, within a given industry—to leverage their buying power for cybersecurity services and to take advantage of common services, such as a common security operations center, large scale cyber defense system, and the like.

Third, small businesses must find a way to work with the government and with larger businesses to share cyber threat information in real time, at network speed. Unlike large businesses that may have a fighting chance—albeit it perhaps small—to adequately defend themselves from a committed, capable cyber threat actor, small business are significantly more challenged. And, given the reality of the threat actors targeting American business today, traditional cyber defenses—whether deployed by a large or small business—are ill positioned to respond in a timely and effective fashion.

Fourth, the government must get more serious about deterring nation-state threat actors. To date, our government's ostensibly new, forward-leaning cybersecurity policy has led to one set of symbolic

---

[63] *See* DNI Clapper, *SFR: World Wide Threat Assessment 2016*, n. 35 *supra* at 3 (highlighting the use of cyberspace by terrorist groups to "organize, recruit, spread propaganda, collect intelligence, raise funds, and coordinate operations" and to conduct information operation campaigns designed to "spur 'lone-wolf' attacks.")

[64] *See Transcript: Cybersecurity Policy and Threats*, n. 27 *supra* at 5.

[65] *See* DNI Clapper, *SFR: World Wide Threat Assessment 2016*, n. 35 *supra* at 4.

[66] *See, e.g.*, *Cisco 2016 Annual Security Report*, n. 22 *supra* at 51.

indictments—with little chance of an actual trial—a cyber sanctions executive order that has sat unused, and a cyber agreement with China that appears to be being honored in the breach at best. Real deterrence in cyberspace will require the government to be more transparent about its offensive capabilities, to be more clear about the conditions under which it would feel obliged to use such capabilities, and to act on such conditions if they come to pass.

Fifth, the government must work to provide more detailed information about the cyber threats facing our nation to key business and political leaders, including as necessary, providing security clearances and access to information at the TS/SCI level.

Sixth, the government must consider positive incentives—particularly for small businesses—to encourage appropriate investment in cybersecurity and information sharing, including, as appropriate, tax credits for such activities.

Seventh, Congress should consider modifying the Cybersecurity Information Sharing Act of 2015, enacted at the end of last year, in order to provide better incentives for, and to remove barriers to, sharing of cyber threat information.[67]

This short list of ideas represents but a partial starting point for Congress and the private sector to consider going forward in addressing these critical issues.

Thank you for offering me the opportunity to participate in this important dialogue. I look forward to your questions.

[67] *See* Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, __ S. Car. L. Rev. ___ (forthcoming 2016) (describing steps Congress might take to address some of the potential shortcomings in CISA 2015).