Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

A Borderless Battle: Defending Against Cyber Threats

Testimony of Frank J. Cilluffo
Director, Center for Cyber and Homeland Security
The George Washington University

Before the U.S. House of Representatives
Committee on Homeland Security

March 22, 2017

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

Chairman McCaul, Ranking Member Thompson and distinguished Committee Members thank you for the opportunity to testify before you today on this subject of national importance. As cyber threats continue to multiply and evolve, your resolve to explore this complex yet critical area is commendable. My testimony will focus primarily on the nature of the threat—including how to think about the major threat actors and their behavior—but will also contain thoughts on how best to respond to the vexing economic and national security challenges associated with America's digital footprint.

As individuals, businesses, and government entities choose to increasingly utilize the advantages of the internet, they expand their exposure to the security vulnerabilities of information technologies that ever more sophisticated and persistent threat actors seek to leverage for political or monetary gain. Magnifying the security problems of growing vulnerabilities and already thinly stretched cybersecurity resources, the threat tempo is accelerating. This is due to a variety of factors including the continued advantage of offense over defense in cyberspace, the added efficiencies associated with division of labor and specialization in the maturing economy for cybercrime, and the weak deterrent force of nascent policy responses that have yet to fully account for the diverse and transnational nature of cyber threats. The first step to addressing the policy problems created by these trends is to seek to understand the complexities of the cyber threat. In order to do so, we should conceive of it as a spectrum upon which the many and varied threat actors can be placed. Not all hacks and not all hackers are the same. To the contrary both intentions and capabilities vary widely:

Nation-States. At the high end of the spectrum are nation-states whose military and intelligence services are both determined and sophisticated in the cyber domain. Russia, China, Iran and North Korea presently top the list; but it is important to understand that every country with a modern military and intelligence service now possesses computer network exploitation (CNE) and computer network attack (CNA) capability. Indeed the line between the ability to exploit and the ability to attack is reed-thin and turns simply upon the question of intent. Also keep in mind that cyber strategy and tactics must be understood in context—as part and parcel of other geopolitical tools and goals (military, political, economic)—not in isolation from them.

Nation-states often use proxies to do their bidding. Countries do so for a range of reasons including to augment capabilities or to obfuscate the true source of the intrusion or attack thereby affording plausible deniability. Depending upon the reason(s) for which their services have been engaged, the proxy may be state-sponsored, state-supported or state-sanctioned.

In previous testimony before this committee I have discussed in detail the capabilities and intentions of the four leading threat actors.[1] Building on that baseline, today I will highlight the latest developments regarding these countries. Note however that the most sophisticated threats

[1] See for example: Statement of Frank J. Cilluffo before the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, "Emerging Cyber Threats to the United States," February 25, 2016. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HHSC_Testimony_Feb%2025-2016_Final.pdf. Also see the resource document, Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, February 22, 2017. http://www.defenddemocracy.org/content/uploads/documents/22217_Cyber_Definitions.pdf

that we face emanate from Russia and China which have both integrated CNA and CNE into their warfighting strategy and doctrine.

Russia: Russia has a long history of cyber aggression against other nations; to wit: Estonia (2007), Georgia (2008), and Ukraine (2014-15, and continuing). Russian efforts persisted in 2016-17, with attempts to interfere in the U.S. election, and information operations targeting multiple countries in both eastern and western Europe—including those with upcoming elections, such as France and Germany. Russia has been particularly adept at integrating cyber into its strategic plans and operations. In February 2017, Russia's Defense Minister acknowledged that the country had created a new military branch: "information warfare troops."[2]

In the cases of Ukraine and Georgia, Russia combined cyber and kinetic operations; and in the case of Ukraine, Russia is believed to have perpetrated the first-ever electricity blackout caused by computer network attack. In recent years, Russia has demonstrated an increasing level of assertiveness in the cyber domain, showing—in the words of then-Director of National Intelligence James Clapper—a "willingness to target critical infrastructure systems and conduct espionage operations even when detected."[3]

In 2009, the Wall Street Journal reported that cyber-spies from Russia (and China) had penetrated the U.S. electrical grid, leaving behind software programs, and trying to navigate the systems and their controls. What purpose could the mapping of U.S. critical infrastructure serve, other than intelligence preparation of the battlefield? The NASDAQ exchange too has allegedly been the target of a "complex hack" by a nation-state; again one questions the motivation.

In Russia, the forces of crime, business, and politics have long converged in a toxic blend; and there is evidence of complicity between the Russian government and cyber-criminals and hackers. Over time, Russian hackers believed to be doing their government's bidding have breached the White House, the State Department, and the Defense Department.

China: China has demonstrated a remarkable level of persistence evidenced by the sheer number of acts of espionage that the country has committed. These aggressive collection efforts have amassed secrets (military – including plans for the F-35, commercial/proprietary, etc.) in order to propel China's economic growth, military power, and technological & scientific capacities—and thereby gain strategic advantage in relation to (actual and perceived) competitor countries and adversaries. In May 2015, data theft on a massive scale, affecting virtually all U.S. government employees, was traced back to China. The extent to which the information gleaned from this hack of the U.S. Office of Personnel Management (OPM) may be used to blackmail and recruit Americans, to China's benefit, remains to be seen.

---

[2] Vladimir Isachenkov, "Russia Military Acknowledges New Branch: Info Warfare Troops," The Associated Press, February 22, 2017. http://www.bigstory.ap.org/article/8b7532462dd0495d9f756c9ae7d2ff3c/russian-military-continues-massive-upgrade

[3] James R. Clapper, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record before the U.S. Senate, Armed Services Committee, February 9, 2016. http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

In September 2015, China and the United States reached an agreement on refraining from conducting economic cyber-espionage. Initially this agreement appeared to reduce the level of activity, although it may simply have pushed China's efforts in a different direction: greater efforts directed at U.S. government (rather than U.S. corporate) targets can be expected, moving forward; in addition, a notable spike in Chinese cyber activity in the region (China's "neighborhood") has been observed. Since the 2015 Obama-Xi agreement, moreover, China appears to have shifted from use of the People's Liberation Army (PLA) to relying more on its security and intelligence services for a greater role in hacking foreign companies. However military officers in China are increasingly known to moonlight as hackers for hire, when off the clock. While Russia has received an overwhelming amount of attention during the past year, this should not detract from the cyber activities and threat posed by other state actors.

Iran. Iran has invested heavily in recent years in order to deepen and expand its cyber warfare capabilities, although this capacity was initially directed internally to repress democratic forces in the country. This effort came in the wake of the Stuxnet worm, which targeted Iran's nuclear weapons development program. In recent years Iran has engaged in a concerted cyber campaign against U.S. banks. U.S. officials also believe Iran to be responsible for a cyber-attack against the Sands Casino in Las Vegas owned by politically active billionaire Sheldon Adelson; the attack wiped clean many hard drives and sought to destroy corporate infrastructure. Hackers linked to the Iranian government have also used cyber means to compromise the control system of a dam north of New York City. Iran has long relied heavily on proxies such as Hezbollah—which now has a companion organization, Cyber Hezbollah—to strike at perceived adversaries. Iran and Hezbollah are believed to have perpetrated the cyber-attacks against Saudi Aramco and Qatari RasGas, which compromised 30,000 computers. Elements of Iran's Revolutionary Guard Corps (IRGC) have also relied upon proxy forces including political/criminal hackers, to work on behalf of the regime.

Iran is expected to hold a presidential election in May 2017. Should a hardline candidate prevail, there may well be a further uptick in the country's aggressive behavior in cyberspace. U.S.-Iran relations moving forward are yet to be fully defined, given that there is also a new administration in the United States that has been in office for just two months. However the Joint Comprehensive Program of Action (JCPOA) regarding Iran's nuclear program looms large in the background. Depending upon U.S. actions and policy in this area—including whether the administration retains the agreement and how it handles the matter of sanctions against Iran—the Iranian regime may decide to act out further in the cyber domain. Notably the JCPOA has resulted in substantial funds being placed in Iranian hands through sanctions relief. The regime will likely devote these funds to the further expansion of its cyber capabilities (offensive/defensive) and should either party move to annul the agreement, we can expect a significant increase in cyber activity against U.S. interests and assets.

North Korea. Many of the details about North Korea's cyberwarfare capabilities are shrouded in secrecy (the same is true of their military capabilities writ large). What we do know is that, much like Iran, North Korea has invested heavily in building cyber capabilities. A recent report by the South Korean Defense Ministry estimates that the North Korean "cyber army" employs an elite squad of 6,000 hackers, many of whom operate abroad in northeast China and

throughout South East Asia.[4] And what North Korea lacks in capability it makes up for with intent (again, like Iran). North Korea has shown little restraint, engaging in computer network attack—disruptive and/or destructive attacks (rather than espionage).

In recent months, there has been a major increase in North Korean cyber-attacks (attempted and successful) targeting South Korean companies and government.[5] Senior Japanese cybersecurity officials confirmed this in recent meetings, and expressed significant concern about both the increase in volume and aggressiveness of North Korean cyber activity. Outside the region, North Korea also operates without compunction, targeting U.S. companies; the most notorious case is their attack on Sony Pictures Entertainment. Recent news articles revealing alleged U.S. cyber activities aimed at stymieing North Korea's ballistic missile program will likely serve to increase the likelihood of additional North Korean cyber-attacks.

North Korea has long turned to illicit activity such as counterfeiting (of bills, pharmaceuticals, and cigarettes) to fill its coffers. More recently the country has turned to cybercrime and is the prime suspect in a string of bank heists. The latest round of UN economic sanctions aimed at North Korea, coupled with China's suspension of coal imports to the country, suggest we ought to be prepared for a spike in North Korean state-sponsored and/or state-supported cybercrime.

Criminal Enterprises. After nation-states, criminal organizations are the next most capable threat actors. Increasingly, the capabilities that used to be the exclusive preserve of nation-states are now in the hands of criminal entities[6]—which outstrip the present abilities of foreign terrorist organizations (FTOs) in this particular regard. Criminal groups are motivated by profit rather than politics or ideology, yet their pursuit of monetary gain often has broader impacts on the integrity of the global economic system which in turn is closely linked to international security. Cyberspace allows criminals to take their malicious activities to a global scale. Powerful organizations, like the recently dismantled Avalanche criminal network can thus create cybercrime tools and infrastructure that can bring malicious actors together so that they may collectively pose a transnational threat to the operations of governments and private entities.[7] The cross-border and interjurisdictional approach of Europol and its partners in the United States and elsewhere to take down the Avalanche group is a testament to the resources and coordination required to effectively address such threats.[8] It is important to note that while cybercriminals are unlikely to ever have the ability to collect and use all-source intelligence as governments can, the gap between the capabilities of sophisticated cyber criminals and nation states is increasingly narrowing. Compounding this challenge is that fact that criminal groups are working ever-more

[4] Martin Anderson, "North Korea's Internet Tundra Breeds Specialised "Cyber Forces" Numbering 6,000," The Stack, January 7, 2015. https://thestack.com/security/2015/01/07/north-koreas-internet-tundra-breeds-specialised-cyber-forces-numbering-6000/

[5] Charlie Campbell, "The World Can Expect More Cybercrime from North Korea Now that China has Banned its Coal," Time, February 19, 2017. http://time.com/4676204/north-korea-cyber-crime-hacking-china-coal/

[6] Doug Olenick, "Cybercriminal's skills now on par with nation states: Mandiant," SC Magazine, March 14, 2017. https://www.scmagazine.com/cybercriminals-skills-now-on-par-with-nation-states-mandiant/article/644124/

[7] Brian Krebs, "Avalanche Global Fraud Ring Dismantled," Krebs on Security, December 16, 2016. https://krebsonsecurity.com/2016/12/avalanche-global-fraud-ring-dismantled/

[8] "Avalanche Network Dismantled in International Cyber Operation," Europol, December 1, 2016. https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

either with or for nation-states such as Russia. The Yahoo hack (2014) that compromised 500 million user-accounts and led to the recent indictment of four individuals—two FSB (Russian domestic intelligence) officers and two cybercriminals—is a case that demonstrates the willingness of states to utilize criminals for hire as proxies.[9]

This convergence of nation-state and criminal forces heightens the dangers posed by both; and also makes it difficult to discern just who is master and who is puppet. Traditionally it has been the forces of crime that seek to penetrate the state; yet in the case of North Korea for example, the opposite is true: the regime engages criminal proxies and their cyber prowess to help achieve the ends that will perpetuate the regime's survival. This tactic is easier than ever to pursue with the emergence of the market model of "Crime-as-a-Service,"[10] which facilitates cybercrime by making the tools and skills needed for it more readily accessible to a wider variety of actors. Compounding the challenge for law enforcement, nations such as Russia and China amount to virtual safe havens for cyber criminals since the United States lacks extradition treaties with these countries.

Foreign Terrorist Organizations. For Foreign Terrorist Organizations (FTOs) there is no shortage of motivation or intent but fortunately, FTOs have yet to fully develop a sustained cyber-attack capability. While this is reassuring to a certain extent, it does not mean that such actors pose no threat in the cyber domain. Even outside of the cyber context, the most pressing threats from terrorist organizations stem from their ability to execute asymmetric, "no-warning" attacks, that do not rise to the level of impact associated with persistent state to state competition or conflict. Nevertheless, such operations can endanger the lives of civilians and interfere with the integrity of critical infrastructure. Therefore, while FTOs are not likely to pose a catastrophic risk to the homeland or America's economy in the near future, it would be imprudent to ignore the efforts of these actors to utilize the internet to their advantage and acquire cyber capabilities that they can then integrate with kinetic force to execute the equivalent of a cyber drive by shooting.

Those FTOs that are currently most concerning from a cyber threat standpoint are entities that benefit from state support or sponsorship and those affiliated with the Islamic State in Iraq and Syria. The western world has already seen the troublesome effects of ISIS' use of the internet to spread propaganda and radicalize vulnerable populations, but their efforts do not stop there. Members of ISIS have repeatedly utilized a tactic known as "doxing" to target U.S. military and law enforcement personnel through the strategic release of their stolen personal information and social media intelligence collection. Also of note, a group known as the United Cyber Caliphate (UCC), which increasingly appears to be functioning as a cyber arm of ISIS, has touted its accomplishments in the realms of hacking and DDoS attacks, and has announced plans to launch a cyber attack against the United States in the near future. America's efforts to target high-value leaders of ISIS, including its most prolific cyber aggressors Junaid Hussain and the UCC's Osed

[9] Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

[10] EUROPOL, European Union, Serious and Organised Crime Threat Assessment, 2017: Crime in the age of technology. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Agha, have demonstrated their capacity to successfully set back ISIS' cyber capabilities. Such groups deserve the continued attention of security officials, especially in cases where they can leverage associations with other malicious actors to augment their cyber capabilities.

Hacktivists. Whether acting alone or loosely in tandem, hacktivists may possess considerable skill and cause significant disruption when they perceive their core interests to be at stake. Oftentimes, hacking collectives such as Anonymous, can leverage their sheer numbers to overwhelm servers and shut down websites or exploit vulnerabilities to bring attention to their cause of the day. While these movements lack the type of centralized command and control infrastructures that would make their influence more troubling, their sometimes populist appeal and dispersed manpower allow them to operate in unique ways that undermine American security interests.

While hacktivists, including malicious insiders, vary in degree of sophistication and tend to be leaderless, their ability to spread discord online can augment existing digital vulnerabilities and reinforce the efforts of other malicious cyber actors. Therefore, they should not be discounted when assessing the wider cyber threat spectrum. Even in the case of unsophisticated hacktivists, who may not possess extensive "in-house" cyber expertise, we must consider the increasing ease with which such malicious actors can simply buy or rent the requisite tools or services on the Deep Web and Darknet(s). Only a small percentage of the material available on the internet is indexed and accessible from standard search engines. Beneath the surface web that we all see is the unindexed Deep Web and its subcomponent, the Darknet, which can only be accessed through password protected sites or when using specific software such as TOR or I2P.[11] It is in such realms of the internet that malicious actors – including FTOs - buy and sell hacking tools and expertise and fence stolen information. As the ability to trade in malicious cyber expertise becomes more prevalent, it is in fact necessary to consider the impacts of this trend in all threat assessments, agnostic to the specific actor in question.

Cyber Domain: Characteristics, Evolution and Vulnerabilities

In the cyber domain, the advantage lies with the attacker. At the same time, the surface of attack has expanded exponentially with the advent of the Internet of Things. However, the dynamism of this environment should not be underestimated and we must recognize that the capabilities of both attackers and defenders in cyberspace are continually changing. Looking ahead, U.S. officials warn that simple theft or disruption of data may give way to data manipulation.[12]

Increasingly, threat actors are setting their sights on America's critical infrastructure which cuts across the public and private sectors. While the U.S. approach of designating 16 sectors critical is sound, not all of these sectors are equally critical. What are known as the "lifeline" sectors— in particular, the energy and electric sectors, water, telecommunications, transportation and financial services -- have an even greater impact on public safety and security than the others.

---

[11] "Illuminating the Deep and Dark Web: The Next Frontier in Comprehensive IT Security," Flashpoint Intel, 2015. https://www.flashpoint-intel.com/book/illuminating-deep-dark-web.

[12] Spencer Ackerman, "Newest cyber threat will be data manipulation, US intelligence chief says," The Guardian, September 10, 2015. https://www.theguardian.com/technology/2015/sep/10/cyber-threat-data-manipulation-us-intelligence-chief

The potential for cascading effects if any of these were rendered inoperative or dysfunctional, especially for a significant length of time, further magnifies their importance. From the standpoint of prevention and response, it is these areas that should be treated as top priority (while bearing in mind the adage that if everything is a priority then nothing truly is). Section 9 of Executive Order 13636 on Improving Critical Infrastructure Cybersecurity provides the framework for a "risk-based approach" of this type.[13]

Examples of cyber incidents and intrusions are regrettably plentiful, but a few cases merit mention here in order to bring into sharper relief some of the concepts referenced above:

SWIFT Hacks: The first case that rises above the noise and warrants attention is the theft of $81 million from the Central Bank of Bangladesh in February 2016 and similar yet less successful attempts at other major banks in the developing world. In the case of Bangladesh Bank, it would have been a $950 million heist had the request not set off alarms due to a coincidental similarity between the address of a bank in which hackers sought to deposit their stolen funds and the name of a corporation sanctioned by the U.S. government.[14] Although $81 million is a significant sum, the loss of which doubtlessly had significant, negative impacts on the bank and its clients, the global economy can absorb relatively minor losses such as this one. From the perspective of security officials, the real worry is how hackers perpetrated this crime and the systemic vulnerabilities in the global financial order that such a cyber heist publicly highlighted. The hackers stole the credentials of target banks to gain access to SWIFT, the interbank messaging system that connects 11,000 banks and financial institutions globally and settles billions of dollars of transactions daily. From there, hackers were able to place illegitimate requests for transfers of funds that most banks fulfill automatically.[15]

These attacks exposed a potential single-point of failure in a system that modern economies depend upon every day. We still do not know the full extent to which hackers have compromised SWIFT's member-banks, but SWIFT recently disclosed that its members have suffered a number of other hacking incidents through its messaging infrastructure in the last year, in which about one in five resulted in stolen funds.[16]

The Carbanak Gang: In 2013, the so-called Carbanak gang perpetrated a series of well-orchestrated assaults on eastern European and Russian banks. Named after the malware used, the Carbanak gang compromised internal bank systems and sent commands directly to ATMs (a scheme known as "ATM jackpotting") throughout eastern Europe, causing the machines to dispense cash. More than 100 banks spanning 11 countries were hit—with losses of hundreds of millions of dollars—highlighting just how much damage cyber-criminals can do.[17] The activities

[13] February 12, 2013. https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
[14] Krishna Das and Jonathan Spicer, "How the New York Fed Fumbled of the Bangladesh Bank Cyber-Heist," Reuters, July 21, 2016. http://www.reuters.com/investigates/special-report/cyber-heist-federal/
[15] Devlin Barrett and Katy Burne, "Now It's Three: Ecuador Bank Hacked via Swift," The Wall Street Jounral, May 19, 2016. https://www.wsj.com/articles/lawsuit-claims-another-global-banking-hack-1463695820
[16] Tom Bergen and Jim Finkle, "Exclusive: SWIFT Confirms New Cyber Thefts, Hacking Tactics," Reuters, December 12, 2016. http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT
[17] David E. Sanger and Nicole Perlroth, "Bank Hackers Steal Millions via Malware," The New York Times, February 14, 2015. https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?partner=socialflow&smid=tw-nytimes&_r=2; Brian Krebs, "Carbanak Gang Tied to Russian Security

of the Carbanak gang continue unabated with new techniques at their disposal and new targets in their crosshairs.

Energy Grid Attacks: On December 24, 2015, western Ukraine experienced a power outage that is believed to have been caused by cyberattack perpetrated by Russia. Though just one power company reported the incident, "similar malware was found in the networks of at least two other utilities."[18] More than four dozen substations were affected, as were more than a quarter of a million customers for up to six hours. In addition, a simultaneous attack on call centers (a telephony denial of service attack) hindered communication and customer reporting of difficulties. The case is truly significant: it is believed to represent the first time that a blackout was caused by computer network attack. But it would not be the last: again, in December 2016, Ukraine witnessed a cyber-attack on their power grid, leaving part of Kiev without power. Once more, all the evidence points to Russia (or its proxies) as perpetrator. These incidents represent a crossing of the Rubicon: a cyber-attack creating real–world, physical implications. The attacks thus sent a message that was loud and clear.

Mirai Botnet: Botnets, or networks of internet connected devices that unbeknownst to their legitimate users can be centrally controlled to perpetrate malicious cyber activities on a grand scale, have been around for a long time. However, this past fall, the Mirai botnet demonstrated how the concept of distributed computing power and centralized command and control can leverage the rampant insecurity associated with the expanding Internet of Things environment. Malicious actors used the botnet, which was primarily made up of vulnerable webcams and internet routers, to execute the most powerful DDoS attack in history against the computer security blogger Brian Krebs.[19] More alarmingly, the Mirai botnet later used a DDoS attack to target Dyn, which supports much of the internet's infrastructure, and successfully interrupted the services of Spotify, Twitter, and PayPal for millions of users.[20] The cases of the Mirai botnet's DDoS attacks are significant because they are just the beginning of what security officials can expect from malicious actors seeking to leverage the digital vulnerabilities of IoT devices and the widespread ignorance or apathy of IoT producers and consumers to these security concerns. Society must begin to consider security over convenience and necessity over luxury when connecting devices, even those that seem relatively innocuous, to the internet. Otherwise, malicious actors will continue to benefit from the bountiful harvest of vulnerable devices ready to be recruited for criminal and other malicious purposes. Currently, estimates show that around tens of billions of devices will be connected to the internet by 2020, an exponential growth in connectivity that runs parallel to a growth in the digital attack surface.[21]

Firm?" Krebs on Security, July 18, 2016. https://krebsonsecurity.com/2016/07/carbanak-gang-tied-to-russian-security-firm/

[18] Reuters, "Experts: Ukraine Utility Cyberattack Wider than Reported," Voice of America, January 5, 2016. http://www.voanews.com/a/reu-experts-ukraine-utility-cyberattack-wider-than-reported/3131554.html

[19] Lily Hay Newman, "The Botnet that Broke the Internet isn't Going Away," Wired, December 9, 2016. https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

[20] Brian Krebs, "Did the Mirai Botnet Really take Liberia Offline?" Krebs on Security, November 4, 2016. https://krebsonsecurity.com/tag/mirai-botnet/

[21] BI Intelligence, "Here's How the Internet of Things Will Explode by 2020," Business Insider, August 31 2016. http://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-2

U.S. Response

The many and varied cyber threats that the United States faces requires a multidimensional response. While the U.S. should continue to invest in its offensive cyber capabilities to, as best as possible, ensure its superiority and escalatory dominance, a powerful defensive component is essential to America's cybersecurity and underlies all the rest. Resources and funding should therefore be balanced between offensive and defensive capacity building. A clearly articulated deterrence strategy is also needed, but remains in its infancy—although the recent Defense Science Board report on the subject is a solid step in the right direction.[22] An effective cyber deterrence strategy should utilize various levers of state power to affect the cost benefit analysis of malicious actors by denying them benefits by demonstrating America's capability and willingness to impose costs on such malicious actors. Cyber deterrence requires more than military underpinnings and the same is true of U.S. cyber response more generally. Public-private partnerships are instrumental to cybersecurity; and the public sector component of that equation includes not only Federal entities but also their State and Local counterparts. Whether partnering with companies or State and Local officials, the Department of Homeland Security (DHS) plays an important and meaningful role in terms of enabling U.S. responses to cyber threats, distinct from the Department of Defense mandate in this area.

Cybersecurity requires both a whole of government and whole of society approach. Government alone cannot get us to where we need to be. Industry and even individuals must each do their part; and industry sectors must collaborate within bounds (with competitor companies) as well as across bounds (with other sectors and with government at all levels). Developments such as the expansion of the Internet of Things serve to reinforce these imperatives.

Private sector initiatives of the type needed are already underway. The financial services sector in particular is leading the way with its Information Sharing and Analysis Center (FS-ISAC), a global industry forum for cyber (and physical) threat intelligence analysis and sharing; and with the Financial Systemic Analysis and Resilience Center (FSARC), intended to deepen threat analysis and mitigate systemic risk.[23] To lead and respond effectively however, companies require the tools to do so—which is why the FSARC works together with government partners including DHS, whose expertise complements that of industry members.

More broadly, the private sector as a whole must be empowered to respond proactively and robustly in the face of cyber threats. Businesses never expected to find themselves on the front lines of cyber-battle, facing sophisticated adversaries with nation-state capabilities. In such circumstances, companies must take steps (ahead of time or in real-time) to protect their data and networks, particularly their crown jewels. In turn, government has a responsibility to clarify the parameters of acceptable corporate action so that businesses fully understand what they can and cannot do in this regard. For those areas deemed outside corporate jurisdiction, government has a responsibility to step in and support/protect the targeted entities and assets. Regrettably the

[22] Department of Defense, Task Force on Cyber Deterrence, February 2017. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

[23] Michael Chertoff and Frank Cilluffo, "Trump Administration Can Help Finance Sector Shift Cybersecurity Paradigm," Forbes, January 18, 2017. https://www.forbes.com/sites/realspin/2017/01/18/trump-administration-can-help-finance-sector-shift-cybersecurity-paradigm/#72d07df0645d

discussion surrounding these issues has been less than nuanced to date; yet there is much that can be done in terms of active defense, apart from the two poles of doing nothing at all or "hacking back."[24] Public and private sector actors should work to jointly develop the private sector's capacity and authorities to utilize active defenses, capabilities that when developed and marshalled responsibly, can begin to flip the equation and give cyber defenders a fighting chance.

The operating principles set out above (e.g., the need for a whole of government approach and public-private partnerships) is equally important at the international level. Alliances between the U.S. Department of Defense and other nation-states' military services – such as NATO - are one crucial component of a solid response posture vis-à-vis cyber domain; but so too are non-military alliances between the United States and foreign governments and companies. While the Five Eyes alliance has served us well over time and will continue to play an integral role in our national security, it may be that a new and broader grouping is needed in order to tackle cyber threats more effectively. A transnational threat requires a transnational solution and it may be constructive to bring together likeminded states with substantial cyber assets in a new international forum with a mandate of responding to international cyber threats.

Returning to DHS, from the standpoint of structure and legislation—and in particular how best to organize the bureaucracy for cybersecurity and infrastructure protection purposes—what matters most at the end of the day is the effective execution of the mission. It is important to emphasize that while the Department of Defense's role in defending the nation against foreign cyber threats is significant, supporting its initiatives should not come at the cost of neglecting the equally important role that DHS plays in protecting critical infrastructure and civilian government networks. In this context, there have been a number of efforts to legislatively address issues related to DHS resourcing and organization. As this committee works to continue these efforts – including progress on its own legislation, the following principles (which are largely consistent with the committee's proposed legislation) should be taken into account: the relevant entities and officials within DHS must possess the necessary authorities and resources to fulfill their cybersecurity missions; and they must be held accountable for their actions through clear lines of responsibility and the application of metrics and measurable goals. Furthermore, as challenges related to the recruitment and retention of necessary cyber talent persist, DHS should also be able to utilize streamlined and flexible hiring authorities to fill cyber positions with qualified individuals in a timely manner. These principles matter more than the wiring diagram per se, if we can agree that implementation is paramount.

Thank you again for the opportunity to testify on such a crucial challenge to America's economic and national security. I look forward to answering any questions you may have

[24] For details, see "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats," CCHS Project Report, October 2016. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf