Prepared Statement of GEN (Ret) Keith B. Alexander*
on
A Borderless Battle: Defending Against Cyber Threats
before the
United States House of Representatives
Committee on Homeland Security

March 22, 2017

Chairman McCaul, Ranking Member Thompson, Members of the Committee: thank you for inviting me to discuss *Defending Against Cyber Threats* with you today, and specifically, the current cyber threat landscape, civilian cyber defense capabilities, and deterrence. I plan to speak candidly about the authorities, roles and responsibilities of the federal government in cyberspace, and how we can provide for our nation's common defense in cyberspace. While some see the offense as superior to the defense when it comes to cybersecurity, I believe that these need to be worked together between the government and industry.

I want to thank both Chairman McCaul and Ranking Member Thompson for making cybersecurity a top priority, including your bipartisan efforts to develop much of the legislation at the heart of the Cybersecurity Act of 2015 and earlier legislation that set the stage for it. This includes the efforts to codify and strengthen the authorities related to the National Cybersecurity and Communications Integration Center (NCCIC) and to improve federal cyber defense efforts, including positive changes to the Federal Information Security Management Act (FISMA) and provisions that will make it easier for us to grow a more capable federal cyber workforce.

We live in an age in which data, and access to data, are key resources. Never has technology been so focused on how we create, use, and communicate data, and this revolution will benefit us as it leads the way for significant strides in technology. It was just over ten years ago that Apple introduced the first iPhone, a portable communications device with a faster processor, more memory, and more storage space than the Cray supercomputers of the 1980s and 1990s. In the same year the iPhone was introduced, we witnessed cyberattacks being used as an element of national power in the attacks on Estonia, the most digitally dependent country in the world. Ten years later, we continue to witness an astounding rate of growth in the amount of unique, new information available worldwide, not to mention huge increases in the velocity of data being transmitted and types of devices communicating information. With the birth of the Internet of Things (IoT) and the continued development and rapid iteration of technology, these trends are likely to continue to accelerate.

We have also witnessed a troubling change in cyberattacks, including an increase in major disruptive attacks, as well as the use of actual destructive attacks on both public and private sector entities in the United States and abroad. In 2012, we saw the advent of destructive

* Gen. (ret.) Keith B. Alexander is the former Director, National Security Agency and the Founding Commander, United States Cyber Command. Currently, he is the President and CEO of IronNet Cybersecurity and recently completed service as a member of the President's Commission on Enhancing National Cybersecurity.

attacks against Saudi Aramco, with over 20,000 computers affected, and a follow-on attack against Qatari RasGas.[1] Similar attacks have recently been reported against the Saudi government.[2] Here in the United States, we have seen destructive attacks conducted by nation-states against private institutions, including the Las Vegas Sands Corporation and Sony Corporation.[3] We have likewise seen massive disruptive attacks targeting American financial institutions, including major attacks taking place multiple times in the last five years. Most recently, we have seen what appear to be cyber-enabled efforts targeting the election of the President of the United States.

We have also seen massive data breaches targeting nearly every major economic sector here in the United States, perhaps most prominently in the customer facing sides of key retailers and health insurers. We have likewise seen an increasing trend with respect to the use of ransomware by organized criminal groups and small actors alike, seeking to hold data or systems hostage at a range of organizations across our nation, from hospitals to educational institutions. According to one report, the key sectors affected by ransomware include the services and manufacturing sectors, making up a combined 55% of ransomware infections.[4]

This does not even account for the ongoing theft of intellectual property from American companies, which I believe continues to represent the greatest transfer of wealth in human history. While we have ostensibly seen a significant downtick in cyber-enabled intellectual property theft by key nation-state actors, it remains to be seen whether this change will be sustained in the long-run and whether it represents an actual reduction in significant activity versus simply a more refined focus on key high value theft.[5]

---

[1] *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/>.

[2] *See* Zahraa Alkhalisi, *Saudi Arabia Warns of New Crippling Cyberattack*, CNN (Jan. 26, 2017), *available online at* < http://money.cnn.com/2017/01/25/technology/saudi-arabia-cyberattack-warning/>; *see also* Jose Pagliery, *Hackers Destroy Computers at Saudi Aviation Agency*, CNN (Dec. 2, 2016) *available online at* <http://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon/?iid=EL>.

[3] *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.").

[4] *See* Symantec, *An ISTR Report: Ransomware and Businesses 2016*, at 8, available online at <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf>

[5] *See* Federal News Service, *Transcript: Hearing Before the Senate Armed Services Committee on Cybersecurity Policy and Threats* at 8 *(Sept. 29, 2015)* ("McCain: As a result of the Chinese leader in Washington there was some

And it is worth noting that the same network penetrations that permit threat actors to steal data can potentially be used to disrupt networks or destroy data. This is particularly important to understand as we watch the increasing convergence of our systems and networks, whether we are talking about the increased links between industrial control systems and corporate networks or the proliferation of devices that are connected to the global network as part of the expansion of the IoT.

We recently saw the practical implications of broad connectivity and convergence when the Mirai botnet turned run-of-the-mill devices into a virtual IoT army and used them to execute a Distributed Denial of Service (DDoS) attack on Dyn (recently acquired by Oracle), a managed DNS and traffic optimization company that serves more than 3,500 enterprise customers, including major companies like Netflix, Twitter, LinkedIn, and CNBC.[6]

As a free society, we have many vulnerabilities and leave ourselves open to various threats that more authoritarian nations are more capable of combatting by limiting access to resources or restricting the freedom of their people. Here in the United States, we are most vulnerable to two asymmetric threats: terrorist attacks and cyber-enabled attacks. While these two types of attacks may overlap, and terrorist groups seek to obtain such capabilities, today the most advanced capabilities are in the hands of nation-states. This is not to discount the threat posed by criminal actors; to the contrary, the most widespread threat to our people today comes from organized criminal groups employing cyber-enabled capabilities to make money.

It is worth noting that our enemies today need not attack our government to have a substantive strategic effect on our nation. Attacking civilian or economic infrastructure may be a more effective approach in the modern era, particularly for asymmetric actors like terrorist groups. Our increasing reliance on digital, connected devices means that while tanks, bombers, and fighter jets are certainly not obsolete, there are newer and perhaps more insidious ways of having similar effects without the need for the large investment that those assets require. Nation-states have long sought access to the critical systems of other nations for espionage, and we now see an expansion from these traditional activities to more aggressive actions by nation-states. The number of nations that possess the capability to exploit and attack continues to grow with less of an incentive to act with appropriate state-to-state behavior and the using these cyber capabilities in a more aggressive way.

Similarly, an increasing number and range of non-state groups use cyber-enabled methods to advance their own agendas. Major criminal gangs, organized crime groups, and terrorist organizations are growing their cyber capabilities to go beyond mere communication, recruitment, and incitement. And though the RAND Corporation estimates that the malware

---

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.")

[6] *See* Dyn, *About Dyn*, available online at < http://dyn.com/about/>.

black market can be more profitable than the illegal drug trade,[7] we do not treat cyberspace threats as an epidemic. Nor do we treat nation-state threats, or worse, nation-state actions, in cyberspace as we would treat the presence of nation-states key naval assets inside our territorial waters. Rather, we treat cyber threats largely as nuisance or, at worst, criminal activity to be dealt with principally through private sector defensive measures and after-the-fact government action, typically by traditional law enforcement agencies. The future of warfare is here, and we need to structure and architect our nation to defend our country in cyberspace.

It is critical that as a nation, we fundamentally rethink how the government and the private sector relate to one another in cyberspace. We need to draw clear lines and make explicit certain responsibilities, capabilities, and authorities. The private sector controls the vast majority of the real estate in cyberspace, particularly when it comes to critical infrastructure and key resources.[8] Given the private sector's role in running the infrastructure upon which our nation relies, there is likewise no question that the government and private sector must collaborate. We need to recognize that neither the government nor the private sector can capably protect the systems and networks they need to without extensive and close cooperation.

One of the key issues we must address is determining where to place responsibility for the cyber defense of the nation, including its key infrastructures and economic sectors. Today, the basic expectation is that the private sector is responsible for defending itself in cyberspace regardless of the enemy, scale of attack, or type of capabilities employed. However, the reality is that commercial, private-sector entities cannot practically be expected to defend themselves against nation-state attacks in cyberspace. They do not have the capacity or capability to respond in a way that would be fully effective against a nation-state attacker, whether from a deterrence or strategic perspective.

For over 200 years, our Constitution has made clear that one of the core goals of our forefathers in forming a federal union was to provide "***for the common defense***."[9] And yet today, as we face a rapidly expanding threat environment in cyberspace and as our national institutions and our economic base in the private sector increasingly come under direct attack from a wide range of actors including highly capable nation-states, we simply do not provide such common defense, at least not in any practical sense of the phrase.

In 2012, then-Secretary of Defense Leon Panetta noted that "the Department [of Defense] has a responsibility…to be prepared to defend the nation and our national interests against an

---

[7] *See* Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data at* 11, RAND Corporation (2014), available online at <http://www.rand.org/pubs/research_reports/RR610.html>.

[8] *See, e.g.*, Office of the Director of National Intelligence, Office of the Program Manager-Information Sharing Environment, *Critical Infrastructure and Key Resources*, available online at <https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources> ("The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation's physical and economic security.").

[9] U.S. Const., preamble (emphasis added and spelling modernized).

attack in or through cyberspace."[10] Even at that time, it was clear that in order to make our overall national cyber architecture truly defensible, we needed to establish a shared understanding of our respective roles and responsibilities, first within the government, then between the government and the private sector. As a result, we worked closely with our colleagues in other agencies across the government spending many hours, days, weeks, and months to put in place a workable structure for sharing authorities and assigning responsibilities at the national level. Indeed, by one count, it took 75 drafts to get agreement on a *single slide* regarding the national division of responsibilities for cybersecurity.[11]

At the end of that process, we assigned the responsibilities as follows: The Justice Department would, among other things, "[i]nvestigate, attribute, disrupt, and prosecute cyber crimes; [l]ead domestic national security operations; and [c]onduct domestic collection, analysis, and dissemination of cyber threat intelligence;" DHS would "[c]oordinate the national protection, prevention, mitigation of, and recovery from cyber incidents; [d]isseminate domestic cyber threat and vulnerability analysis; and [p]rotect critical infrastructure;" and DOD would "[d]efend the nation from attack; [g]ather foreign threat intelligence and determine attribution; [s]ecure national security and military systems."[12] Moreover, the "bubble chart," as this document was called, assigned the following lead roles: DOJ: investigation and enforcement; DHS: protection; and DOD: national defense.[13]

The reality, however, is that the vision of the "bubble chart" has never been fully realized. The truth is that today, our government agencies appear to be confused by the different terms of protection, incident response, and national defense. More needs to be done in defining these roles within the key departments, and we must practice how the government is going to collectively execute their responsibilities. The relationships amongst our various government agencies and between the government and the private sector continue to be a source of friction, the "bubble chart" notwithstanding. Clearly more remains to be done to fully achieve the valuable vision set forth in the "bubble chart."

Many have also argued that it is important for the creation of "a new component agency, or [the] repurpose[ing of] an existing agency, to serve as a fully operational cybersecurity and

---

[10] *See* Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City* (Oct. 11, 2012), available online at <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> .

[11] *See* Department of Defense Information Operations Center for Research and Army Reserve Cyber Operations Group, *Cyber Endeavor 2014: Final Report – When the Lights Go Out*, at 5 (June 26, 2014), available online at <https://my.nps.edu/documents/105372694/0/Cyber Endeavour 2014 - Final Report - 2014-08-13.pdf>

("The need to define these partnerships and relationships [] led the Government and U.S. Federal Cybersecurity Operations Team to define their national roles and relationships as highlighted in Figure 1, which is commonly referred to as the 'Bubble Chart.' There were seventy-five (75) versions made of this chart before all parties agreed on how this works, and it was powerful and important just to get an agreement.")

[12] *See id*. at 6, Fig. 1.

[13] *See id*.

critical infrastructure protection agency on par with other component agencies."[14] This agency would be a "DISA equivalent" for the civilian government agencies. This could be run by the government or outsourced to a commercial entity. As I've previously noted, I generally support this recommendation, and think that it is important that the new Administration give this idea some serious consideration.

For the government to effectively work with the private sector to secure the nation in cyberspace, perhaps the single most important thing the government can do is to build real connectivity and interoperability with the private sector. Such connectivity and interoperability on a technology level is critical, but it is also important on the policy and governance level. That is, in part why the Commission recommended the creation of a National Cybersecurity Public-Private Partnership (NCP^3).[15] This entity, as set forth in Commission's report, would serve the President directly, reporting directly through the National Security Advisor and would be used "as a forum for addressing cybersecurity issues through a high-level, joint public–private collaboration."[16] Part of the NCP^3's key role would be to "identify clear roles and responsibilities for the private and public sectors in defending the nation in cyberspace," including addressing critical issues like "attribution, sharing of classified information…[and] an approach—including recommendations on the authorities and rules of engagement needed—to enable cooperative efforts between the government and private sector to protect the nation, including cooperative operations, training, and exercises."

In line with this recommendation, the Commission also recommended that the "[t]he private sector and Administration should launch a joint cybersecurity operation program for the public and private sectors to collaborate on cybersecurity activities to identify, protect from, detect, respond to, and recover from cyber incidents affecting critical infrastructure."[17] In my view, empowering such joint efforts is critical to ensuring our long-term national security in cyberspace. As the Commission indicated, "[k]ey aspects of any collaborative defensive effort between the government and private sector [will] include coordinated protection and detection approaches to ensure resilience; fully integrated response, recovery, and plans; a series of annual cooperative training programs and exercises coordinated with key agencies and industry; and the development of interoperable systems."[18] Having such mechanisms in place well ahead of crisis is critical so that public and private sector entities can jointly train and exercise these rules of engagement and mitigate any potential spillover effects on ongoing business or government activities. In my view, implementing these two recommendations of the Commission are amongst the most important things we might do as a nation in the near-term.

Finally, I think it is worth highlighting that it is critical that this be a two-way partnership between government and the private sector. The government can and must do more when it comes to partnering with the private sector, building trust, and sharing threat information—yes,

---

[14] *Id*. at 44 (action item 5.5.2)

[15] *Id*. at 14 (action item 1.2.1)

[16] *Id*. at 14-15.

[17] *Id*. at 15 (action item 1.2.2.)

[18] *Id*.

even highly classified threat information—at network speed and in a form that can be actioned rapidly. Building out a cross-cutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to the air traffic control picture. As the air traffic control picture ensures our aviation safety and synchronizes government and civil aviation, the cyber common operational picture can be used to synchronize a common cyber defense for our nation, drive decision-making, and enable rapid response across our entire national cyber infrastructure. This would prove a critical defensive capability for the nation.

The information sharing legislation enacted by Congress as part of the Cybersecurity Act of 2015 is a step in the right direction. However, it lacks key features to truly encourage robust sharing, including placing overbearing requirements on the private sector, overly limiting liability protections, restricting how information might effectively be shared with the government, and keeping the specter of potential government regulation looming in the background.[19] Moreover, while the government has placed this responsibility with the DHS today,[20] and DHS established the Automated Indicator Sharing platform (AIS) as a "capability [that] enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed,"[21] it is important for this Committee—as the primary oversight organization for the Department—to recognize the perception in industry is that DHS faces significant challenges in this area and that it simply lacks the technical capabilities to succeed.[22] When we first discussed this approach, DHS was the portal, but it would be a true partnership between DOD, DHS, and DOJ. We must help drive DOD, DHS, and DOJ to work together to evolve our government's roles and responsibilities.

More can be done here, and I stand ready to work with this Committee and others in Congress and the Administration as we seek a path forward on this important issue. As with the recommendations of the Commission above, I believe that implementing real, robust real-time threat information sharing across the private sector and with the government could be a game-changer when it comes to cyber defense.

---

[19] *See, e.g.*, Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, __ S. Car. L. Rev. __ (forthcoming 2017).

[20] *See, e.g.*, Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (Feb. 13, 2015), available online at <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari> ("The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002…shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents.").

[21] *See* DHS US-CERT, Automated Indicator Sharing (AIS), available online at <https://www.us-cert.gov/ais>.

[22] *See* Commission on Enhancing National Cybersecurity, *Testimony of Greg Rattray*, Director of Global Cyber Partnerships & Government Strategy, J.P. Morgan Chase (May 16, 2016) (describing DHS's six information sharing initiatives, as "too broad and [simply] not meet[ing] the need[] to enhance cyber defense"); *Testimony of Mark Gordon*, n. 13 *supra* (arguing that while tactically accelerating automating and systemizing threat indicator content with the government is a big vision, it is not a reality today); *see also* Jaffer, n. 14 *supra*, at __ ("DHS is generally seen as facing major challenges in capability in the cyber area and a number of other agencies, from DOD/NSA to FBI, are seen by industry as more capable, reliable, or secure.").

In sum, Mr. Chairman, I think much remains to be done to fully put our nation on a path to real security in cyberspace, but I am strongly hopeful for our future. With your leadership and that of the Ranking Member, working together collaboratively across the aisle and with the White House and key players in the private sector as well as other key committees in Congress, I think we can achieve some real successes in the near future.