Prepared Statement of GEN (Ret) Keith B. Alexander[*]
on
Cyber Warfare Today: Preparing for 21st Century Challenges
in an Information-Enabled Society
before the
House Armed Services Committee

April 11, 2018

Chairman Thornberry, Ranking Member Smith, Members of the Committee: thank you for inviting me to discuss the current threats and challenges that we face as a nation in cyberspace and how we might modify our current policies to address these problems. I applaud you both for approaching these issues in a bipartisan, strategic manner and for the series of hearings and briefings that today's panel kicks off. I know that you will hear later today from some of our government's leaders in this area in both an open and closed setting and that you'll be focused on operational and budgetary matters in upcoming sessions, so my plan today is to set out some of the larger trends and issues that I see facing our nation and to put on the table some initial ideas about how these issues might be addressed.

Mr. Chairman, as you know, I've long been an advocate for the view that in the modern era of threats that face our nation, we must fundamentally rethink our nation's architecture for cyber defense. Today we face strategic threats in cyberspace from two nations that have long been our key adversaries in this domain: China and Russia. We also face tactical threats from a range of actors, including increasingly active nation-states like North Korea and Iran, as well as wide array of non-state actors from criminal gangs to terrorist groups. And some of these latter actors are working on behalf of, or alongside, the nation-states that are also operating against us in the cyber domain.

And while we increasingly recognize these threats as a nation, and as our government becomes more open and robust about calling out those who would threaten our national security, we still remain overly cautious about making hard decisions regarding the appropriate roles and responsibilities of the government and the private sector. Even as our nation maintains the lead in technological innovation and builds our economy based in significant part on growth in the technology sector, I worry that we are not yet ready as a nation to grapple with the reality that cyberspace has become a domain for warfare and that we very much are in the throes today of a series of ongoing—albeit currently low-level—conflicts in cyberspace.[1]

[*] Gen. (ret.) Keith B. Alexander is the former Director, National Security Agency and Founding Commander, U.S. Cyber Command. Gen. Alexander currently serves as President and CEO of IronNet Cybersecurity, a startup cybersecurity firm and in a range of other capacities in the public and private sectors. Gen. Alexander is testifying before this Committee today in his personal, individual capacity.

[1] *See, e.g.*, Office of the Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, at 5-6 (Mar. 6, 2018) ("The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war….Russia, China, Iran, and North Korea will pose the greatest cyber threats to the United States during the next year. These states are using cyber operations as a low-cost tool of statecraft, and we assess that they will work to use cyber operations to achieve strategic objectives unless they face clear repercussions for their cyber operations…. The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to

The recent National Security Strategy (NSS) released by the White House makes clear what we have long known: economic security is national security.[2] As the NSS makes clear, "[a] strong economy protects the American people, supports our way of life, and sustains American power…[and a] growing and innovative economy allows the United States to maintain the world's most powerful military and protect our homeland."[3] At the same time, we've long known that our economic security is being challenged directly in cyberspace by nations, like China, that continue to siphon off massive amounts of economic wealth through the theft and coerced transfer of the very intellectual property that is at the heart of our modern economy.[4]

Our national security is even more directly threatened by nations like Russia who have engaged in obvious efforts to undermine confidence in our political system,[5] have sought to put in place long-term penetrations in critical infrastructure sectors in order to conduct espionage and prepare the battlespace for potential future conflict scenarios,[6] and have conducted what our government recently referred to as the most "destructive and costly cyber-attack in history."[7]

sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners."), *available online at* <https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf>

[2] The White House, *National Security Strategy of the United States of America* at 17 (Dec. 2017), *available online at* <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

[3] *Id*.

[4] *See, e.g.*, The White House, *Remarks by President Trump at Signing of a Presidential Memorandum Targeting China's Economic Aggression* (Mar. 22, 2018) (statement of U.S. Trade Representative Robert Lighthizer) ("Lighthizer:… Technology is probably the most important part of our economy. There's 44 million people who work in high-tech knowledge areas. No country has as much technology-intensive industry as the United States. And technology is really the backbone of the future of the American economy….And we concluded that, in fact, China does have a policy of forced technology transfer; of requiring licensing at less than economic value; of state capitalism, wherein they go in and buy technology in the United States in non-economic ways; and then, finally, of cyber theft."), *available online at* <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-signing-presidential-memorandum-targeting-chinas-economic-aggression/>.

[5] *See, e.g.*, U.S. Department of Treasury, *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks* (Mar. 15, 2018) ("Today's action counters Russia's continuing destabilizing activities, ranging from interference in the 2016 U.S. election to conducting destructive cyber-attacks, including the NotPetya attack, a cyber-attack attributed to the Russian military on February 15, 2018 in statements released by the White House and the British Government."), *available online at* <https://home.treasury.gov/news/press-releases/sm0312>.

[6] *See, e.g.*, Department of Homeland Security, *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (Mar. 15, 2018), ("This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors….DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS)."), *available online at* <https://www.us-cert.gov/ncas/alerts/TA18-074A>; *see also Worldwide Threat Assessment*, *supra* at n. 1 ("In the next year, Russian intelligence and security services will continue to probe US and allied critical infrastructures, as well as target the United States, NATO, and allies for insights into US policy.").

[7] The White House, *Statement from the Press Secretary* (Feb. 15, 2018) ("In June 2017, the Russian military launched the most destructive and costly cyber-attack in history….The attack, dubbed 'NotPetya,' quickly spread

And these threats don't even account for the fact that our government has recently called out similar IP theft and destructive attacks by both Iran[8] and North Korea.[9]

At the same time, even though we are currently in the middle of a very real series of (minor) military skirmishes in cyberspace, and even though our Constitution has made clear for over 200 years that one of the core missions of the federal government is to provide "for the common defence,"[10] we remain woefully underprepared as a nation to provide effectively for such defense in the cyber domain.

This is not to say we don't have the forces or capabilities in place to do so. The creation of U.S. Cyber Command under my watch within the Department of Defense, with the strong support of this Committee and its members, as well as Cyber Command's continued close work with the National Security Agency, the world's premiere signals intelligence agency, provides our nation with very real and robust capabilities in both the offensive and defensive areas, capabilities that have the ability both protect our nation writ large and to make cyber deterrence a reality in the global arena.

However, the problem is not fundamentally one of force structure at this point. It is one of roles, responsibilities, authorities, and relationships. And on this account, there remains a great deal more to be done. While this Committee has leaned forward and pressed the Department to think more actively about its capabilities, authorities, and warfighting doctrine when it comes to the cyber domain, I remain concerned that we have not yet really grappled with two major issues when it comes to the defense of the nation in cyberspace: (1) how we organize ourselves as a government to defend, fight, and win in this domain; and (2) how we build real jointness between the public and private sectors in what is inevitably going to be a conflict that requires

worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas.") *available online at* <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>.

[8] *See, e.g.*, Department of Justice, *Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps* (Mar. 23, 2018 (describing Iranian hackers that "conducted a coordinated campaign of cyber intrusions into computer systems belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund."), *available online at* <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary>; *see also Worldwide Threat Assessment*, *supra* at n. 1 at 6 ("Iran's cyber attacks against Saudi Arabia in late 2016 and early 2017 involved data deletion on dozens of networks across government and the private sector."), *available online at* <https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf>.

[9] *See, e.g.*, The White House, *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea* (Dec. 17, 2017) ("In May of this year, a dangerous cyberattack known as WannaCry spread rapidly and indiscriminately across the world. The malware encrypted and rendered useless hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries….This was a careless and reckless attack. It affected individuals, industry, governments. And the consequences were beyond economic. The computers affected badly in the UK and their healthcare system put lives at risk, not just money. After careful investigation, the United States is publicly attributing the massive WannaCry cyberattack to North Korea."), *available online at* <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>.

[10] *See* U.S. Const., preamble.

both the government and industry to act with speed and vigor if we are going to truly be able to defend the nation.

Over half a decade has passed since 2012, when then-Secretary of Defense Leon Panetta made clear that it is the U.S. government's policy that "the Department [of Defense] has a responsibility…to be prepared to defend the nation and our national interests against an attack in or through cyberspace"[11] and this year's National Defense Strategy highlights the importance of providing such defense, noting that

> It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion…[And the] increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities.[12]

And yet, as this Committee all too well knows, the reality is that today, U.S. Cyber Command lacks the clear authorities and rules of engagement to make this policy effective. While many are rightly concerned with providing authorities prior to the beginning of a conflict, the reality is that in this domain, more than others, we need to ensure that our warfighters can act with speed and agility when the enemy strikes. And structured properly, with appropriate civilian oversight, reporting to Congress, and additional authorizations, the government can effectively mitigate any major concerns with providing such authority now. Indeed, given the potential for overreach, there are significant benefits to working together now, in a bipartisan manner, to provide U.S. Cyber Command with the appropriate authorities and key rules of engagement (ROE) in the relative calm of the current moment rather than making policy in the maelstrom of an ongoing crisis.

But simply providing Cyber Command with robust authorities and solid ROE is not enough. The reality today is that the vast majority of American cyber infrastructure is owned and operated by the private sector and, as a nation, we do not want the government to maintain a long-term, active presence on private sector networks to provide defensive capabilities. As a result, it is critical that that government works closely with the private sector in three areas: (1) setting the conditions for a truly defensible cyber infrastructure; (2) significantly empowering private sector defensive capabilities; and (3) providing for interoperable capabilities and joint exercises in the event that a national crisis requires the government to assist the private sector in a more direct manner or to respond directly against a threat to the nation.

To set the conditions for a truly defensible cyber infrastructure, we must recognize a basic fact about the cyber threat environment today: namely that no single entity—whether a private sector company or a government agency—can stand alone against the most capable threat actors.

[11] *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> .

[12] *See* Department of Defense, *Summary of the 2018 National Defense Strategy* (Jan. 19, 2018), at 3, *available online at* <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

Indeed, in no other area do we expect individual private companies to defend themselves against nation-states. For example, while we reasonably expect Target to have high fences and armed guards around its warehouses to protect against thieves, we surely don't expect Target or Walmart or any other American company to have surface-to-air missiles on the roofs of those warehouses to defend against the threat of a Russian bomber dropping munitions.[13] And yet today, when it comes to cyberspace, we expect exactly that. This policy simply makes no sense; expecting individual companies, standing alone, to defend themselves against all comers, including nation-states—which, to be fair, is our current expectation—is a policy designed to fail.

Instead, as a nation, we need to move to a collective defense architecture both within the private sector, as well as between the public and private sectors. The good news is that we have already taken significant steps in this direction, with various sectors creating information sharing and analysis centers and organizations (ISACs/ISAOs) and the government crafting legislation to encourage information sharing amongst companies as well as with the government. The reality, however, is that even with these organizations in place, we still have yet to create the right incentives to share information at scale and speed within the private sector and with the government.[14] To be sure, some sectors, like the energy and financial sectors, are beginning to lead in this space. But more remains to be done, both as a matter of policy as well as authorities. We must increasingly think of our critical industries not just as a coalition of key companies and sectors, but as a set of strategic assets that require a combined, joint arms effort to defend them. Much good intellectual work has been done in this space including: (1) discussions about creating and empowering a Strategic Infrastructure Coordinating Council (SICC);[15] (2) the extremely valuable and practical recommendations of the National Infrastructure Advisory Council (NIAC);[16] and (3) the notion of creating a public-private advisory body to the National Security Council (NSC) in the form of the National Cybersecurity Public-Private Partnership

[13] *See, e.g.*, Keith B. Alexander, et. al, *Clear Thinking About Protecting the Nation in the Cyber Domain*, 2 Cyber Defense Review 29, 33 (No. 1) (2017) ("The fact is that commercial and private entities cannot be expected to defend themselves against nation-state attacks in cyberspace. Such organizations simply do not have the capacity, the capability, nor the authority to respond in a way that would be fully effective against a nation-state attacker in cyberspace. Indeed, in most other contexts, we do not (and should not) expect corporate America to bear the burden of nation-state attacks. For example, we do not expect Target to employ surface-to-air missiles to defend itself against Russian planes dropping bombs in the United States. Rather, that responsibility belongs to the DoD. Today, however, in cyberspace, that expectation is flipped on its head.")

[14] *See* Keith B. Alexander, *Prepared Statement on Cyber Strategy and Policy before the Senate Armed Services Committee* (Mar. 2, 2017) ("The cyber legislation enacted by Congress last year 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"), available online at <https://www.armed-services.senate.gov/imo/media/doc/Alexander_03-02-17.pdf>.

[15] *See, e.g.*, Electricity Subsector Coordinating Council, *ESCC Initiatives* (Jan. 2018), *available online at* <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.

[16] *See, e.g.*, Department of Homeland Security, National Infrastructure Advisory Committee, *Securing Cyber Assets: Addressing Urgent Threats to Cyber Infrastructure*, at 3-4, 7-20 (Aug. 2017), *available online at* <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>

(NCP3),[17] as recommended by a recent Presidential commission that I served on alongside key individuals from the private sector including the former CEO of IBM, Sam Palmisano, and the CEO of Mastercard, Ajay Bangha. But the time for purely intellectual exercises has passed; it is now critical that we begin taking the right steps to implement these ideas in practice.

When it comes to empowering private sector defensive capabilities, here too the government can and should do more. For far too long the government has talked about the need to share threat information at speed and scale with the private sector. But continued talk will mean little if the day comes to pass where the government knew of a major threat to the American private sector that it could have helped defend against and but didn't share it in an actionable form, in real-time. The government must be prepared not only to share declassified information with the private sector in real-time and at machine-speed, but also must be prepared to use its overseas intelligence collection architecture to collect on threats to the American private sector and to pass on this information—even in its highly classified form—to the private sector, so that it may be utilized to defend industry. Similarly, if the nation is to become truly defensible, the government must work with industry to develop a cyber common operational picture, analogous to the air traffic control picture. Just as the air traffic control picture ensures aviation safety and helps synchronizes government and civil flights, a cyber common operational picture can help synchronize our national common cyber defense and enable rapid response in a time of crisis.

Finally, the government and industry ought to work together to develop interoperable capabilities that can be utilized in a crisis and to exercise these capabilities in advance of an actual threat. Such efforts, as recommended by the NIAC,[18] will allow the nation to have a plan and capability in place should the need arise in case of an actual cyber conflict scenario.

As a former commander of forces deployed around the world, I also feel strongly that unity of command is critical. Today we divide responsibility for the ongoing, day-to-day defense of the government amongst various agencies, including Cyber Command and DHS. We likewise divide responsibility for private sector outreach and collaboration on cyber defensive efforts between Cyber Command, DHS, and FBI. To that end, it is my view that in the time of a crisis, all of these capabilities have got to come under a single authority. And while I know this will be a hotly debated recommendation—not to mention where the authority ought to reside—the reality is that while we have gotten away for a quite a while with various agencies stepping on one another's toes, more must be done going forward to get the government working more closely together if we are to be able to respond effectively in a crisis scenario. At a minimum, as the government debates and discusses the wisdom of such a larger effort, at least within the White House, the President ought to immediately elevate existing roles by appointing an Assistant to the President for Cybersecurity who reports to the President through the National Security Advisor and charge that individual with leading national cybersecurity policy and

[17] *See, e.g.*, Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Dec. 1, 2016), at 14-15, *available online at* <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf>.

[18] *See, e.g.*, Department of Homeland Security, National Infrastructure Advisory Committee, *Securing Cyber Assets: Addressing Urgent Threats to Cyber Infrastructure*, at 8-9, 18 (Aug. 2017), *available online at* <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>

coordinating implementation of the nation's cyber protection program and taking input from the recommended NCP3.

In sum, Mr. Chairman, I think much remains to be done to create a truly defensible national cyber architecture. But I believe that we can get there, particularly with the support of this Committee and its leadership, reaching across the aisle to solve this truly national problem. I stand ready to assist you, the Ranking Member, and the other members of this Committee and your staff to work on this effort. Thank you to both you and the Ranking Member for your leadership and for holding this hearing. I am prepared to answer any questions you or the members of the Committee may have.