FINAL

Prepared Statement of Jeh Charles Johnson
Before the House Armed Services Committee
Hearing on "*Cyber Operations Today: Preparing for 21st Century Challenges in an Information-Enabled Society*"
April 11, 2018

Chairman Thornberry, Ranking Member Smith and members of this Committee:

From February 10, 2009 to December 31, 2012, I served as General Counsel of the Department of Defense. From December 23, 2013 to January 20, 2017, I served as Secretary of Homeland Security. As Secretary, I had the privilege of working with Congress to provide additional authorities to the Department of Homeland Security to defend the Nation's and the federal government's cybersecurity, through the Cybersecurity Act of 2015,[1] the National Cybersecurity Protection Act of 2014,[2] the Federal Information Security Modernization Act of 2014,[3] and other new laws.[4]

I am pleased the Committee has convened this hearing on the important topic of cyber operations and cybersecurity, and I'm pleased to be joined at the witness table by Secretary Chertoff and General Alexander. The views I express here are my own, based upon my personal experiences in national security and, now, as a concerned private citizen.

You have asked the witnesses today to focus our testimony on the following:

> *[T]he current cybersecurity challenges and threats to U.S. military superiority being posed by Russia, China and other state-sponsored actors aggressively engaged in the cyber domain conducting activities to enable information warfare below the traditional level of armed conflict. Please also discuss policy and capabilities with respect to current U.S. plans and strategies, including ways to improve interagency coordination for cyber threats. Lastly, we ask*

[1] Pub. L. No. 114-113, 129 Stat. 2242, 2935 (2015).
[2] Pub. L. No. 113-282, 128 Stat. 3066 (2014).
[3] Pub. L. No. 113-283, 128 Stat. 3073 (2014).
[4] *E.g.*, the Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 2995 (2014) (including additional authorities for cybersecurity recruitment and retention).

that you recommend ways and means to better prepare for 21st century challenges in an information-enabled society by improving the organization of the U.S. government.

The Threat Picture

Cyberattacks on our homeland, of all manner and from multiple sources, are going to get worse before they get better. In this realm and at this moment, those on offense have the upper hand; those on defense struggle to keep up. Whether nation-state actors or non-state cyber-criminals, hacktivists, or those who engage in the growing industry of Ransomware, those on offense are ingenious, tenacious, agile, and getting better all the time.

To understand the current cybersecurity threats to our homeland from nation-states and others, we must, in my view, divide them into five broad threat streams:

First, the threat of cyberattack by a nation-state or other entity to seize, disable, or destroy components of our Nation's critical infrastructure. This form of cyberattack implicates national security, and, if significant enough in its effects, may amount to an act of war.[5] This form of cyberattack may also occur as part

[5] A key question many ask is: under what circumstances can a cyberattack constitute an act of war? At the moment, there is no legal definition for the term "cyberwar." The 1022-page Department of Defense Law of War Manual, which was published in 2015 and took decades, literally, to write, contains a section on cyber operations, but does not contain a definition of the term cyberwar or take on the question of when a cyberattack constitutes an act of war, justifying an armed response. On this issue, I agree with the existing assessments from legal scholars I have come to know and trust, Professors Jack Goldsmith (Harvard Law) (Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT'L L. 129 (2013)); Oona Hathaway (Yale Law) (Oona Hathaway, *et al.*, *The Law of Cyber Attack*, 100 CAL. L. REV. 817 (2012)) and Major General (ret) Charles Dunlap (Duke Law) (Charlie Dunlap, *Are Cyber Norms as to What Constitutes an "Act of War" Developing as We Would Want?*, LAWFIRE (Sept. 15, 2017), https://sites.duke.edu/lawfire/2017/09/15/are-cyber-norms-as-to-what-constitutes-an-act-of-war-developing-as-we-would-want/), among others.

Essentially, the answer from them, and me, is "maybe," or "it depends," or "we will know it when we see it."

The experts recognize that the terms "use of force" and "armed attack" are hard to translate into the cyber realm. However, the consensus view calls for an analysis of the kinetic effects of an attack, not just the kinetic means. That is, a cyberattack that causes serious kinetic effects, such as the explosive destruction of an air field or an electric grid, and/or physical death and injury (as opposed to cyber espionage or cyber theft of data), should almost certainly be considered an act of war. This is a simple, common-sense approach to the issue. In my judgment, it is not in the interest of the United States to reach for a more creative or expansive definition. An enlarged definition of a cyber "act of war" could be invoked by other nations unilaterally as a justification for an armed response under Article 51 of the UN Charter, or

and parcel of an ongoing armed conflict that has begun in a traditional kinetic fashion.

Second, cyber espionage, practiced principally by nation-states, and similar in purpose to forms of traditional espionage.

Third, hacking and unwanted exfiltration and theft of data and intellectual property. As General Alexander notes in his prepared statement, the theft of intellectual property by nation-states is a significant part of this threat stream. As we saw in 2016, this threat stream also includes, but is hardly limited to, the risk of attack on election infrastructure by nation-state actors, which represents a threat to our very democracy.

Fourth, the problem of widespread use and misuse, but not necessarily theft, of personal, private data on the internet. The reality is that the American public has surrendered and entrusted much of our private lives to the internet. Technically with consent, but often without our knowledge, much of this private data is shared for marketing and commercial purposes, and there is now a growing industry of data mining companies, data brokers, and data intelligence companies dedicated to further exploiting this target-rich environment. Because of its prevalence on the internet, private information is now discoverable and exploitable not only by conventional actors, but by criminal hackers and nation-states. Consequently, this is not just an issue of privacy; it is an issue of security.

Fifth, and finally, the problem that can be considered a form of cyberattack, but not exclusively so – fake news and hateful, extreme views published and republished on the internet, used as a weapon by foreign and domestic forces seeking to alter elections, sow discord, or otherwise alter public opinion generally. The recent indictment of 13 Russian individuals by the Special Counsel[6] confirms that this was part of the Russian attack against us in 2016.

---

for invocation of Article 5 of the NATO treaty. Mistakes in attribution—for which there is an enhanced concern in the cyber realm—could also complicate matters.

This is not meant to imply that the U.S. should not formulate a comprehensive strategy for these attacks—to the contrary, we must continue to develop a set of international rules and norms of acceptable behavior in cyberspace, and the United States should lead that effort.

[6] Indictment, *United States v. Internet Research Agency LLC et al.*, No. 18-cr-00032-DLF, (D.D.C. Feb. 16, 2018), ECF No. 1.

Roles, Responsibilities, and Capabilities

There are vital roles for the U.S. military, the intelligence community, law enforcement, and the Department of Homeland Security in the U.S. government's cybersecurity efforts.

Broadly speaking, the Department of Defense should be responsible for defending the Nation against attacks, and securing national security and military systems; the Department of Justice should be the lead agency responsible for investigating[7] and prosecuting cybercrimes, and the lead agency for domestic national security operations; and DHS should be the lead agency for protection, prevention, mitigation, and recovery when it comes to domestic private and government cyber incidents, as well as securing federal civilian networks. (In addition, the head of each federal agency is responsible for the immediate security of his or her own agency's particular network.)

As between DOJ and DHS, I concur with the approach taken in Presidential Policy Directive 41,[8] which specifies that DOJ is the lead agency for "threat response" (*i.e.*, law enforcement and national security investigations) to significant cyber incidents and DHS is the lead agency responsible for "asset response" (*i.e.*, patching vulnerabilities, forensics, and technical assistance) to significant cyber incidents.

I also support efforts to reorganize DHS internally to more effectively address current cyber threats. There should be a cybersecurity agency of the U.S. government. DHS's current "National Protection and Programs Directorate" should be reorganized into a leaner and more efficient "Cyber and Infrastructure Security Agency" that has two key missions, cybersecurity and infrastructure protection, and recognizes the interconnectivity of these two missions. I support legislative efforts to accomplish these goals.[9]

---

[7] In addition to the FBI, the Secret Service and Homeland Security Investigations have considerable expertise and experience in investigating cybercrimes.

[8] Presidential Policy Directive 41, United States Cyber Incident Coordination (2016).

[9] *See* Cybersecurity and Infrastructure Security Agency Act of 2017, H.R. 3359 (115th Cong.) (2017), passed by the House in December 2017, and Department of Homeland Security Reauthorization Act, H.R. 2825 (115th Cong.) (2017), reported out of the Senate Homeland Security and Governmental Affairs Committee and pending in the Senate.

As for the relative roles in cybersecurity between U.S. Cyber Command and NSA, I defer to the views of General Alexander.

Inevitably, given its nature, cyber security must also be a public-private partnership. As General Alexander notes in his prepared statement, the vast majority of our Nation's cyber infrastructure is owned and operated by the private sector.

In 2015, DHS established near-real-time automated information sharing capability with the private sector. Through the Cybersecurity Act of 2015, Congress provided further incentives for the private sector to share cyber threat indicators with DHS. As of the time I left office, however, not enough businesses had taken advantage of automated information sharing capability. No matter how sophisticated a company's cybersecurity is, everyone benefits from information sharing about the latest cyber threats. The federal government should focus on strengthening partnerships with the private sector, to ensure better information sharing.

By contrast, in my judgment, addressing the problem of fake news and extremist views is not a matter for the security agencies of our government. Foreign influence in federal elections is a matter for the federal election laws, and activities that violate criminal laws are a matter for law enforcement. Beyond that, we must be extremely careful not to go down the road of empowering security agencies to regulate or restrict speech, particularly political speech, on the suspicion that it might have a foreign or extremist origin. Self-regulation by private internet access providers should be the first solution. And the public should be more skeptical about what we read and see.

To meet all of these demands, continued U.S. government investments in both cyber talent and technology are key. I am pleased that the President's FY2019 budget proposes significant amounts for DHS's Continuous Diagnostics and Mitigation Program, and continued deployment of the EINSTEIN system to protect federal civilian networks. The recruitment and retention of cybersecurity talent is perhaps the biggest cybersecurity challenge for DHS and other federal agencies.

Beyond that, I agree with Secretary Chertoff's prepared statement that the U.S. government must define a cyberwarfare doctrine, develop clear guidelines for determining attribution, and continue to incentivize public-private information sharing and investments by the private sector in cybersecurity.

I am prepared to discuss further my own views on these topics, and I look forward to your questions.