Clear Thinking About Protecting the Nation in the Cyber Domain*

General (Ret.) Keith B. Alexander (U.S. Army)
Jamil N. Jaffer
Jennifer S. Brunet

The key systems and networks that are colloquially referred to as *cyberspace* constitute a set of critical assets that enable communication, promote economic growth and prosperity, advance the cause of freedom globally, and help ensure US national security and that of our allies. At the same time, cyberspace has become a digital battleground where nation-states and their proxies, organized criminal groups, terrorists, hacktivists, and others seek to gain an advantage over one another, whether through surveillance and espionage, criminal activity, recruitment, planning, and incitement to attacks, and the repression of free speech and expression. Increasingly, the US recognizes that while the benefits of global connectivity far outstrip the potential costs, our increased connectivity also makes us more vulnerable: as individuals, as groups, and as a nation. Today the spread of advanced technologies and the increased connectivity of networked devices to physical systems make it more possible than ever before to create real-world effects through cyber activities. As a result, the US must proactively take steps to protect ourselves, our information, and our critical assets from the vagaries of crime, theft, espionage, and, increasingly, from potentially destructive activities. Unfortunately, as a nation, the US has yet to have the critical conversations and make the decisions necessary to put in place the foundational capabilities necessary to protect the nation in this new domain.

* This article is adapted in part from testimony delivered by General (Ret.) Keith B. Alexander on July 13, 2016 before a combined hearing of two subcommittees of the U.S. House of Representatives Committee on Government Reform and Oversight on Digital Acts of War, testimony delivered by Jamil N. Jaffer before a hearing of the U.S. House of Representative Committee on Small Business on July 6, 2016 on Foreign Cyber Threats, and testimony delivered by General (Ret.) Alexander on November 3, 2015 before a hearing of the U.S. Senate Armed Services Committee on the Future of Warfare.

General (Ret.) Keith B. Alexander is the former Director of the National Security Agency and former Commander, United States Cyber Command. General Alexander currently serves as the President and CEO of IronNet Cybersecurity, a startup technology company headquartered in the Washington, DC metropolitan region.

Technology is an area of rapid and dramatic change and growth, with processing capacity doubling every two years under Moore's law.[1] Indeed, some have suggested that any person with access to Google today has better access to informationthan the President of the United States did fifteen years ago.[2] Others have previously suggested that by 2049, a $1,000 computer will exceed the computational capabilities of the entire human race.[3] The rate of connectivity is increasing rapidly. By 2020, it is expected that IP traffic on global communications networks will reach ninety-five times the volume of the entire global Internet in 2005,[4] and Cisco estimates that by 2020 there will be more than three IP-connected devices per person around the world.[5]

While this expansion of technology and connectivity means that we can expect to reap tremendous social, economic, and political benefits, it also means the attack surface for bad actors to target the US is likewise expanding. From our perspective, there are four major threats in the cyber domain: cyberattack, cyber espionage, cyber-enabled theft of intellectual property, and criminal activity. In 2014, the Centerfor Strategic and International Studies estimated the worldwide loss from cybercrime to be $445 billion annually.[6] While we are all now well aware of the huge threat posed to our economic security by the rampant theft of intellectual property from American private sector companies by nation-states and their proxies—constituting the greatest transfer of wealth in human history—there is an even more troubling trend that began to take hold in the past four years: the emergence of actual destructive cyberattacks, where cyber or other systems, data, or capabilities are permanently destroyed or disabled.

Jamil N. Jaffer is the former Chief Counsel & Senior Advisor to the Senate Foreign Relations Committee and a former Associate Counsel to President George W. Bush. Mr. Jaffer currently serves as an Adjunct Professor of Law and Director, Homeland & National Security Law Program at the Antonin Scalia Law School at George Mason University and as Vice President for Strategy & Business Development for IronNet Cybersecurity.

In 2012, a set of destructive cyberattacks conducted against Saudi Aramco and Qatari Ras Gas disabled over 30,000 computers at Saudi Aramco alone.[7] In February 2014, the US saw the first-ever publicly reported destructive cyberattack by a nation-state on its soil, with Iran attacking the Las Vegas Sands Corporation.[8] This was followed by North Korea's attack on Sony Pictures in November 2014.[9] These attacks represent a particularly concerning trend, as they demonstrate a expansion in cyber activity from nations that are more likely to be unpredictable and dangerous that the typical nation-state attackers with strong capabilities. These attacks also lay bare the fact that the US has no real strategy or doctrine for how to deal with such events, much less deter other nation-states from undertaking them.

To develop such strategies and doctrines, and perhaps most importantly, to effectively deter these type of actions, the US needs to understand better what actions might constitute acts of war in the cyber domain and start putting in place the key elements of a truly defensible national cyber architecture.

When it comes to understanding what might constitute acts of war in cyberspace, it is easy to imagine categories of cyberattacks with consequences that we would likely be prepared to call acts of war. For example, attacks that cause major loss of life, destruction or incapacitation of significant portions of key infrastructure, or even attacks that cause massive economic damage, are likely to cross that line. At the same time, there remains an enormous gray area of hostile nation-state actions that might approach, or may even cross such a line.

In part, the determination of what constitutes an act of war is a legal determination and has legal consequences. International law, including the U.N. Charter, seeks to define when a nation may act in

Jennifer S. Brunet is a former U.S. Air Force defense analyst and staff member of U.S. Cyber Command and the National Security Agency. Ms. Brunet currently serves as an executive staff member at IronNet Cybersecurity.

self-defense and how the international community might respond to a breach of the peace.[10] Similarly, a determination by NATO that a member-state has been attacked could trigger the collective defense commitment in Article V of the NATO Treaty.[11]

At the same time, we cannot ignore the political and moral aspects of determining what constitutes an act of war. Even if a nation suffers an "armed attack" under the U.N. Charter definition, it may choose not to respond. In addition, many argue that the right of self-defense does not require a nation to wait until an armed attack takes place before invoking its right of self-defense against an imminent, pressing threat.[12] Moreover, the decision whether or not to go to war, what constitutes a just cause for war, and how a nation chooses to respond, including the means of warfare it employs, are profoundly moral questions with implications for the overall conduct of war going forward and the ethical constraints we can, and should, apply to ourselves in conducting even a war that is just and legal. These are issues that must be debated, both in the US as well as through international institutions, to assess whether it is possible to develop the beginnings of a reasonable international consensus.

In looking at these questions, particularly in a new domain like cyberspace, the US must think not just about the right and left boundaries of what constitutes an act of war, and how and when to respond, but also about the vital center, and the hard questions that lie within. While there are no detailed answers, it is worth noting that we are not writing on a blank slate; many have considered the implications for just war theory and international law of new domains or new methods of warfare before, whether during the advent of air warfare or the development (and use) of nuclear weapons.[13]

Perhaps even more importantly, we are not even writing on a blank slate when it comes to cyberspace itself. The Tallinn Manual, a NATO-sponsored effort, provides helpful guidance in this area,[14] and will likely continue to do in coming years, as it is being updated in February 2017.

When it comes to adversary activities in cyberspace—whether such activities rise to the level of an act of war or not—it is worth considering how the US might best defend itself against such activities. Today, America's enemies need not attack our government to have a substantive national strategic effect. Indeed, in some ways, attacking the US civilian or economic infrastructure may be a more effective approach in the modern era, particularly for asymmetric actors or nation-state proxies. The future of warfare is here, and we need to understand how to architect the US for this new reality.

One of the key issues the US must address, in creating defensible national cyber architecture, 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, the scale of the attack, or the type of capabilities employed. While this is the norm today, we must consider whether such an approach continues to make sense going forward, particularly when it comes to nation-state attacks.

The future of warfare is here, and we need to understand how to architect the US for this new reality.

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.[15] Today, however, in cyberspace, that expectation is flipped on its head.

Some argue that private sector entities should be authorized to 'hack back' or to respond to breaches in an affirmative matter. While this may be a tempting option at first blush, the reality is that authorizing such action could have significant downstream consequences. Offensive actions against a nation-state adversary in cyberspace, regardless of who takes them, could potentially lead to real-world, physical consequences. In most cases, a private entity responding to a nation-state attack will not likely bear the cost of its response. Moreover, in the case of a nation-state attacker, there is also significant potential for a mistake—whether in the scope of the response or with

attribution. It is, therefore, no surprise that, at least as a historical matter, we typically assign responsibility for offensive actions to the government, putting such decision-making in the hands of our elected political leaders, not private sector entities or CEOs.

In 2014, then Secretary of Defense Leon Panetta made it clear that US government policy was that "the Department [of Defense] has a responsibility not only to defend DoD's networks but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace."[16] The reality is, however, that U.S. Cyber Command (USCYBERCOM) does not today have necessary authorities, rules of engagement, and visibility to effectively defend even the federal government itself, much less the whole of the US private sector.[17] The newly elected President should, therefore, work to provide the authorities and rules of engagement necessary to defend at least the government to USCYBERCOM and begin architecting the government's systems to provide the necessary visibility that such a defensive capability would require. This assignment of responsibility and authority ought then be followed by a period of training and exercising of these authorities and capabilities to demonstrate USCYBECOM's readiness and ability to respond to threats at network speed, as appropriate.

The US must recognize that sharing and collaboration are not the end, but rather are a means to a more capable national cyber defense.

It is also worth noting that even if USCYBERCOM had the authority necessary to defend the nation writ large, yet another challenge is that, today as a general matter, the government (and in particular the DoD), lacks the relationships and technological fabric between itself and the private sector necessary to make such authority effective.

This latter point is perhaps the most important one. Neither the government nor the private sector can properly protect the relevant systems and networks without extensive and close cooperation. This is true, in large part, because of the way these systems matured and interacted over the past 20 to 30 years. In particular, the private sector controls a vast majority of the cyberspace real estate, particularly when it comes to critical infrastructure and key resources,[18] which means that to create a truly defensible cyber architecture for the nation as a whole, the government and the private sector must closely collaborate.

To do so, we must 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. Given that a key principle of attack is to aim at the seams of command and control, clearly defined rules, including identifying areas of overlapping responsibility, will help minimize opportunities for a cyberattack.

At the same time, the US must recognize that while creating and assigning responsibilities is necessary to address these challenges, it is not sufficient. The US government must collaborate with private entities to help provide the most effective defense. We must learn how to work together in a cooperative environment, and confront the threats the nation faces. Just as the modern military has learned, over the past three decades, how to train, exercise, operate, and fight in a joint, combined arms environment, so too today must the US public and private sectors learn how to train, exercise, and operate cooperatively in cyberspace.

Initially, the government should partner with the private sector to share both government and private threat information, in real time, at network speed, and in a manner that it can be actioned rapidly. Building out a crosscutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to air traffic control. Just as the air traffic control picture ensures aviation safety and synchronizes government and civil aviation, a cyber common operational picture can synchronize a common cyber defense for the US and its allies, drive decision-making, and enable rapid response.

> The US must stay ahead of the problem, think clearly about the challenges we face, and effectively make the critical decisions that are before us today.

Operating collaboratively also means increased side-by-side interaction in the prelude to a crisis, including cooperative training and exercises. As difficult as it was to convince US armed forces to truly adopt 'jointness' and fight as one force, it will be even more difficult to make the private sector and the government interoperable and capable of performing as single, cooperative unit. However, as with the various military agencies in the post-Goldwater-Nichols era, if the nation's cyber architecture is going to be truly defensible in our increasingly networked and vulnerable world, private sector companies must learn how to work with one another in crisis mode, as well as with the government. This will require some measure of interoperability, common practices and procedures, the ability to quickly and tightly integrate, and, perhaps most importantly, a core level of trust.

At the same time, the US must also recognize that sharing and collaboration are not the end, but rather are a means to a more capable national cyber defense. Sharing and collaborating is essential, but taking action and having the capability and authority to act in appropriate circumstances is critical.

The US therefore also needs to build a complementary foundation within the DoD and must put the right rules, procedures, and structures in place within the larger defense and intelligence communities. In recent years, the government successfully established

USCYBERCOM and brought a joint, combined arms approach to this problem. We must now go further by elevating USCYBERCOM to a Unified Command as directed in the FY 2017 National Defense Authorization Act signed by President Obama this past December, providing a consistent and increased set of funding authorities, developing clear authorities and rules of engagement for the defense of the nation, and investing in both people and technology enhancements, thus preparing for what is a more dangerous and rapidly changing environment.

At the same time, important progress already made ought not to be reversed. The way we intend to operate in cyberspace should define the way we are organized. Moreover, it also means that the cyber investments the government makes should continue to be analogous to and undertaken with the vigor and focus of the Manhattan Project, and ought to involve government, academic, and industry participants.

The situation we have faced in recent years—with a fundamental lack of clear thinking about these problems—is particularly troubling because the reality is that adversaries will not wait for us to get this right. The US cannot rely on a false sense of security; while our systems today are resilient and we are working harder to make them more so, we can and must do more now. Assuming blithely that the private sector or the government standing alone will be able to defend the nation is tantamount to the French reliance on the Maginot Line before World War II.

The US ought not to repeat that historically catastrophic mistake in this new domain of cyberspace. The US must stay ahead of the problem, think clearly about the challenges we face, and effectively make the critical decisions that are before us today—in a time of relative calm and before a major incident. If we fail to do so, we will have no one to blame but ourselves when that day arrives, as it inevitably will.

NOTES

1. Annie Sneed, *Moore's Law Keeps Going, Defying Expectations,* Scientific American (May 14, 2015) available online at http://www.scientificamerican.com/article/moore-s-law-keeps-going-defying-expectations/.

2. Peter Diamandis, *The Future is Brighter Than You Think,* CNN (May 6, 2012) ("Right now, a Maasai warrior on a mobile phone in the middle of Kenya has better mobile communications than the president did 25 years ago. If he's on a smart phone using Google, he has access to more information than the U.S. president did just 15 years ago.").

3. Ray Kurzweil, *The Law of Accelerating Returns* (March 7, 2001), *available online* at http://www.kurzweilai.net/the-law-of-accelerating-returns.

4. Cisco, *The Zettabyte Era—Trends and Analysis* (June 2016) at 1, *available online* at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf; *see also* Cisco, *VNI Complete Forecasts Highlights Tool, available online* at http://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html.

5. *Zettabyte Era,* n. 4 *supra* at 2.

6. Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (May 2014), *available online* at http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

7. 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/.

8. 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 cyberattacks 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.")

9. Ibid.

10. United Nations, *U.N. Charter* Ch. 7, Arts. 39, 41, 42 51, *available online* at http://www.un.org/en/sections/un-charter/un-charter-full-text/index.html.

11. North Atlantic Treaty Organization, *Wales Summit Declaration* (Sept. 5, 2014), *available online* at http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber; North Atlantic Treaty Organization, *North Atlantic Treaty,* Arts. 4-5, *available online* at http://www.nato.int/cps/en/natolive/official_texts_17120.htm; see also North Atlantic Treaty Organization, *Cyber Defence Pledge* (July 8, 2016), *available online* at http://www.nato.int/cps/en/natohq/official_texts_133177.htm.

12. White House, *The National Security Strategy of the United States of America* (Sept. 2002), *available online* at http://www.state.gov/documents/organization/63562.pdf; Brian Egan, *International Law, Legal Diplomacy, and the Counter-ISIL Campaign* (Apr. 4, 2016), *available online* at https://www.justsecurity.org/wp-content/uploads/2016/04/Egan-ASIL-speech.pdf.

13. W. Hays Parks, *Air War and the Law of War,* 32 A.F. L. Rev. 1 (1990); Jill M. Sheldon, *Note: Nuclear Weapons and the Laws of War: Does Customary International Law Prohibit the use of Nuclear Weapons in all Circumstances?,* 20 Fordham Int'l L.J. 181 (1996) (collecting materials).

14. NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), available online* at https://ccdcoe.org/tallinn-manual.html.

NOTES

15. Department of Defense, About *USNORTHCOM, available online* at http://www.northcom.mil/About-USNORTHCOM/ ("USNORTHCOM partners to conduct homeland defense, civil support and security cooperation to defend and secure the United States and its interests. USNORTHCOM's AOR includes air, land and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles."); Department of Defense, *North American Aerospace Defense Command* (Apr. 25, 2013), *available online* at http://www.norad.mil/Newsroom/Fact-Sheets/Article-View/Article/578770/north-american-aerospace-defense-command/ ("The North American Aerospace Defense Command (NORAD) is a United States and Canada bi-national organization charged with the missions of aerospace warning and aerospace control for North America. Aerospace warning includes the detection, validation, and warning of attack against North America whether by aircraft, missiles, or space vehicles, through mutual support arrangements with other commands. Aerospace control includes ensuring air sovereignty and air defense of the airspace of Canada and the United States.").

16. 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.

17. See General Accountability Office, *DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents* at 12 (Apr. 2016) ("We found that DOD guidance…does not clearly define the roles and responsibilities of key DOD entities…if they are requested to support civil authorities in a cyber incident…Further, we found that, in some cases, DOD guidance…does not provide the same level of detail or assign roles and responsibilities for cyber support. In other cases, the designation of cyber roles and responsibilities in DOD guidance is inconsistent."); *id.* at 20 ("[T]he absence of clarity in roles and responsibilities to address a cyber incident represents a clear gap in guidance. The gap, and the uncertainty that results, could hinder the timeliness or effectiveness of critical DOD support to civil authorities during cyber-related emergencies that DOD must be prepared to provide…[W]ithout clarifying guidance on DOD roles and responsibilities in a cyber incident, DOD cannot reasonably ensure that the department will be able to most effectively employ its capabilities to support civil authorities in a cyber incident."); *see also* Department of Defense, *The DOD Cyber Strategy* at 7 (Apr. 2015), *available online* at http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf ("For example, DoD's own network is a patchwork of thousands of networks across the globe, and DoD lacks the visibility and organizational structure required to defend its diffuse networks effectively.").

18. 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.").