Prepared Statement of GEN (Ret) Keith B. Alexander[*]
on Digital Acts of War: Evolving the Cybersecurity Conversation
before the Subcommittees on Information Technology and National Security
of the Committee on Oversight and Government Reform

July 13, 2016

Chairman Hurd, Chairman DeSantis, Ranking Member Kelly, Ranking Member Lynch, and Members of the Committee: thank you for inviting me to discuss digital acts of war with you today, and specifically, to engage in a dialogue with this Committee about the rules, norms, and constructs regarding acceptable behavior in cyberspace.

I also want to thank both Chairman Hurd and Chairman DeSantis for playing a leading role in the House of Representatives on cybersecurity matters, including through efforts like Chairman Hurd's legislation on state and local cybersecurity, which passed the House late last year, as well as Chairman DeSantis's leadership in looking into the Office of Personnel Management hack last year. And I know both of you have terrific partners in the ranking members on both your subcommittees, with Ranking Member Kelly's efforts on federal IT acquisition reform and Ranking Member Lynch's work on the OPM investigation.

As members of these subcommittees well know, the key systems and networks that make up what we call colloquially refer 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 our national security and that of our allies. At the same time, cyberspace, as we know it today, has also become a digital battleground where nation-states and their proxies, organized criminal groups, terrorists, hacktivists, and others seek to gain an advantage on one another, whether through surveillance and espionage, criminal activity, recruitment, planning, and incitement to attacks, and repression of free speech and expression. Increasingly, we recognize that while the benefits of global connectivity far outstrip the potential costs, our increased connectivity makes us more vulnerable, as individuals, as groups, and as a nation. As a result, we also increasingly realize that we must proactively take steps to protect ourselves, our information, and our critical assets from the vagaries of crime, theft, espionage, and, yes, potentially destructive activities. And, perhaps most importantly, we understand that the increased connectivity of networked devices to physical systems makes it more possible to create real-world effects through cyber activities.

The numbers on the dramatic growth and expansion of our network connectivity are clear: by 2020, it is expected that IP traffic on global communications networks will reach 2.3 zettabytes, or 95 times the volume of the entire global Internet in 2005.[1] And, as you all know, underlying technology in this area is also growing rapidly, with processing capacity doubling

---

[*] Gen. (Ret) Keith Alexander is the former Director of the National Security Agency and former Commander, United States Cyber Command. He currently serves as the President and CEO of IronNet Cybersecurity, a startup

[1] *See* 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>.

every two years under Moore's law.[2] This combined growth in technology and IP traffic will be accompanied by rapid growth in the sheer number of IP-connected devices, particularly given our move towards the Internet of Things (IoT). Cisco estimates that by 2020 there will be 26.3 billion networked devices, the equivalent of more than three IP-connected devices per person around the world.[3] Traffic from wireless and mobile devices will also account for two-thirds of all IP traffic by 2020,[4] and worldwide mobile Internet penetration is expected to reach more than 70% around the same timeframe.[5]

And 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 our nation is likewise expanding. And while we are all also 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 what I have previously described as the greatest transfer of wealth in human history—I want to highlight an even more troubling trend that began to take hold in the past four years: the emergence of actual destructive cyber attacks, where cyber or other systems, data, or capabilities are permanently destroyed.

In 2012, we saw a set of destructive cyber attacks conducted against Saudi Aramco and Qatari Ras Gas, an attack that resulted in over 30,000 computers being disabled at Saudi Aramco alone.[6] And in February 2014, we saw the first-ever publicly reported destructive cyber attack by a nation-state on U.S. soil, with Iran conducting a cyber attack on the Las Vegas Sands Corporation in February.[7] This was followed later that year, in November, by the North Korea's attack on Sony Pictures.[8] These attacks represent a particularly concerning trend because they demonstrate an expansion in significant cyber capabilities from nation-states like China and

---

[2] *See* 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/>.

[3] *See Zettabyte Era*, n. 1 *supra* at 2.

[4] *See Zettabyte Era*, n. 1 *supra* at 2.

[5] *See* Internet Society, *Global Internet Report 2015*, at 9, *available online at* <http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf>.

[6] *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/>.

[7] *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.")

[8] *Id*.

Russia whose actions are more constrained by external political and economic considerations, to nations that might be more inclined to act or at least may be more unpredictable in the nature and scope of their actions. They are also particularly concerning because the fact of the attacks—and our nation's relatively limited, if any response to them—lay bare the fact that we have no real strategy or doctrine for how to deal with such events, much less deter other nation-states from undertaking them.

In order to develop such strategies and doctrines, and perhaps most importantly, to effectively deter these type of actions, we first need to understand better what constitute acts of war in the cyber domain. The reality today is that while we can all easily imagine acts that regardless of where or how they are undertaken, whether in cyberspace or otherwise, would constitute acts of war—the more challenging part is determining where that line should be drawn in the hard cases. That is, while there are cyber attacks with consequences that would almost certainly fall within the parameters of what we would 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—there still remains an enormous gray area of hostile nation-state actions that might approach, and even cross, the 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 self-defense and how the international community might respond to a breach of the peace.[9] Similarly, a determination by the NATO Alliance that a member-state has been attacked could trigger the collective defense commitment in Article V of the NATO Treaty.[10] Indeed, this issue is all the more pressing given NATO's increased focus on cyber defense and its ongoing recognition, since at least September 2014, that activities in cyberspace can potentially trigger Article V obligations.[11]

At the same time, however, 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 meaning of the U.N. Charter, it may choose not to respond. And many argue that the right of

---

[9] *See* 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>.

[10] *See* North Atlantic Treaty Organization, *North Atlantic Treaty*, Arts. 4-5, *available online at* <http://www.nato.int/cps/en/natolive/official_texts_17120.htm>

[11] *See* North Atlantic Treaty Organization, Cyber Defence Pledge (July 8, 2016), available online at <http://www.nato.int/cps/en/natohq/official_texts_133177.htm> ("We reaffirm our national responsibility…to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales."); *See* 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> ("To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence…. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.").

self-defense does not require a nation to actually wait until an actual armed attack takes place and the consequences are suffered, in order to invoke its right of self-defense against an imminent, pressing threat.[12] Moreover, the decision of 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 uses in response, are profoundly moral questions with implications for the overall conduct of such conflicts 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 here at home, as well as through international institutions, so that we can at least see if it is possible to develop the beginnings of a reasonable international consensus on these matters.

In looking at these questions, particularly in a new domain like cyberspace, we have to think not just about the right and left boundaries of what constitutes acts of war and how and when we might respond, but also about the vital center, and the hard questions that lie within. And while there are no detailed answers to be immediately had in short form, we are also not writing on a blank slate: many have considered the implications on just war theory and international law of new domains or new methods or warfare before, whether with the advent of air war 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 in particular. The Tallinn Manual, a NATO-sponsored effort, provides helpful guidance in this area,[14] and will likely continue to do so, as it is currently in the process of being updated.

When it comes to determining, whether as a legal, political, and moral/ethical matter, what type of acts constitute an act of war, there are some basic constructs one can look towards. First, it seems obvious that the extent of and nature of the damage caused will have some impact on this decision. Second, the intent of the threat actor matters. The nature and type of the systems or data affected by the attack will also certainly play a role, as will the potential immediate and downstream impact of the attack, including the economic, political, and social aspects of such impact. And, perhaps even more importantly, the ability to identify the source of the attack and publicly attribute it may play a crucial role in determining whether a given attack constitutes an act of war and whether or how a given nation might respond. It is fairly obvious

---

[12] *See, e.g.*, 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> ("For centuries, international law recognized that nations need not suffer an attack before they can lawfully take action to defend themselves against forces that present an imminent danger of attack. Legal scholars and international jurists often conditioned the legitimacy of preemption on the existence of an imminent threat—most often a visible mobilization of armies, navies, and air forces preparing to attack."); 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> ("Under the jus ad bellum, a State may use force in the exercise of its inherent right of self-defense not only in response to armed attacks that have occurred, but also in response to imminent ones before they occur….The absence of specific evidence of where an attack will take place or of the precise nature of an attack does not preclude a conclusion that an armed attack is imminent for purposes of the exercise of the right of self-defense, provided that there is a reasonable and objective basis for concluding that an armed attack is imminent.")

[13] *See, e.g.*, 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] *See* 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>.

where an attack is coming from if you see a land-based missile launched with a particular radar or heat signature or a bomber flying over your territory; it is much harder when the attacker is coming at you in cyberspace across a series of hop-points, some of which may be in your own territory, and employing sophisticated obfuscation methods that are widely accessible to a broad range of actors.

Beyond determining whether an act of war has actually taken place, one must be prepared to consider what might be done in response to such an act. Today as it stands, there is very little talk about our cyber capabilities, whether it comes to offense or defense. While it is not obvious that an attack in cyberspace requires a response in the same domain, it is fair to assume that a cyber response must at least be part of the calculus. Without much public discussion of our basic cyber capabilities, particularly on offense, we face two major challenges: it is difficult to have a reasoned discussion of how we might respond—at least in the cyber domain—and it is that much harder to deter offensive actions by others. After all, basic deterrence theory is premised on the notion of being clear on what a nation would likely to do in response to a defined set of actions by an attacker. Without talking about capabilities and defining what set of actions would trigger the use of those capabilities (as well as a clear willingness to actually undertake such a response), it is no surprise that deterrence does not work particularly well today in the cyber domain. And this is all the more important as we see the spread of cyber capabilities to more unpredictable nation-state actors, as discussed above, and even more worryingly, perhaps in the longer-run, to non-state, asymmetric actors like terrorist groups.

The fact of the matter is that today we are not well equipped to address these threats. We have yet to fully think through the doctrine or strategies in this area, much less the authorities and the rules of engagement. And while U.S. Cyber Command is beginning to build the forces and capabilities necessary to carry out this mission on behalf of the U.S. government and our nation, we are a long way from getting to where we need to be to make sure we do it right. In doing so, we also need to make sure that the Department of Defense and the Intelligence Community are properly postured to protect the nation, both through the collection of intelligence and the readiness to respond. This means, in part, that the current approach to ensuring full cooperation and coordination through the dual-hatting of the Director of NSA and Commander of U.S. Cyber Command ought not be undermined by nascent efforts to divide the two out of a need for improved optics. Undermining our readiness and capability to act swiftly in order to address perception issues sets us on exactly the wrong course.

The current situation is particularly troubling because the reality is that the enemy will not wait for us to get this right. We cannot rely on a false sense of security; while our systems today are fairly resilient and we are working harder to make them more so, we must do more. Perhaps most importantly, given the fact that the vast majority of our key networked infrastructure is owned and operated by the private sector, the government and the private sector must learn to work together to defend our nation in cyberspace. Assuming that either the private sector or the government standing alone will be able to defend our nation is tantamount to the French reliance on the Maginot Line during the lead-up to World War II. We ought not repeat that historically catastrophic mistake.

I’m glad to be here today to discuss these issues with you and look forward to answering your questions.