Prepared Statement of GEN (Ret) Keith B. Alexander[*]
on the Future of Warfare before the
Senate Armed Services Committee

November 3, 2015

Chairman McCain, Ranking Member Reed, Members of the Committee: thank you for inviting me to discuss the future of warfare with you all today and, specifically, to engage in a dialogue with this Committee about two of the most pressing threats facing our Nation: (1) the threat from terrorist groups with global reach and ambitions; and (2) the threat from criminal syndicates and nation-states in cyberspace. I plan to talk candidly about these topics and give you a sense of where I think we are headed and what we might do to mitigate the very serious risks and threats we face as a nation.

I want to thank you, Mr. Chairman, for taking the time to look at the major issues facing the Department of Defense and how we might architect the Department and our military services as we face evolving threats in this new environment. The efforts both you and the Ranking Member have made in this area will help ensure the security of our going forward and will help us keep faith with the men and women who serve our country with pride and honor in the far reaches of the globe.

Before we turn to the future of warfare, it is important to discuss some of the significant changes going on in the hugely challenging global environment we find ourselves in today. In my mind, this discussion is critically important because it frames the way we need to think about future conflicts and how we might shape the Defense Department and our military services to be prepared for these conflicts.

We live in amazing, challenging, and threatening times. Around the world, we see conflicts or situations that could easily spiral out of control, dramatically affecting our national security. Indeed, in many places, this process has potentially already begun. From the longstanding homeland threat posed by al Qaeda core and its affiliates around the world, to the growth of a potential terrorist state in the lands of Iraq and Syria, and the increasing role of Hizballah and Hamas in various conflict zones, just to name a few, the threat of terrorism is on the rise. Even more troubling, major nation-states continue to behave in ways that seek to challenge the United States and intimidate our allies.

China continues to experience tremendous economic difficulties that drive their need to steal intellectual property and strengthen their stance in the South China Sea. Russia's intervention in Ukraine and in the Syrian conflict are just the start of a potential series of actions that seek to reshape the international environment in ways that do not reflect America's interests. And a number of key allies and other important states face the very real threat of internal dissent and potential collapse. These regional conflicts and the surge of terrorist activities point to an uncertain future, with tremendous potential impact on our Nation.

Moreover, in the cyber realm, we also see threats increasing. Whether it is the growing spread of nation-state espionage, including hacks against government systems and the rampant theft of core U.S. intellectual property from our companies, or financial crime conducted by criminal syndicates and nation-

[*] 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 technology company headquartered in the Washington, DC metropolitan region.

state sponsored groups, or the very real threat of destructive cyber attacks against critical infrastructure companies, we are seeing a rapid increase of challenges in this domain also.

The evolution of computers and networks, the growing challenges to network and cyber security, and underlying concerns about civil liberties and privacy greatly complicate these areas. I am deeply concerned that our current cybersecurity strategy is incomplete at best and is further complicated by many of these issues.

I would like to start first with technology, then turn to terrorism, and finally briefly discuss how we might work to improve military readiness in these areas.

Technology is an area of rapid and dramatic change and growth, with processing capacity doubling every two years under Moore's law.[1] Moreover, Cisco estimates that annual global IP network traffic will exceed one zettabyte by the end of 2016 (or nearly 1 billion gigabytes per month), and will nearly double to two zettabytes per year by 2019.[2] This means that global Internet traffic in 2019 will be approximately 66 times the volume of the entire global Internet traffic in 2005.[3] And, around the world, the number of devices connected to IP networks will be more than three times the global population by 2019.[4]

And while former Secretary of Education Richard Riley's prediction in the early 2000s about the job change across the economy may not have been exactly right, it certainly seems to me that his point is spot on when it comes to technology: namely, that many of the specific jobs available in technology today didn't even exist a decade ago; indeed, the notion, attributed to Riley, that "we are training young people for jobs that don't even exist yet, to use technology that hasn't been created yet, to solve problems that we don't even know are problems yet" seems clearly right.[5] Others have noted that for the first time in history, we have four generations working side-by-side: the "write me," "call me," "email me," and "text me" generations.[6] Today, we think and talk about communications and human interaction fundamentally differently. We talk about "hanging out" – not in person, but online via Google; we talk about swiping, not to steal something, but to look for a mate on Tinder. Indeed, any person with access to Google today has better access to information than the President of the United States did 20 years ago. And some have suggested that by 2049, a $1,000 computer will exceed the computational capabilities of the entire human race.[7]

[1] *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/>.

[2] *See* Cisco, *The Zettabyte Era—Trends and Analysis* (May 2015), *available online at* <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html>

[3] *Id.*

[4] *Id.*

[5] *See* Steve Gunderson, et al., THE JOBS REVOLUTION: CHANGING HOW AMERICA WORKS, 58-60 (2004); David Tritelli, *From the Editor*, Liberal Education, vol. 9, no. 1 (Winter 2009), available online at <https://www.aacu.org/publications-research/periodicals/editor-56>.

[6] *Cf., e.g.*, Mareisha Winters, *Write Me, Call Me, Text Me: Generational Differences in the Workplace*, Let's Talk About Work (Aug. 15, 2012), available online at <http://www.letstalkaboutwork.tv/write-me-call-me-text-me-generational-differences-workplace/>.

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

These changes are stunning and, in my view, form the foundation for other great revolutions. For example, nanotechnology is utilizing these data advances to make amazing progress. In June of 2014, I had a chance to see the improvements IBM is making in addressing brain cancer by partnering with the Genome Center in New York City. The prognosis on brain cancer radiation treatment that used to take nearly a month for a panel of oncologists can now be done in minutes with computer analytics.

As such, technological change presents tremendous opportunities. But with these tremendous opportunities come tremendous vulnerabilities. From my perspective, there are four major threats in the cyber domain: cyber attack, cyber espionage, cyber theft of intellectual property, and criminal activity. In 2014, the Center for Strategic and International Studies estimated the worldwide loss from cybercrime to be $445 billion annually.[8] While this number seeks to account for the theft of intellectual property, in my view, the value of theft of intellectual property from American industry is significantly greater than accounted for in this study and, in fact, represents the single greatest transfer of wealth in history.

At the same time, the potential for actual cyber attacks also represents a major threat to our national security. Both the scope and nature of this threat is growing, as is the probability of increasing disruptive and destructive attacks. Specifically, since the 2007 attacks against Estonia, the pace and nature of cyber attacks has grown. In 2008, we had the attacks against Georgia and the discovery of agent.btz malware in U.S. military systems. In 2012, we learned of the first publicly disclosed destructive attack against Saudi Aramco, where data on approximately 30,000 computers was destroyed, followed soon there after by a similar attack on Qatari RasGas. Between 2012 and 2014, we saw large-scale distributed denial of service attacks on U.S. bank websites. And we have all heard about the potential impact of the Havex and BlackEnergy malware on industrial control systems in the energy industry. We also see cyber threats from criminal actors, although these are largely focused on theft, including of customer data, at places like Target and Home Depot.

And while many of these hacks might be achieved with relative ease, most of the prominent events that we discussed have involved very sophisticated attackers using unique skill sets, clearly suggesting that there is some measure or potential of nation-state involvement or sponsorship.

Having now talked about the cyber threat, I like to turn back to the terrorism threat, which we discussed briefly earlier and then get into how we might think about some of these issues going forward.

On terrorism, just a few key points. There has been a massive increase in global terrorist acts and deaths from terrorism in recent years. According to State Department statistics, between 2012 and 2013, we saw a 43% increase in terrorist attacks worldwide and 61% increase in people killed as a result of terrorism.[9] Between 2013 and 2014, we saw another 39% increase in attacks and an 83% increase in

[8] *See* 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>.

[9] *Compare* U.S. State Department, COUNTRY REPORTS ON TERRORISM 2012*,* National Consortium for the Study of Terrorism and Responses to Terrorism: *Annex of Statistical Information* (2013), *available online at* <http://www.state.gov/j/ct/rls/crt/2012/210017.htm> (6771 attacks; 11098 fatalities) *with* U.S. State Department, COUNTRY REPORTS ON TERRORISM 2013, National Consortium for the Study of Terrorism and Responses to Terrorism: *Annex of Statistical Information* (2014), *available online at* <http://www.state.gov/j/ct/rls/crt/2013/224831.htm> (9707 attacks; 17891 fatalities)

deaths, which represents a nearly tripling of deaths in just two years.[10]

When you combine these statistics with the issues we discussed briefly before: the permissive environments created by government collapse in countries like Yemen and Libya, ISIS control of territory between the lands of Iraq and Syria, increased Iranian support for proxy group like Hizballah and Shia militias in Iraq, continued interest by core al Qaeda and its affiliates like AQAP in homeland attacks, and the increasing pace of conflicts that continues to potentially destabilize countries in the Middle East, North Africa and elsewhere, we see a very challenging environment for America's national security and a clearly increasing terrorist threat.

Having discussed the challenges facing us in both the cyber and terrorism environments, I would like to also briefly talk about key areas we need to change within the Defense Department to counter these asymmetric threats.

When I retired in April 2014, I believed I could "continue the mission" by helping the private sector better protect themselves with better cybersecurity solutions. I believe there is much to be done to bring commercial cybersecurity to the "right" standard and my experience, to date, is that business leaders are working these issues hard. In building a comprehensive approach to cybersecurity, we need to build a foundational framework that will give us the opportunity to provide game-changing new defensive capabilities to the private sector.

More importantly, commercial and private entities cannot defend themselves alone against nation-state attacks nor nation-state-like attacks in cyberspace. And we do not want them to "fire" back. The U.S. Government is the only one that can and should "fire" back. That is, it is the government's job to defend this country in cyberspace from the type of destructive attacks that hit Sony and the disruptive attacks that hit Wall Street from August 2012 to April 2013. Truth be told, our Nation simply is not prepared for these events, at least at this time.

To resolve this problem, we need cyber legislation that provides clear authority and liability protection to incentivize information sharing. Thank you for the work all of you have done in passing the cyber legislation. However, that legislation needs to ensure the government can do its job of defending our Nation at network speed, because that is the speed of these attacks. We also need industry to be able to "tell" the government when they are under attack, at network speed, and the appropriate entities in government should receive this information at network speed, without delay. Our Nation will depend on that capability and speed in the next cyber engagement we face.

In particular, for the Department of Defense, this means that DOD needs to receive information—directly and at network speed—that will help it protect the Nation. DHS and other entities can receive this information at the same time, but information relevant to the defense of this country should not be delayed by another department or agency. I know that the legislation has a range of provisions on this issue, some that provide flexibility, and others that route information through particular paths. It is critical that as the two Houses confer on the final bill, members should keep in mind the critical

[10] *Id.*; *compare also* COUNTRY REPORTS ON TERRORISM 2013 (9707 attacks; 17891 fatalities) *with* U.S. State Department, COUNTRY REPORTS ON TERRORISM 2014, National Consortium for the Study of Terrorism and Responses to Terrorism: *Annex of Statistical Information* (2015), *available online at* <http://www.state.gov/j/ct/rls/crt/2014/239416.htm> (13463 attacks; 32727 fatalities).

importance of speed and flexibility for protecting the Nation against threats that morph rapidly and in real-time.

As a consequence, we also need to build a complementary foundational framework within the Department of Defense. Most importantly, we need to have the right structure in place. As you know, during my tenure as Director of NSA, we worked closely within the Executive Branch and with this Committee to come up with the right structure and capability for U.S. Cyber Command. And while these efforts have been successful and we have been able to bring a joint, combined arms approach together at Cyber Command, we now have an opportunity to go further. In my mind, some of the important concepts to consider include elevating U.S. Cyber Command to a Unified Command, providing it a consistent and increased set of funding authorities, investing in both people and technology enhancements, and preparing for what is an obviously more dangerous and rapidly changing environment. I believe our cyber investments should be analogous to and undertaken with the vigor and focus of the Manhattan project, and should involve both government and industry participants.

On both the cyber and terrorism fronts, we also need to make significant progress in thinking more clearly—both in strategic and tactical terms—about how to deal with the increasing scale and scope of asymmetric threats. In particular, the use of asymmetric capabilities by an increasingly broader array of actors, many of whom don't respond to typical state-to-state incentives, raises tough issues for our military. A lighter, faster, more responsive and agile set of forces, specifically aimed at the terrorism and cyber target sets, is critical. Similarly, providing more authority and flexibility to commanders in the field working in these areas is critical to taking advantage of a more flexible and responsive force.

In the end, while we have may significant progress in these areas in recent years, much more remains to be done and I look forward to providing you whatever assistance I can in your efforts going forward.

Thank you for your time and attention.