Testimony of Admiral James Stavridis, USN (Ret)

Before Senate Armed Services Committee

Cyber Security

22 May 2017, SD-G50, Dirksen Senate Office Building

Chairman McCain, Ranking Member Reed, Members of the Committee:

Thank you for the invitation to appear before you today to discuss the most disruptive force facing America's military and society today: the rapid emergence of cyberspace as an operational domain for armed conflict, as well as a gaping vulnerability in our commercial, financial, and infrastructure systems. I commend the members of this Committee for their continued commitment to advancing America's defense interests in cyberspace, and I ask that my remarks, which were provided to the committee previously, be entered into the record.

And I am honored to appear with two Air Force Generals whom I have known and deeply admired for decades. You may also note this is a panel that may not always agree on our views and but we have managed to coordinate our hairlines. ☺

Cyberspace is indeed a new domain of warfare but it is one unlike sea, air, and land in that it is not physically traversable by our sailors, airmen, and soldiers. The digital battle space of the twenty-first century is not marked by geographic landmarks or public infrastructure, but rather operating systems, routers, switches, and servers — most of which are designed, manufactured,

owned and operated by both American and international companies and citizens, i.e. the private sector. As a nation we are under-educated in these systems, and few could actually explain how an email gets from their iPhone 7 to their grandmother's iPad. Yet these systems are highly at risk at every level, from our national security – proven by well-documented attacks from Iran, North Korea, China, and Russia; in our commercial sector, with cyber crime rising rapidly and approaching perhaps hundreds of billions of dollars globally on an annual basis; and indeed in the most intimate details of our personal lives, which are far-too-often carried unprotected in the super computers we casually carry in our pockets and purses. Of all the threats our nation faces, only cyber cuts across so many dimensions.

There are 7 billion people on the planet, but perhaps 20 billion (or more) devices connected to the Internet. As we saw during the recent attack on Dyn, the internet of things became a "botnet of things" creating significant commercial havoc and threatening consumer confidence in the security and reliability of commoditized online services. There are 23 victims of malicious cyber activity per second according to a 2016 report from Norton, and many studies suggest that damage to our national economy approaches $200 billion per year. We have seen North Korea, China, Iran, and Russia – among other nations – attempt to penetrate of cyber defenses and conduct a wide variety of espionage, commercial damage, data manipulation, and kinetic destruction to infrastructure. The Department of Justice has brought indictments against agents from all of those nations

Because we are under-educated and lightly protected, offensive cyber actors, comparatively large in numbers and concealed by the identity-obfuscating properties of cyberspace, enjoy a

significant advantage over the defense, which, in the United States, is necessarily constrained in its maneuverability to protect our citizens' privacy and civil liberties.

Today, therefore, I would like to preface my opening comments by declaring two seemingly obvious but fundamental truisms that I would suggest inform the Department of Defense's and the Nation's cyber policies and strategies in this decade and beyond.

First, the United States military is today deeply challenged in *preventing* destructive cyber attacks against the nation from capable adversaries, to include state and non-state actors. While we have made progress, we have not trained, equipped, and organized ourselves to be safe in cyber space.

Second, and closely related, the United States is undoubtedly most visible, exposed and lucrative target Nation in this new military domain and therefore subject to disruptive and destructive attacks from not just well resourced nation-states and sophisticated criminals, but also jihadist and other terrorist organizations.

Given these basic facts, the Department's cyber posture must shift from one that is primarily focused on mitigating and defending from malicious cyber activity to one that also aims to deter state and non-state adversaries and belligerents in cyberspace while reducing the threat from lower level actors. Raising the barriers to entry for bad actors will require a stronger and more robust military capability; better organization within the US government at the cabinet and agency level; higher levels of societal education about the risks and concerns we face; better

technology and equipment; and a vastly improved level of private-pubic cooperation. Overall, we must make it harder, costlier, and more time intensive for our adversaries to effectively operate in cyberspace.

Creating real deterrence in cyberspace against opposing national actors will be challenging. If we can agree that deterrence is the combination of both capability and credibility, it is clear that we have work to do on both fronts.

In terms of capability, we have extraordinary offensive and defensive cyber tools, but we must continue to improve as our opponents are doing so rapidly. I would argue that it is also time to strongly consider whether or not we want to create a dedicated cyber force.
While the individual services today – Army, Navy, Marine Corps, Air Force and Coast Guard – are working hard, they are like five horses who can often pull in slightly different directions. Unfortunately the current distributed force structure across each of the services not only breeds redundancies, threatens unity of command, and fosters unproductive competition within the Department, but it also dilutes the increasingly rare and therefore precious core competencies of our cyber planners, operators, trainers, and commanders.

United States Cyber Command declared Full Operational Capability (FOC) in 2010 and seven years later, despite the valiant and well-intentioned efforts of Admiral Mike Rogers and his predecessor, General Keith Alexander, the Cyber Mission Force has demonstrated to be a less than formidable and sustainable model. Most recently, of the 126 Airmen who completed their first tour with the Cyber Mission Force, zero were retained for a second tour. In other words, all

126 Airmen were assigned to other Air Force missions with no cyber nexus whatsoever. In this regard, establishing an independent cyber force would constitute a *show of force* — sending a message to our allies and adversaries alike that the United States is committed to recruiting, retaining, and training cyber warriors not just for a single tour but for a career — one that is in some ways traditional to military life and in other ways wildly different and perhaps more representative of life at a Silicon Valley start-up.

From an historical perspective, we have stood at this moment before, roughly a hundred years ago, as we contemplated another new medium in which combat would occur: the air. The Navy and Army fought the idea of an Air Force for decades until forced to concede after Congressional action. Today, and I think my esteemed panelists would agree, we cannot imagine our joint warfighting capability without a US Air Force. It is time we at least began a conversation about a US Cyber Force. The idea will be vehemently opposed by the services, just as the Army and Navy fought the idea of an Air Force. But sooner or later, common sense tells us we will end up with a specialized force in this zone of combat.

I will also observe that many of these same arguments would apply to both Space warfare specifically and Information Dominance broadly. It is certainly worth exploring whether a Cyber force, a Space force, or a broad Information Dominance force makes the most sense. Chairman Rogers in the House gave a powerful and sensible speech on the space aspects of this. Since we are looking today at Cyber, I will keep my arguments focused on a cyber force; but I freely admit this is a broader question that encompasses space and information dominance together.

A good model to consider as a "starter step" for a cyber force would be to fully make Cyber Command independent and then use the Special Forces model – a defined budget, specialized operators form the services (think SEALS, Rangers, Green Berets, PJs, and Recon Marines), but a defined career path in Cyber much as a Navy SEAL largely has a defined operational career path in the Special Forces. Over time, we may want to shift beyond this to a full blown individual service.

This could start relatively small, with numbers in the 5-10,000 range, a lean administrative structure, and connectivity to the larger services.

The Congress may want to task the Department of Defense with studying the idea and reporting on the options worth considering. The administrative path of Goldwater-Nichols may be instructive.

While standing-up a U.S. Cyber Force would constitute a major step towards establishing a credible deterrent, it is not sufficient by itself. In addition to signaling our long-term commitment to defending our interests in cyberspace, we must also signal both the capability *and* the will to project cyber force across the globe. For this to happen, we must satisfy two conditions.

First, we must somewhat lift the veil off of military cyber operations. I have no doubt that the United States' Armed Forces boasts some of the most advanced, if not *the* most advanced, cyber capabilities in the world. But if we refuse to demonstrate or even acknowledge this capability we are only encouraging aggression from other, less capable actors against our highly vulnerable

infrastructure. In a world in which the number of networked devices exceeds the world's population by more than three fold, we simply cannot afford to confine cyber operations to the covert toolkit. To the contrary, cyber operations are a legitimate means of projecting national power, especially when proportionately supplemented by kinetic force, and we should advertise them accordingly.

In addition to shedding light on our non-kinetic military capabilities, we must convince the world that we, despite living in a glass house, are not afraid to throw stones. Interestingly, the United States' unwillingness to operate offensively in cyberspace is driven less by a fear of retaliation and more by a fear of compromising our Intelligence Community's sensitive tradecraft. The diminished stature of United States Cyber Command as a Sub-Unified Combatant Command (COCOM) under United States Strategic Command, combined with its institutional, leadership, and technical ties to the National Security Agency (NSA), has limited our Armed Forces' cyber freedom of maneuver in support of military objectives.

We should also increase our work with allies, many of whom are quite adept in this sphere. In addition to NATO partners like the UK, France, Germany, and Estonia, other nations with significant ability include Israel, Japan, South Korea, Singapore, Sweden, Australia, and others. Cyber security is a team sport not only in the interagency, but within our international alliances and coalitions.

Related to this, the Department must embrace and employ an agile software development lifecycle and mindset that accommodates development sprints and high rates of failure. These

methodologies, tested and proven in the private sector, will enable our cyber warriors to keep pace with what is certain to be a more fluid and dynamic operational tempo than ever before.

It is also imperative that the Department establish a solid doctrinal foundation. The policies governing how our military operates in cyberspace will likely change many times over in the next decade, but we must quickly establish a common vernacular — not just within the Pentagon but across the national security apparatus and the government as a whole. For starters, we must not diminish the many forms of cyber aggression our governments, companies, and citizens are experiencing. Consider, for example, the Sony hack in 2014 reportedly attributed to North Korean and dubbed an act of "cyber vandalism" by former President Obama. "Cyber vandalism" is defacing a webpage over an ideological difference; the Sony hack could certainly be considered as an act of war – in addition to millions of dollars of kinetic damage to Sony's hardware, a high level of business value was destroyed. While no one died, the damage was significant. We, of all Nations, cannot afford to understate or diminish the significance of force projection in cyberspace. We need to create a "definition of a cyber attack," which differentiates among surveillance, espionage, commercial interference, data modification and manipulation, data destruction, infrastructure attack on critical infrastructure, kinetic damage, and loss of human life.

We should be thinking more holistically about how the US government conducts cyber security and the role of the Department of Defense in that mission. Today, cyber security falls under a plethora of different cabinet departments – DHS, DOJ (FBI), DOD (NSA), and DNI. There are six different cyber security centers run by the US Government. We have a Secretary of

Agriculture and a Secretary of the Interior in the Cabinet, but not a single voice for Cyber. There are a number of ways to address this, from a Department of Cyber that fuses all of those functions and centers (much like the British have done with the creation of their National Cybersecurity Centre NCSC, embedded in GCHQ) to giving a unifying voice to one Cabinet Secretary (perhaps the DNI becomes the DNIC, Director of National Intelligence and Cyber Security). Many of these ideas were explored by the Commission on Enhancing National Cybersecurity, led by fomer National Security Adviser Tom Donilon – I endorse many of its findings. As a side note, I think it is also time to strongly consider splitting the positions of US Cyber Command (a military warfighting Combatant Command) and the Director of the National Security Agency (fundamentally an intelligence gathering operation, although also invested with cyber activities both offensive and defensive). The span of control and differing missions makes continuing to merge those in one person – even one as good as the two officers with me today or Admiral Mike Rogers – less than optimal. Bottom line – we are not organized to seamlessly defend or fight in cyberspace as a nation and have a great deal of work to do, both as a nation and within the Department of Defense.

Finally, as an educator myself these days, I cannot resist making a comment about the role of education in increasing our national security and indeed our own efficiency within the Department of Defense. We have to improve all level of Science, Technology, Engineering, and Math in our educational system, of course; but there needs to be particular emphasis on the practical skills of cyber as well as understanding how to defend ourselves individual. Over 70% of all hacks, intrusions, cyber crimes, and so forth result from simple failures in cyber hygiene. This is true for society at large and the Department of Defense. More emphasis on this aspect is

like “soft power” in the context of national strategy – it is preventative, cheap, and has enormous ancillary benefits. While not specifically under the purview of this Committee, it is something the Congress can be influential in pushing and would go far toward helping with the overall mission of cyber security.

In so many ways, in the world of cyber security we are still “on the beach” at Kitty Hawk to use an aviation analogy. Or to shift to a maritime one, we are sailing in very choppy seas. The Congress can play an important role, as it has historically, in helping the Department of Defense and the rest of the Federal Government to improve all elements of our security.

Again, thank you for asking me to come and testify. I am happy to answer any questions the Committee may have.