ORAL REMARKS OF

MS. KATE CHARLET

ACTING DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

TESTIMONY BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

APRIL 4, 2017

(816 Words)

Thank you [Senator McCain,] Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee. It is an honor to appear before you to discuss the Department's efforts to respond to growing cyber threats.

I am here today in my role as Acting Deputy Assistant Secretary of Defense for Cyber Policy, in which I oversee cyber policy in the Department, including policies governing CYBERCOM's activities and operations. I am grateful to have my interagency colleagues with me today, because these challenges require a whole-of-government approach. I would also like to acknowledge behind me Major General Ed Wilson, the Deputy Principal Cyber Advisor, whose team plays a key role in cyber issues that cut across DoD organizational boundaries.

As my DNI colleague noted, we face diverse and persistent cyber threats. Our adversaries have the cyber capabilities to hold at risk U.S. critical infrastructure as well as the broader ecosystem of internet-connected and enabled devices. These threats cannot be defeated through the efforts of any single organization, a challenge reinforced by the fact that the majority of critical infrastructure in the U.S. is owned and operated by the private sector.

DoD is developing cyber forces and capabilities to accomplish three primary missions in cyberspace: 1) to defend DoD networks, systems, and information to ensure that DoD can accomplish its core missions; 2) to defend the United States and its interests against cyberattacks of significant consequence; and 3) to provide integrated cyber capabilities in support of contingency and operational plans. This second mission is the focus of efforts to defend critical infrastructure, but I would be happy to address any of the three in Q+A.

The Cyber Mission Force plays a key role carrying out these missions. These include: First, Cyber Protection Teams, which focus on network defense missions; Second, National

Mission Teams, which are aligned to specific adversaries. These teams develop and, if directed, undertake operations to prevent, preempt, stop, or blunt an imminent or ongoing cyberattack or malicious cyber activity; and Third, Combat Mission Teams, which take the fight to the adversary, for example, by conducting offensive cyber operations against ISIS. NSA's authorities, capabilities, and intelligence are also powerful tools to help us understand adversaries as well as develop operations and mitigations in real-time.

The Department supports federal partners in protecting critical infrastructure through our Defense Support of Civil Authorities and other missions. This support occurs through cyber fusion center integration, robust information sharing agreements, and liaison and detailee programs. During cyber incidents, DoD may directly support DHS's lead for protecting, mitigating, and recovering from domestic cyber incidents, and/or DOJ's lead in investigating, attributing, disrupting, and prosecuting cybercrimes.

In particular, the Department's 68 Cyber Protection Teams represent a significant capability to support a broader domestic response, if necessary. These forces are focused on defending DoD networks, but select teams could provide additional capacity or capability to our federal partners if necessary. These teams are aligned to protect a variety of systems and networks, including industrial control systems and other cyber-enabled Platform Information Technology.

DoD is developing significant cyber capability and capacity within the Reserve Component, including the National Guard. The teams that are being built can act in either federal or state capacities. They are trained, equipped, and held to the same standard as their Active Duty counterparts.

DoD also plays a leading role in protecting the critical infrastructure of the Defense Industrial Base, one of the 16 critical infrastructure sectors. Using voluntary and mandatory reporting requirements, the Department partners with DIB stakeholders to maintain a strong cybersecurity and information assurance program that allows for improved threat awareness, enables mitigation in case of an incident, and protects DoD information on DIB networks. 197 cleared defense contractors participate in the program.

Finally, DoD recognizes its own reliance on cyber-enabled critical infrastructure to conduct its core missions. Accordingly, we are working with our U.S. domestic and international partners to identify cyber vulnerabilities at the platform, mission, and campaign plan level. There remains much work to be done, but we are applying risk management processes to develop resilience strategies for the capabilities most critical to DoD, such as those necessary to project power, protect the U.S. homeland, and prevail in conflicts.

Although roles and responsibilities are largely understood, we are still working through seam and gap issues. These include, for example, better understanding the circumstances when DoD would be asked to support domestic authorities, refining procedures to ensure maximum speed and flexibility, and exercising combined physical and cyber incidents. It's important to note that any significant realignment of roles and responsibilities would have opportunity costs, including absorptive capacity to build mission capability in a new area.

Our relationship with Congress is critical to everything we are doing to defend the nation from cyber attacks of significant consequence. I am grateful for the Subcommittee's interest in these issues, and I look forward to your questions.

STATEMENT OF

MS. KATHERINE CHARLET

ACTING DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

TESTIMONY BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

APRIL 4, 2017

Thank you Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee. It is an honor to appear before you to discuss the Department's efforts to respond to growing cyber threats. I appear before you today in my role as Acting Deputy Assistant Secretary of Defense for Cyber Policy.

I have been asked here to discuss the Department's approach to responding to cyber-enabled information operations and DoD's role as part of an interagency response in protecting critical infrastructure. I am grateful to have my interagency colleagues here to join me today, because adequately addressing these important challenges requires a whole of government approach, of which the Department of Defense and its developing capabilities in cyberspace are just one part.

To begin, I want to acknowledge the threat and level of malicious activity that we are facing in cyberspace. We face a diverse and persistent set of threats from state and non-state actors who probe and scan U.S. networks for vulnerabilities. The states we watch most closely in cyberspace include China, Iran, North Korea, and especially Russia. As my colleagues from the Office of the Director of National Intelligence and U.S. Cyber Command's J2 will discuss in detail, Russia is a full-scope cyber actor that poses a major threat to the U.S. Government, military, diplomatic, commercial, and critical infrastructure networks and systems. Russian efforts to influence the 2016 U.S. presidential election represent the most recent expression of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order, but these cyber-enabled activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls." Russia's intelligence services conducted cyber operations against targets associated with the 2016 U.S. presidential election, including targets associated with both major U.S. political parties. Moreover, we expect Moscow will apply lessons learned from the campaign aimed at the U.S. presidential election to future influence efforts worldwide, including against U.S. allies and their election processes.

More broadly, our adversaries have the cyber capabilities to hold at risk U.S. critical infrastructure as well as the broader ecosystem of internet-connected and enabled devices. The cyberattacks on the Ukrainian power grid in 2015 and 2016 demonstrate how such malicious cyber activities might be accomplished and the implications for the physical world. If an adversary can accomplish its objectives through cyberspace, it provides new avenues for coercion and deterrence that demand our attention.

Given this context, the Department is developing cyber forces and capabilities to accomplish three primary missions in cyberspace: to defend DoD networks, systems, and information to ensure that DoD can accomplish its core missions; to defend the United States and its interests against malicious cyber activities and cyberattacks of significant consequence; and to provide integrated cyber capabilities in support of contingency and operational plans. More broadly, the U.S. government is strengthening a whole-of-government approach to address the type of influence activities described previously. As part of the Fiscal Year 2017 National Defense Authorization Act, Congress expanded the mission of the State Department's Global Engagement Center (GEC) – which previously focused solely on non-state actors – to include countering state-sponsored propaganda and disinformation efforts as well. DOD works closely with the GEC, contributing detailees, funding, and technical expertise to support the whole of government efforts led by the GEC.

Although all of the missions are important, given your focus today, my intent is to speak primarily about DoD's efforts to defend the United States and its interests against malicious cyber activities and cyberattacks of significant consequence and its efforts to provide defense support for civil authorities, as these are the missions that frame the Department's approach to cyberspace operations and define DoD's role in protecting critical infrastructure within the United States.

The Cyber Mission Force (CMF) is the Department's principal capability to carry out DoD's cyber mission. Consisting of more than 6,000 Soldiers, Sailors, Airmen, Marines, and civilians, this Force achieved initial operational capability (IOC) in October 2016 and is projected to reach full operational capacity (FOC) by the end of fiscal year (FY) 2018. In recent years, the Department has made significant investments in building the workforce and systems to develop the CMF and continues to do so consistent with the FY2017 and soon-to-be-released FY2018 budget requests. In terms of readiness, as well as operational activities in support of the campaign to destroy the Islamic State in Iraq and Syria (ISIS), DoD is already seeing the results of those investments paying off. U.S. Cyber Command's increased experience, expertise, and capability is also driving the Department to pursue elevation of U.S. Cyber Command to a Unified Functional Combatant Command, consistent with Section 923 of the National Defense Authorization Act of FY2017. Among other benefits, elevation of the command will allow the Department to streamline the military chain of command and consolidate responsibility for cyberspace operations under a single commander, reporting directly to the Secretary.

Although many elements of the CMF contribute to defending the nation against malicious cyber activities and cyberattacks of significant consequence, the National Mission Teams (NMTs) play a key role. NMTs are reinforced by National Support Teams (NSTs), which provide additional capacity in analysis, linguists, reporting, capability development, and targeting. As the primary counter-cyber forces, the NMTs and NSTs are adversary-aligned and are focused on learning the tactics, techniques, and procedures of our adversary's cyber forces in order to detect malicious activity. They develop and, if directed, undertake operations to prevent, preempt, stop, or blunt an imminent or ongoing cyberattack or malicious cyber activity. The CMF's other forces—the network defense-oriented Cyber Protection Teams (CPTs) and the operations-focused Combat Mission Teams (CMTs)—also help impose costs on adversaries responsible for malicious cyber activities or cyberattacks by respectively denying them success in their operations and taking the fight to them. The combined efforts of these teams gives the CMF the capacity to operate on a global scale and against the broad spectrum of adversaries.

The National Security Agency (NSA) also plays an important role in the Department's efforts in defending the nation from cyber malicious activities and cyberattacks of significant consequence. Signals intelligence and information assurance inform our cybersecurity operations. Harnessing the power of NSA's authorities, capabilities, and intelligence—as well as its understanding of the cyber threat—allows the NSA to get ahead of foreign-based cyber adversaries and preempt significant cyber incidents against networks vital to the United States. NSA counters our adversaries' experience in cyberspace by discovering and s haring adversaries' plans, intentions, and capabilities; developing, planning, synchronizing, and executing operations and mitigations to counter malicious cyber activities in real-time; and leading and collaborating across the U.S. Government, allied partners, and industry to increase collective understanding of our adversaries' cyber tradecraft.

From both a deterrence and response standpoint, these teams are central to the Department's approach to cyber operations and to support U.S. Government efforts to protect critical infrastructure. With a goal of ensuring U.S. military dominance in cyberspace, these teams support the Department's efforts to deny the adversary the ability to achieve its objectives. And, when directed, the teams may also undertake military action to impose costs through cyberspace in response to an imminent, ongoing, or recent attack or malicious cyber activity. Although DoD's focus is on preparing for and preventing malicious cyber activities or cyberattacks of significant consequence, the President may determine that a military cyber response to malicious activity below the threshold of significant consequence or an armed attack may be necessary and appropriate.

The outward, threat focus of DoD's cyber capabilities complements the strengths of our interagency partners, and we continue to refine the policies, procedures, and relationships to ensure synergy of our combined efforts. Whether through day-to-day information and threat awareness sharing, development of national plans, exercises to strengthen our response, or interagency deliberations on malicious cyber activity, DoD is grounded in a whole of government effort to protect U.S. national interests in and through cyberspace.

Consistent with national policies as well as core roles and capabilities, the Department works closely in support of domestic partners as they carry out their responsibilities to protect critical infrastructure as part of the broader Defense Support of Civil Authorities and other missions. DoD regularly works closely with domestic partners through cyber fusion center integration, robust information sharing agreements, and liaison and detailee programs. During cyber incidents, DoD may directly support the Department of Homeland Security's (DHS's) lead for protecting, mitigating, and recovering from domestic cyber incidents , the Department of Justice's (DOJ's) lead in investigating, attributing, disrupting, and prosecuting cybercrimes, State Department's lead in working with foreign countries, and other lead federal agencies, as appropriate and engage the Cyber Threat Intelligence Integration Center (CTIIC) for intelligence support and related activities.

Accordingly, when requested or directed, DoD may provide support to Federal, State, and local authorities. The CPTs are the Department's leading forces to hunt for adversaries on DoD networks and systems. Aligned to support a variety of systems and networks, including industrial control systems and other cyber-enabled Platform Information Technology, the 68 CPTs in the CMF represent a significant capability to defend systems enabled by cyberspace. Although these forces are focused on DoD networks, systems, and information, select teams could be directed to provide additional capacity or capability to our federal partners providing support to industry in the event of malicious cyber activity against or a cyberattack on U.S. critical infrastructure.

Additionally, DoD is developing significant cyber capability and capacity within the Reserve Component, including the National Guard. The Air National Guard is developing 12 Air National Guard Squadrons to provide two full-time CPTs to the CMF; the Army National Guard has established the first of 11 CPTs which will be built out through 2020. The U.S. Army Reserve will follow by establishing 10 teams of its own. All of these teams are likely to further benefit from strong relationships with State and local authorities. To strengthen these relationships and support preparedness, National Guard units coordinate, train, advise, and assist eligible organizations and activities outside DoD when incidental to military training in accordance with section 2012 of title 10, U.S. Code.

In conjunction with DHS, DoD also plays a leading role in protecting the critical infrastructure of the Defense Industrial Base (DIB), one of the 16 identified critical infrastructure sectors. Using voluntary and mandatory reporting requirements, the Department partners with DIB sector stakeholders to maintain a robust cybersecurity and information assurance program.

DoD recognizes its own reliance on cyber-enabled critical infrastructure to conduct its core missions. We are a member of this information technology ecosystem and quite frequently are a target of these cyberattacks. Accordingly, we are working with our U.S. domestic and foreign partners and allies, including DHS, to identify our cyber vulnerabilities through multi-level analysis at the platform, mission, and campaign plan level, with a particular focus on cross-cutting Platform-Information Technology enabled systems. This effort continues to develop. In addition to these external partnerships, the Department is leveraging its own risk management processes to ensure identifies, prioritizes, and mitigates the most impactful vulnerabilities to the critical infrastructure that is fundamental to DoD's ability to project power and protect the nation, our people, and our allies and partners.

Although roles and responsibilities are largely understood, there are still some seams and gaps that may affect efforts to protect critical infrastructure. As a result, DoD has a number of efforts to improve both our readiness and that of our interagency partners. For instance, we are continually refining policies and authorities to improve the speed and flexibility to provide support, and we organize and participate in exercises, such as CYBER GUARD, with a range of interagency, State, and local partners to improve our understanding of our planning to respond to threats or attacks on critical infrastructure. Although these arrangements are still being refined, it is also important to recognize that any significant realignment of roles and responsibilities will have opportunity costs, including absorptive capacity to build mission capability in a new area.

Before I wrap up, I want to discuss briefly two related topics that are important to U.S. Government efforts in cyberspace. First, DoD has participated in efforts led by our partners at the State Department regarding international norms of responsible Nation-State behavior in cyberspace. Through those efforts, the international community has generally affirmed that existing international law applies to State conduct in cyberspace, and many States, including the United States, have been engaged in efforts to identify additional voluntary, non-binding norms of responsible State behavior that apply to peacetime activities in cyberspace. These voluntary, non-binding norms are not arms control measures. Instead they collectively define behavior that would be considered unacceptable if conducted during peacetime and reflect expectations of responsible State behavior that are to apply to cyberspace activities, consistent with international law.

Second, no discussion of cyber threats would be complete without some discussion of deterrence. This subject has rightly been the focus of a lot of attention in recent years as we seek to calibrate the right mix of actions to deter malicious cyber activities effectively. In developing mature cyber capabilities and through the employment of our cyber forces, DoD seeks to deter malicious cyber activities by demonstrating our ability to deny our adversaries any advantage in cyberspace, to impose costs, and to signal our resolve to defend our national interests and objectives. However, DoD is only one part of a comprehensive, whole of government cyber deterrence strategy involving other Departments and Agencies. Successful deterrence depends on the totality and unity of U.S. actions, including threat and asset response procedures, declaratory policy, effective response procedures, timely indications and warnings, the resiliency of U.S. networks and systems, and availability of effective resources and options to respond. We welcome the recent Defense Science Board report on the subject and will explore those recommendations that are not already being implemented in cooperation with our interagency partners.

In conclusion, the Department of Defense is committed to defending the nation and is prepared to defend its critical infrastructure from malicious cyber activities and attacks of significant consequences that may occur in or through cyberspace. It has undertaken comprehensive efforts, both unilaterally and in concert with interagency partners, allies and partners, and the private sector to improve our Nation's cybersecurity posture and to ensure that DoD has the ability to operate in any environment at any time. Our relationship with Congress is absolutely critical to everything the Department is doing. To that end, I am grateful for the Subcommittee's interest in these issues, and I look forward to your questions.