STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY

AND PRINCIPAL CYBER ADVISOR

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

MARCH 4, 2020

Thank you Chairman Langevin, Ranking Member Stefanik, and Members of the Committee. I am pleased to be here with General Nakasone, Commander of U.S. Cyber Command (USCYBERCOM), to report on the progress the Department of Defense (DoD) has made implementing the 2018 DoD Cyber Strategy and achieving the Department's objectives in cyberspace. This afternoon, I am testifying in both my roles as Assistant Secretary of Defense for Homeland Defense and Global Security, and as Principal Cyber Advisor (PCA) to the Secretary of Defense. I am responsible for advising the Secretary and the Deputy Secretary on cyberspace activities and the development and implementation of the Department's cyber strategy and cyberspace policy; leading our interagency partnerships and coordination of our whole-of-government cyber efforts; engaging with our allies and partners; and ensuring the integration of cyber capabilities across the Joint Force in support of the President and Secretary of Defense.

Strategic Context

To start, I would like to offer our perspective on the current threat environment. As our National Defense Strategy (NDS) makes clear, we are in a renewed era of great power competition. Strategic competitors such as Russia and China are asserting their military and non-military power to challenge the rules-based international order. Although our military superiority has deterred conventional aggression against the United States, states such as China, Russia, North Korea, and Iran are increasingly taking actions in the gray zone below the threshold of the use of force to undermine our security. There is perhaps no area where this is more true than in cyberspace.

For more than a decade, our competitors have taken actions in and through cyberspace to harm the United States, our allies and partners, and the international order. Our competitors are conducting long-term, coordinated campaigns of malicious activity to gain political, economic, information, and military advantage. Their objective is to "win without war," and, in the event of a conflict, to leverage accesses and capabilities developed prior to hostilities to achieve decisive military advantage.

The Intelligence Community (IC) assesses that China, Russia, Iran, and North Korea are using, and will continue to use, cyber capabilities to steal information, to influence our citizens, to undermine democratic institutions, and to prepare to disrupt critical infrastructure that our national security depends on.

China remains a persistent and growing threat to the United States in cyberspace. As Secretary Esper said at the Munich Security Conference in February 2020, China is seeking to gain an advantage over the United States by any means, at any cost, including by exerting its growing power in ways that are threatening, coercive, and counter to the rules-based international order. China's growth has been fueled by theft, coercion, and the exploitation of free market economies, private companies, and academia. These activities are enabled by China’s cyber capabilities, as we saw from the Justice Department’s (DOJ’s) recent indictment of four members of the PLA for hacking Equifax to steal valuable trade secrets and the personal data of Americans. The IC also assesses that China maintains the ability to use its cyber capabilities to cause localized, temporary, and disruptive effects on critical infrastructure inside the United States.

Russia continues to be a highly sophisticated and capable adversary, integrating cyber espionage, attack, and influence operations in mutually reinforcing ways to achieve political, economic, and military objectives. The IC assesses that Russia is pre-posturing capabilities that could disrupt or damage U.S. civilian and military infrastructure before or during a crisis. We have already seen Russia conduct such attacks against our allies and partners, including the October 28, 2019, attack against the Republic of Georgia that disrupted thousands of websites and at least two major television stations.

Although China and Russia remain our two primary strategic competitors, the threats to the United States in cyberspace include a diverse set of additional actors. Iran and North Korea are employing their cyber capabilities to conduct espionage, and they remain a threat to public and private U.S. critical infrastructure. Terrorists and violent extremists continue to leverage the digital domain to advance their agenda. And the growing availability and use of publicly and commercially available cyber tools is increasing the overall volume of unattributed cyber activity around the world.

The digital domain also enables campaigns of malicious foreign influence with the goal of shaping our alliances and partnerships, policy outcomes, and, most significantly, undermining our democratic institutions. As you have frequently heard from our IC colleagues, threats to U.S. elections this year could be broader and more diverse than before, as more nations and other actors attempt to interfere with U.S. institutions and society by targeting social media and elections infrastructure.

It is in this context of determined, rapidly maturing adversaries that the 2018 DoD Cyber Strategy called for a more proactive approach to competing in the domain. We can no longer allow our strategic competitors to flout norms of responsible state behavior in cyberspace while claiming to be responsible actors. The DoD Cyber Strategy normalizes the Department’s activities in cyberspace by directing the Joint Force to integrate cyber operations fully into military operations. The Cyber Strategy also makes clear that the Department’s focus in cyberspace, like in other domains, is to prevent or mitigate threats before they harm U.S. national interests. The Department will “defend forward” in cyberspace in the same way we operate outside our borders on land, in the air, at sea, and in space to understand and defeat threats before they reach the United States.

The Department defends forward by conducting operations that range from collecting information about hostile cyber actors, to exposing malicious cyber activities and associated infrastructure publicly, to directly disrupting malicious cyber actors. In order to be successful, we must be in malicious cyber actors' networks and systems and continually refresh our accesses, capabilities, and intelligence. Defending forward simultaneously puts "sand in the gears" of the offensive operations of malicious cyber actors, and generates the insights that enable our interagency, industry, and international partners to strengthen their resilience, address vulnerabilities, and defend critical networks and systems.

Finally, cyber – unlike many other domains – is a field where people are the real capability. As the first inaugural President's Cup Cybersecurity Competition proved, the nation's best cyber defenders are in uniform. I took particular note of the fact that out of thousands of competitors, our nation's best individual cyber professional is a Cadet First Class at the Air Force Academy. The Department remains committed to using the authorities granted to it by Congress – including new pays, promotions, and commissioning tools – to grow an experienced cyber cadre of talented professionals capable of tackling the world's hardest digital tasks.

The Department values its partnership with Congress, which has ensured that we have the authorities and policies in place governing cyberspace operations to enable our strategic approach to compete and prevail in the cyber domain. This includes, as provided in the National Defense Authorization Act for Fiscal Year 2019 (NDAA for FY 2019), both the affirmation of the President's authority to counter active, systemic, and ongoing campaigns in cyberspace by our adversaries against the Government and the people of the United States (Section 1642) and the clarification that certain cyber operations and activities are traditional military activities (Section 1632).

Implementation of the DoD Cyber Strategy: Overview of Progress To-date

The DoD Cyber Strategy set out five core objectives for the Department in cyberspace. These objectives are: (1) Ensuring that the Joint Force can achieve its missions in a contested cyberspace environment; (2) Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages; (3) Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident; (4) Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and (5) Expanding DoD cyber cooperation with interagency, industry, and international partners.

We have taken major strides toward being able to achieve these objectives. However, much work remains ahead of us. In particular, we have devoted substantial attention to three areas.

First, we are maturing the nine lines of effort identified in the strategy. These lines of effort include objectives such as: empowering timely, integrated cyberspace operations; modernizing networks and systems; protecting the Defense Industrial Base (DIB); enabling allies and partners; workforce development; and deterrence and mission assurance. Achieving these objectives requires a Department-wide effort to translate relatively broad strategic guidance into specific objectives, tasks, and subtasks that are focused on outcomes. Integral to this effort is the ability to measure results clearly and objectively so that we can assess outcomes. We are not only refining end-states, but also developing project plans, tasks, and measures of effectiveness and performance so that we can continually monitor and evaluate our progress.

Second, we are directing funds to priority areas to address critical gaps identified in the congressionally directed Cyber Posture Review. For example, the FY 2021 budget request includes increased resources for modernizing networks and systems through investments in cross-domain solutions, next-generation encryption development and deployment, and network modernization technologies, such as “Comply to Connect” and “Automated Continuous Endpoint Monitoring.”

Third, we have focused on building and employing a cross-functional team of experts, in the Office of the Principal Cyber Advisor (OPCA), to manage actively the implementation of the process across the entire DoD enterprise. The Department has augmented the expertise and capacity of OPCA, allowing closer collaboration with Principal Staff Assistants on key issues, and enabling assessment to inform and advocate for DoD Cyber Strategy implementation throughout the Department.

Although we still have a long way to go, the Department's focused effort on strategy implementation has delivered some important achievements in the past year. Some quick highlights include:

- Initiating the first DoD-wide effort to achieve enterprise-wide visibility at the operating system level and to enable automated federating reporting using common software tools. The standardized use of this tool across the enterprise allows Joint Forces Headquarters Department of Defense Information Network (JFHQ-DoDIN) to visualize and defend the network more effectively.
- Defining what constitutes the Department's Cyberspace Operating Force and finalizing readiness standards for the Cyber Mission Force that will allow the Department to measure readiness accurately across the Services.

- Working closely with other U.S. departments and agencies and the Cyberspace Solarium Commission to mature the concept of layered deterrence. Layered cyber deterrence combines traditional deterrence mechanisms and extends them beyond the Federal Government to develop a whole-of-society approach. It also incorporates the concept of defending forward to address the range of malicious cyber activity that the United States has thus far been unable to deter.

Putting Our New Cyberspace Authorities Into Practice

Our new, proactive approach to competition in cyberspace is enabled by new Presidential policy on cyberspace operations, as well as by legislation, including the NDAA for FY 2019, which complements and strengthens the Department's authorities. Taken together, these changes have advanced and modernized the Department's ability to operate in cyberspace, resulting in transparent, well-coordinated, timely operations.

These new policies and authorities have been instrumental in enabling the Department's efforts in support of protecting the integrity of U.S. elections, both in 2020 and looking to the future. My guidance from the Secretary is clear: defending U.S. elections is an enduring mission of the Department of Defense. To that end, we are supporting a whole-of-government effort to defend the 2020 U.S. elections. The Department, principally through U.S. Cyber Command's and

NSA's Election Security Group, is complementing the work of other Federal departments and agencies by leveraging DoD's unique capabilities and capacity and our proactive approach to defend forward. We are countering interference and covert foreign influence against our elections by:

(1) Generating insights to understand adversary activity;

(2) Enabling domestic partner departments and agencies, for example, by sharing indications and warning of indicators of compromise or threat activity with the Department of Homeland Security (DHS) to help them better protect our systems and providing information to the FBI to help expose covert influence online; and

(3) Conducting cyber operations to disrupt, degrade, or defeat malicious cyber activity.

The November 5, 2019, Joint Statement on Ensuring Security of the 2020 Elections released by the Attorney General, Secretary of Defense, Acting Secretary of Homeland Security, Acting Director of National Intelligence, and others, highlights the threat to our elections posed by Russia, China, and Iran. The expansion of the Department's cyberspace authorities is a recognition of the changing cyber threat landscape and the need to position DoD to support whole-of-government efforts by enabling a more proactive and assertive approach during day-to-day competition to deter, disrupt, and defeat foreign cyber campaigns. The

Department, through USCYBERCOM, the National Security Agency (NSA), U.S. Indo-Pacific Command, U.S. Northern Command, and the National Guard Bureau, is poised to support and complement the efforts of DHS and FBI in protecting U.S. elections.

Defending Forward in cyberspace is not limited, however, to defending U.S. elections. Through outstanding cooperation with our interagency partners and the National Security Council staff, the Department is able to conduct the full range of missions articulated in the NDS and DoD Cyber Strategy. Accordingly, our cyber forces are increasingly engaged in cyberspace to promote stability and security and to defend the United States.

Empowered with the necessary authorities, a new strategy, and increasingly close collaboration with our interagency and international partners, we are developing innovative concepts of operation. For example, the Cyber National Mission Force executes “hunt forward” operations involving the deployment of defensive cyber teams globally at the invitation of allies and partners to look for malicious cyber activity. Upon discovering malicious software, one option Cyber Command has employed successfully is to publicly expose malicious signatures to the cybersecurity community, allowing organizations and individuals around the world to mitigate identified vulnerabilities, thereby degrading the efficacy of malicious tools and campaigns.

Progress of DoD Partnerships Across the Federal Government and With the Private Sector

Our interagency, international, and private sector partners are key to ensuring that the Department can achieve its objectives in cyberspace. The increasingly provocative activities of key competitors, such as the NotPetya cyber operation conducted by Russia in February 2018, demonstrate how vulnerable the Department is to attacks against the many non-DoD-owned assets that are nevertheless critical to our ability to execute our missions. These assets include civilian ports, airfields, energy systems, and other critical infrastructure. Vulnerabilities in these areas will likely be targeted by our adversaries to disrupt military command and control, financial operations, the functioning of operationally critical contractors, logistics operations, and military power projection, all without ever targeting the comparatively well-protected DoD Information Network. Any large-scale disruption or degradation of national critical infrastructure represents a significant national security threat.

To address these challenges, the DoD Cyber Strategy directs DoD to strengthen alliances and attract new partners to ensure that we are taking a whole-of-society approach and to enable better security and resilience of key assets. In the past year, we have made some notable progress to enable DoD missions through both domestic and international partnerships.

For example, to enable collaboration and unity of effort between DoD and DHS concerning critical infrastructure and defense-critical assets, we have focused on maturing processes and procedures for cooperation and information sharing and for enabling operational collaboration. Under this framework, which stemmed from a 2018 Secretary of Defense-Secretary of Homeland Security memorandum, DoD:

- Established an Executive Steering Group (ESG) to coordinate DoD-DHS collaboration for the protection of critical infrastructure from cyber threats;
- Carried out combined public-private training events with DHS and private sector entities to enable DoD cyber forces to understand more fully the domestic critical infrastructure that they may be called upon to defend;
- Collaborated with DHS to exchange cyber threat information with private sector entities to enable the Department to understand more fully adversary cyber tactics, techniques, and procedures;
- Exercised with DHS to refine our respective roles and procedures during a cyber incident; and
- Conducted combined planning to ensure that, if DHS requests DoD support in a crisis, DoD cyber forces would be prepared to augment DHS's cyber incident response elements.

Additionally, we are finalizing a Memorandum of Agreement between DHS and DoD to implement Section 1650 of the NDAA for FY 2019, which authorizes DoD to provide DHS with as many as 50 cybersecurity technical personnel, on a non-reimbursable basis, to enhance cybersecurity cooperation, collaboration, and unity-of-government efforts. This enhanced collaboration under Section 1650 is an example of what can be achieved when the Legislative and Executive Branches make common cause.

Although individually none of these engagements itself represents a strategic change to the Nation's posture in cyberspace, they together reflect a new pattern of systematic collaboration and engagement among DoD, DHS, and our critical infrastructure partners. Such engagements, sustained over time, are helping to build a united approach that strengthens our national ability to prevent, respond to, and mitigate complex cyber threats.

With international partners, DoD is driving new approaches to expand and strengthen traditional security cooperation tools in support of these important relationships. In 2019, the Secretary of Defense issued new International Cyberspace Security Cooperation Guidance to clarify priorities for addressing cyberspace threats through building the capacities of our international partners and refining responsibilities among DoD components. The guidance directs how DoD components will collaboratively pursue the objectives of the National Defense

Strategy, the National Cyber Strategy, and the DoD Cyber Strategy, as they apply to security cooperation in cyberspace.

In parallel with development of the new Security Cooperation Guidance, DoD has been leveraging 10 U.S. Code Section 333 Building Partner Capacity resources in advancing security cooperation in the cyber domain with our international partners. It is our aim over the coming year, in furtherance of the DoD Cyber Strategy and with the continuing support of Congress, to build on our existing cyber-related capacity-building engagements overseas and to expand DoD cyber cooperation with international partners.

The Department also continues to work alongside its interagency and international partners, in bilateral and multilateral engagements, to promote international norms for responsible state behavior in cyberspace. Doing so helps to set expectations for state behavior and makes it easier to recognize when malicious state actors engage in behavior outside those boundaries. The Department actively supports the Department of State in the United Nations Open-Ended Working Group as well as in the Group of Governmental Experts, both of which are tasked to look at how international law applies in cyberspace and what are appropriate standards of responsible state behavior.

The Department must also ensure that our allies and partners are aware of the national security risks that result from relying on vendors that lack good security practices or that can be unduly influenced by state or non-state actors. We work closely with our allies and partners to illustrate the total costs of ownership of subsidized networks, such as those offered by Huawei, as well as the long-term impact on their security and economic competitiveness. The Administration has made it a priority to communicate the security threats presented by manufacturers of concern to our partners, particularly where it stands to impact our bilateral cooperation and information sharing.

The Future: Budget Overview

The FY 2021 President's Budget is designed to build on the progress we made last year towards implementing the 2018 DoD Cyber Strategy by enhancing our defensive and offensive capabilities. The Department's request of $9.8 billion for the Cyberspace Activities budget represents an increase in cyberspace funding of $0.2 billion compared to the FY 2020 budget request. These enhancements will reduce risk to DoD networks and to systems and information, and they will continue to grow our warfighting capabilities.

Conclusion

Thank you once again for the opportunity to appear before you today. With the 2018 National and DoD Cyber Strategies in place, we are confident that the Department has the right policy, guidance, and funding levels to support the defense of our Nation in cyberspace. The Department has made tremendous strides towards achieving our national objectives in cyberspace since I last appeared before this Subcommittee a year ago. Cooperation across the Executive Branch and with our private sector and international partners has reached new heights, we have begun to use our expanded authorities to enable our mission to defend forward, and, through the efforts of the OPCA, we continuously aim to ensure that the elements necessary for the success of the overall strategy are properly aligned. Although challenges lie ahead, I look forward to working with you and our critical stakeholders inside and outside the U.S. Government to ensure that the U.S. military continues to compete, deter, and win in cyberspace.