Opening Statement
Chairman James R. Langevin
Intelligence, Emerging Threats and Capabilities Subcommittee
FY 2020 Budget Request for Military Operations in Cyberspace
March 13, 2019

Video link to HASC Intelligence, Emerging Threats and Capabilities Subcommittee Chairman Langevin opening remarks here: https://armedservices.house.gov/hearings?ID=C1F7C8E4-3C1C-4FBA-B71D-8468DAD41165

Technology and the Internet have fundamentally changed how citizens, the nation, the military, our adversaries, and the world operate. We have more access to information and lower barriers to conduct commerce. We collectively benefit from the opportunities afforded by the technology we incorporate into our lives. However, the connections that we rely on also create vulnerabilities and new potential avenues for our adversaries to exploit at our nation's expense. "Cyber," as we understand it in government, will be always be something that creates risk to go along with its great.

The issues that stem from our increasing dependence on technology will never be purely military, or solely for the military to solve. Technology has increased the interconnectedness of our society, and the problems that have come with it will only be solved with interconnected, interdisciplinary approaches. The Department will have to work in new ways with stakeholders from agencies as varied as the Department of Commerce and Department of Education and with non-governmental stakeholders such as private industry and academia.

The Executive Branch will have to work diligently to address and solve the cyber challenges facing the nation. Yet this Administration has taken actions that call into question the seriousness with which it views this emerging domain. Most

notably, the Administration eliminated the Senior Cyber Coordinator position at the National Security Council.

Relatedly, there are several documents pertaining to cyber that Congress has repeatedly requested from the Administration and has yet to receive. This includes recent guidance pertaining to operations in cyberspace. Such documents are imperative to creating a congressional framework for oversight. Withholding these critical documents from Congress impacts our ability to appropriately support the command and may have far reaching consequences in the National Defense Authorization Act.

At the cabinet level, the Department of Defense (DoD) and U.S. Cyber Command (CYBERCOM) have no shortage of challenges in front of them, issues that often develop and change as fast as the technological landscape changes. Today, we will hear about some of those challenges including personnel recruitment and retention, as well as efforts to protect critical infrastructure in tandem with domestically oriented departments and agencies.

The Cyber Mission Force achieved full operational capability (FOC) last year. This was a notable event, but it would be a mistake to assume that FOC is synonymous with readiness. We must begin to examine the differing standards by which the Services are training their teams, and whether CYBERCOM is adequately fulfilling its mandate to set training standards and ensure compliance.

Readiness is especially important in the context of the current strategic landscape, which has evolved significantly over the last year. In the fall, the DoD released a new cyber strategy that articulated the intent to “defend forward” and operate across the full spectrum of conflict through persistent engagement. DoD

also completed the inaugural Cyber Posture Review. Under the auspices of new guidance from the Administration and the new DoD strategy, CYBERCOM played a crucial role in defending the 2018 elections from interference.

The military's actions in cyberspace were also enabled by multiple provisions in the Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA). This includes a provision recognizing activities conducted in cyberspace as traditional military activities.

The FY19 NDAA also allowed the National Command Authority to take direct and proportional action in cyberspace against Russia, China, North Korea, and Iran upon determination of a cyberattack against the homeland or U.S. citizens. Congress and this Subcommittee will continue to support military operations and provide the legal authorities to enable CYBERCOM's success against adversaries in cyberspace. However, we will also remain judicious in our oversight responsibilities to ensure that the Department operates in a manner that enhances stability in cyberspace and that is consistent with both Congressional intent and American values.

I commend CYBERCOM for its efforts during the 2018 elections. However, as a nation, we can never rest on our laurels. We need to examine the strategic impacts that CYBERCOM operations, and other whole-of-government efforts, had on actors seeking to interfere in our elections. Much like the traditional battlefield, we must *measure* the impact of our operations to assess our warfighting effectiveness towards the larger objectives and ensure our strategic vision reflects the realities of engagement in cyberspace.

CYBERCOM's ability to execute its operations is closely tied to and enabled by its partnership with the National Security Agency (NSA). These organizations will always have a robust partnership given the dynamism of cyberspace and NSA's deep expertise and enabling role in military cyberspace operations.

At this time, there is still one individual that leads both of these organizations. This arrangement is quite unique within the national security establishment and the intelligence community. However, this arrangement allows for the CMF to mature, enables better synchronization of cyberspace operations, and permits proper consideration of the intelligence and military objectives in the domain.

Before any significant changes are implemented in the dual-hat arrangement, this Subcommittee expects a robust understanding of how and why it is necessary to split the leadership function of NSA Director and CYBERCOM Commander. I believe it would be premature to split these organizations in the immediate future.

CYBERCOM is a maturing organization, and I am proud of the work we have done on this subcommittee to support its maturation. I have often said that we will never again see warfare without a cyber component, so CYBERCOM's continued development will remain an urgent priority. But it is therefore important that we build for the long term with sustainable, scalable approaches to integrating cyber into DoD operations and into our whole-of-government approach to protecting our nation in cyberspace. This is no small task, especially given the newness of this domain. But working together, with full transparency, I

am confident we can head off problems early and ensure we reap the benefits of a free, open, interoperable and secure Internet.

Before closing, I'd like to introduce our two witnesses.

Mr. Kenneth Rapuano serves as both the Assistant Secretary of Defense for Homeland Defense and Global Security and as the Principal Cyber Advisor to the Secretary of Defense. Prior to returning to government service, Mr. Rapuano worked for Federally Funded Research and Development Corporations, focusing on issues related to homeland security, counterterrorism, and countering weapons of mass destruction. Mr. Rapuano served as Deputy Homeland Security Advisor in the George W. Bush Administration. He served 21 years on active duty and the reserve as a Marine Corps infantry and intelligence officer. Mr. Rapuano, welcome back.

General Paul Nakasone serves in three capacities concurrently: Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. Before his current role, he commanded U.S. Army Cyber Command, and has served as a career intelligence officer through his 32 years in uniform. This is General Nakasone's first appearance before the Subcommittee since assuming command of CYBERCOM. General Nakasone, we are pleased you are here with us today.