STATEMENT OF

GENERAL PAUL M. NAKASONE

COMMANDER

UNITED STATES CYBERSPACE COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON

INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

4 MARCH 2020

Chairman Langevin, Ranking Member Stefanik, and distinguished members of the Committee, I am honored to appear before you today to discuss the accomplishments of United States Cyber Command (USCYBERCOM) over the last year and to discuss its future. It has been ten years since the Department of Defense created Cyber Command and began investing in its success. Today, I want to reflect on three areas where Cyber Command offers a return on those investments in line with the priorities of the National Defense Strategy. Cyber Command:

1. Imposes tailored, non-kinetic costs on adversaries, contributing to the lethality of the armed forces;
2. Expands military-to-military relationships, contributing to more effective partnerships for the armed forces; and
3. Innovates to address hard internal problems, reforming our business practices.

These returns on the nation's investment in Cyber Command are made possible by a professional force of soldiers, sailors, airmen, marines, civilians, and contractors. It is a force whose readiness continues to improve.

USCYBERCOM performs three main missions: it defends the military's networks, it supports the broader joint force with cyber operations, and it defends the nation from significant cyber attacks. It executes an FY20 budget of $596 million and has requested a budget of $638 million for FY21. Its full-time personnel total 1,778 military and civilians, plus contractors. In January 2020, we rostered 5,094 active duty service members and civilians in the Cyber Mission Force (CMF).

A decade ago, we trained and postured our cyber forces like any other military force: to prevail in future conflict. A central challenge today is that our adversaries compete below the threshold of armed conflict, without triggering the hostilities for which DoD has traditionally prepared. That short-of-war competition features cyber and information operations employed by nations in ways that bypass America's conventional military strengths.

The Chinese Communist Party (CCP) use of political repression and economic coercion – particularly through forced tech transfers and state-sponsored commercial espionage – harms U.S. interests and undermines the sovereignty of our allies and partners. Russia's efforts to undermine western institutions and to intimidate its neighbors have showcased its willingness to launch destructive cyber operations and pervasive influence campaigns. The latter remains the top concern when it comes to the 2020 elections, a topic to which I will shortly return. Iran has conducted disruptive cyber attacks against U.S. companies and partners, and employs similar tactics, along with information operations, to push its own narratives across the Middle East. North Korea uses cyber operations to steal currency that it would otherwise be denied under international sanctions. Violent extremist organizations also have used the Internet to command and control forces, to recruit, and to spread terrorist propaganda.

In 2018, "defend forward" became the cornerstone of DoD's cyber strategy to deal with the threats I've just described. It set an important tone for the joint force, stressing just how serious these threats have become to the military, and to encourage disrupting these threats before they harm the nation. This strategic direction drives Cyber Command's doctrine called persistent engagement: it enables partners with unique insights, and it stands ready to act by imposing costs when authorized.

Cyber Command imposes tailored, non-kinetic costs on adversaries, contributing to the lethality of the armed forces.

Cyber Command contributes to the broader joint force's ability to impose costs through hunt forward missions, offensive cyber operations, and information operations. First, I will describe how cost imposition fits in to our support to the whole-of-government effort to protect the 2020 elections. Second, I will describe how Cyber Command increases the lethality of other combatant commands. Third, I will explain how Cyber Command's defensive cyber operations improve the resilience of the military's networks, which forces adversaries to expend resources for diminishing returns.

Defend the Nation and Election Security

Today, we are 244 days from the 2020 Presidential election. Last year, we institutionalized our efforts from the Russia Small Group before the 2018 elections into an enduring Election Security Group for 2020 and beyond. The group reports directly to me and is led by representatives from Cyber Command and the National Security Agency. Its objectives are to generate insights that lead to improved defenses and being prepared, if ordered, to impose costs on those who seek to interfere. To be sure, we place a high priority on collecting and sharing information with our partners at DHS and FBI to enable their efforts as part of a whole-of-government approach to election security. But Cyber Command's authorities mean that it must also be prepared to act.

In 2018, these actions helped disrupt plans to undermine our elections. During multiple hunt forward missions, Cyber Command personnel were invited by other nations to look for adversary malware and other indicators of compromise on their networks. Our personnel not

only used that information to generate insights about the tradecraft of our adversaries, but also to enable the defenses of both our foreign and domestic partners. And by disclosing that information publicly to private-sector cybersecurity providers, they took proactive defensive action that degraded the effectiveness of adversary malware.

Cyber Command also executed offensive cyber and information operations. Each featured thorough planning and risk assessments of escalation and other equities. Each was coordinated across the interagency. And each was skillfully executed by our professional forces. Collectively, they imposed costs by disrupting those planning to undermine the integrity of the 2018 midterm elections.

Cyber Command's contributions to broader government efforts to protect elections are part of its mission to defend the nation in cyberspace. To defend the nation from this and other kinds of malicious cyber activity, persistent engagement with our adversaries allows Cyber Command to generate new insights that drive new methods of defense, and inform future options to impose cost. This approach drives the Election Security Group's approach to the 2020 elections, ensuring that exquisite intelligence drives tailored operations, which in turn generate more insight and opportunities to harden defenses and impose costs if necessary.

Support to Combatant Commanders

While persistent engagement drives Cyber Command's defense of the nation in cyberspace, the command simultaneously works with my 10 fellow Combatant Commanders to support and enable their efforts as part of the joint force. That support improves the defenses of their portions of DoD's networks and makes each command more lethal in its missions. Our

new Cyber Operations-Integrated Planning Elements (CO-IPEs) allow for greater integration into each command's operations.

As an example of how Cyber Command supports other joint force commanders, consider the support Cyber Command provides to U.S. Special Operations Command. The Marine Corps is the service that supports SOCOM, so MARFORCYBER provides the team of uniformed and civilian personnel that comprise the CO-IPE at SOCOM. The team's presence at MacDill Air Force Base and other SOCOM locations allows it to understand and facilitate SOCOM's dynamic requirements for cyber support to accomplish its missions. The CO-IPE also offers lessons learned and new options to SOCOM planners based on insights from fellow CO-IPEs at other commands.

To extend this example to the battlefield, MARFORCYBER's Joint Task Force-ARES has imposed costs on violent extremists online to support the overall counter-terrorist mission. ISIS is now mostly confined to publishing text-only products, instead of their previous, gruesome multi-media products. These products used to be disseminated in multiple languages through mass-market platforms. Now, ISIS struggles to publish in non-Arabic languages and is confined to less-traditional messaging applications. Of course, the collapse of the physical caliphate made it harder for ISIS to operate online. But Cyber Command's efforts through JTF-ARES remains important to contesting ISIS's attempts at establishing a virtual caliphate as well.

For years, Cyber Command has supported Central Command objectives in Iraq and Afghanistan, especially with information operations to protect U.S. and allied forces. As the entirety of the Department of Defense reorients around the 2+3 construct, so too have our efforts to provide cyber support.

Defensive Cyber Operations and Resilience

A third way Cyber Command imposes costs on adversaries is by improving the resilience of military networks. By taking preventive measures, we try to limit the incidence of network compromises. By being more rapid with our incident response, we aim to detect, quarantine, and expel intruders in as short a time as possible. By expediting network reconstitution, we can restore functionality to return the force to mission faster. By making the DODIN harder to compromise, and by reducing the operational impact of compromises, our networks are becoming more resilient. This imposes a cost on adversaries because they must expend greater resources, only to reap diminishing returns. My priority for defense in 2020 is to emphasize a command-centric model so that our network defenders are threat informed and our leaders are accountable for the security of the networks they operate.

Cyber Command expands military-to-military relationships, contributing to more effective partnerships for the armed forces.

So much of Cyber Command's success reflects and informs close partnerships it has built across the U.S. government and with industry and academia. Over the last year, I have placed a particular emphasis on expanding military-to-military partnerships. In part, this is because such partnerships are critical to the joint force as a whole. However, the return of great-power competition, and how that competition manifests in cyberspace, makes it all the more prudent to work with our allies on activities that promote collective security.

Just as the partnerships with the United Kingdom, Australia, Canada, and New Zealand anchor NSA's foreign engagement, so too do relationships with several of these countries form

the bedrock of Cyber Command's international partnerships. But Cyber Command has a more expansive partnership agenda, starting in the Pacific. Many nations there have grown increasingly concerned by the malicious cyber activity they have encountered. Last year, I had the honor of visiting my counterparts in Japan and South Korea. Each is making impressive strides towards growing the capability to better protect their networks from cyber intrusions and compromise. Our militaries have important shared equities, so improving common network defense, expanding combined training, and sharing lessons and vulnerability information is of mutual benefit.

It has been heartening to see the maturation of how our partners in Europe are organizing for cyber defense. Cyber attacks in Europe have been a concern for over a decade. In October, I met with 30 of my counterparts for consultations and presentations. We discussed education, mission planning, training, exercising, and operations. I was impressed to see the importance they placed on thinking through the long-term investments required to build professional forces, capable of making material contributions to combined cyber operations.

What is also clear is that in cyberspace, just because a partner is located in one theater of the world does not mean the value it brings to a partnership is limited to that theater. Our adversaries have aspirations for influence and control that transcend geographic boundaries. So too must the utility of our partnerships. A partner in the Pacific, for example, might be ideal to work with to counter a threat in the Middle East. Indeed, this logic informs an initiative Cyber Command undertook with Southern Command last year to improve the cyber capacity of several South American partner militaries. In August of 2019, our forces built a network in country to simulate and test defensive tactics. This kind of capacity building is also augmented by the National Guard's State Partnership Program. The partnership between the Maryland Guard and

Estonia, for example, allows for longer-term relationships to be formed, which builds greater familiarity with the partner's infrastructure. With that familiarity comes trust and experience, which leads to tailored exercises that inform more actionable lessons learned.

The global connectivity that the Internet powers therefore creates new opportunities for military-to-military partnerships, and Cyber Command will be at the forefront of making those partnerships count for the joint force.

Cyber Command innovates to address hard internal problems, reforming our business practices.

Cyber Command has a special responsibility and opportunity to embrace innovative solutions to reform the way we do business. I'll discuss three of these efforts: the work enabled by a facility called Dreamport, our new Command Acquisition Executive, and our approach to capability development under the Joint Cyber Warfighting Architecture (JCWA).

Dreamport originated from Cyber Command's $4 million investment in a partnership with the Maryland Innovation and Security Institute (MISI), a non-profit organization. MISI operates Dreamport, as part of a 44,000-square foot unclassified collaboration venue. Having an unclassified space may not seem like much, but it is crucial to working with companies and other non-government entities like academics and researchers who lack the requisite clearances to work on the NSA campus. Many of our cybersecurity challenges are not unique to DoD: we can learn much through outside engagement, and Dreamport has brought that engagement to fruition.

Over the past 18 months, Dreamport has allowed the Command to engage more than 1,000 private companies, educate over 1,000 military personnel on innovative technologies, and involve more than 350 students and interns from 65 colleges and high schools on STEM initiatives. It has been home to Cyber Command's effort to begin implementing the principles of

zero-trust networking on the military's networks. Dreamport also hosted the public-private collaboration that resulted in kits that help enable the Cyber National Mission Force to conduct Hunt Forward operations. The traditional ways of doing business would have been too cumbersome and too slow. Dreamport is key to the command's ability to engage in public-private partnerships at the unclassified level.

If Dreamport provides the venue and the mechanism, then our Command Acquisition Executive (CAE) is our senior leader for those efforts. Last year, Cyber Command hired its first CAE, a member of the Senior Executive Service, to lead our team of innovators and capability developers. She executes her responsibilities under Cyber Command's acquisition authority to rapidly develop and deliver joint cyber capabilities. During FY19, the Command executed 81 contracting actions valued at $74.9M, staying within the $75M ceiling. The CAE is also establishing a JCWA integration office and is working with OSD and services to synchronize critical cyber capability development.

To enable our personnel to achieve their missions, Cyber Command works with the Services to develop the JCWA. It will allow Cyber Command to employ its forces to conduct offensive and defensive operations against common objectives regardless of service and physical location. To do so, Cyber Command needs: sensors for situational awareness; a Unified Platform to manage, store, and analyze data; Joint Cyber Command and Control for mission planning and execution; tools for cyber operations; a Persistent Cyber Training Environment to train and rehearse missions; and a Joint Common Access Platform from which to perform operations.

For example, the Rapid Capability Development Network is one of the most promising platforms for tool development. It allows developers and operators to co-locate and produce,

test, and deploy capabilities. When paired with the Army's mission rehearsal environment, cyber mission teams can develop, test, and rehearse to ensure that the desired operational effects are available if and when a mission is authorized.

A Professional Military Cyber Force

None of what I have described thus far is possible without the professional forces under my command. With the Cyber Mission Force reaching Full Operational Capacity in 2018, Cyber Command headquarters, together with the service cyber components, are improving the CMF's readiness. Ensuring the force is ready, trained, and equipped to impose costs on our adversaries was my top priority last year. To that end, Cyber Command standardized readiness metrics across the services for Cyber Protection Teams, and is currently establishing standards for the Cyber Mission Teams and Cyber Support Teams. Additionally, the Command is working with the services to review the team structure to ensure that capability and capacity reflects the National Defense Strategy's prioritization of the 2+3 threat construct.

The return on investment the cyber force has brought over the last several years is a direct result of the accomplishments of the talented cyber workforce provided by the services. Talent management is key. We have learned that financial incentives retain people, but not necessarily the most talented people. Keeping the best of the best focused on the hardest but most rewarding aspects of our unique missions is one of our best retention tools. Over the coming year we will engage the services to continue building a manpower model to support retaining the most talented professionals.

One of the most impactful components of that manpower model is the reserve component. Like in other domains of warfare, forces in the reserve component can augment active duty forces for Title 10 missions. Members of the Air National Guard augment a full time National Mission Team and two Cyber Protection Teams. The Army National Guard mobilizes over 150 cyber personnel to defend Army infrastructure as Task Force Echo. For additional cyber capacity, the Army is building 21 Cyber Protection Teams across the Reserve and Guard. The Air Force Reserve and Navy Reserve provide additional augmentation to active duty Cyber Protection Teams and Combat Support Teams. Their value to the nation is increased by the leadership and experience of so many of these individuals in the private sector. Since over 80% of critical infrastructure is in the private sector, members of the guard and reserve are a valuable source to bridge the knowledge between the government and private sector. There is much experience to be shared between the C-suite and the command suite.

The Cyber Excepted Service hiring authorities have helped the Command recruit skilled civilians with competitive compensation packages and faster hiring decisions. USCYBERCOM can now recruit talent directly at job fairs, which we have hosted at Fort Meade, Baltimore, San Antonio, and Silver Spring, Maryland. The Cyber Excepted Service has also led to shorter hiring timelines, allowing the Command to compete for talent by citing its nearly unique status as an employer in which personnel work as cyber warriors and perform or support full-spectrum cyberspace operations on behalf of the nation.

Distinguished members of the committee, I look forward to discussing these and other topics with you. Thank you again for inviting me, and especially for your support. I am happy to answer your questions.