POSTURE STATEMENT OF

GENERAL PAUL M. NAKASONE

COMMANDER, UNITED STATES CYBER COMMAND

BEFORE THE 117TH CONGRESS

SENATE ARMED SERVICES COMMITTEE

MARCH 25, 2021

Chairman Reed, Ranking Member Inhofe, and distinguished members of the Committee, I am honored to appear before you today and to represent the men and women of United States Cyber Command (USCYBERCOM). 2020 presented some unique challenges to USCYBERCOM that will inform our actions over the next year. Indeed, 2021 is offering opportunities for USCYBERCOM to build upon.

USCYBERCOM was established in 2010 and became a unified combatant command in 2018. Our mission is to plan and execute global cyberspace operations, activities, and missions to defend and advance national interests in collaboration with domestic and international partners across the full spectrum of competition and conflict. We direct, synchronize, and coordinate cyber planning and operations. Our three enduring lines of operation are as follows:

- Provide mission assurance for the Department of Defense (DoD) by directing the operation and defense of the Department of Defense Information Networks (i.e. the DoDIN) and its key terrain and capabilities;

- Defeat strategic threats to the United States and its national interests; and

- Assist Combatant Commanders to achieve their missions in and through cyberspace.

In January 2021, our Cyber Mission Force (CMF) comprised roughly 6,000 service members and civilians out of an authorized a total of 6,187 positions. This includes Guard and Reserve personnel on active duty serving at our headquarters and on our CMF teams. For comparison, the 2018 DoD *Cyber Posture Review* counted about 238,000 personnel in the Department's cyberspace operations forces, including the CMF, USCYBERCOM's subordinate command elements, cybersecurity service providers (CSSPs), special capability providers, and specialty units.

The DoD depends on USCYBERCOM and its performance. Every operational plan and every mission across the Department builds from the assumption that we will be able to assure that the bandwidth and data that military forces require will be accessible and trustworthy.

A Look Back at 2020

In 2020, USCYBERCOM made progress in the face of significant challenges. Operationally, we helped to lead the successful defense of the 2020 elections and played a key role in the Government-wide response to the SolarWinds breach. We also gained Departmental commitments to enhanced resources and a better alignment of cyberspace responsibilities and authorities for the Command (including the FY21 NDAA elimination of the $75 million cap on funds available for acquisition activities).

We saw increasingly capable cyber adversaries target the United States via influence operations, efforts to compromise sensitive data, and attempts to gain access to our weapons systems. Adversaries still seek to exploit gaps and seams between our organizations and authorities:

- China is a sophisticated cyber adversary. Beijing conducts effective cyber espionage and other operations and has integrated cyber activities into its military and national strategy. Despite public exposure and indictments of Chinese cyber actors, China remains focused on shaping the global narrative and exploiting American networks and cyber systems.

- Russia is a sophisticated cyber adversary. It has demonstrated its ability to conduct powerful influence campaigns utilizing the medium of social media. Moscow conducts effective cyber-espionage and other operations and has integrated cyber activities into its military and national strategy. Despite public exposure and indictments of Russian cyber actors, Russia remains focused on shaping the global narrative and exploiting American networks and cyber systems.

- North Korea has demonstrated the capability and intent to strike the United States in cyberspace. Its regime sponsors cyber exploitation of international finance via cyber means to evade United Nations sanctions.

- Iran has demonstrated both the capability and intent to strike the U.S. in cyberspace. Iranian cyber actors are growing adept at exploiting systems as well as delivering disruptive and destructive attacks, and have attempted to execute a series of influence campaigns.

- Finally, non-state actors and criminal cartels remain threats to us and our interests, whether by financing, recruiting, and advertising violent extremist tactics, or through the exploitation of data for theft or ransom.

All of these actors felt the effects of the COVID-19 pandemic – as did we. Fortunately, we saw their operational tempo briefly diminish at roughly the same time that we had to restrict access to our facilities. COVID-19 mitigations remain in full effect across our enterprise, and we are vaccinating our personnel as fast as vaccine supplies and local conditions allow. Overall, I am pleased that the pandemic has not limited the force's readiness or posture to fulfill its missions.

Last year, I emphasized the importance of defending the election against foreign interference, in part through the Election Security Group (ESG), a combined team from USCYBERCOM and the National Security Agency (NSA). The ESG ensured that intelligence informed whole-of-nation efforts to harden defenses and prevent or disrupt threats to the U.S. elections. We built on lessons from earlier operations and honed partnerships with the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), sharing information with those who needed it as fast as possible. We also worked with the National Guard Bureau to create a mechanism that enabled Guard units to share information about incidents quickly, easily, and uniformly. We called it the Cyber 9-line, given the nine lines of information a reporting entity would complete. As the election approached, every state had joined this program. I am proud of the work the Command and the ESG performed, as part of a broader government effort, to deliver a safe and secure 2020 election.

USCYBERCOM conducted more than two dozen operations to get ahead of foreign threats before they interfered with or influenced our elections in 2020. Three points stand out for me:

- First, USCYBERCOM must be ready and able to act. Threats can arise rapidly, and opportunities can be fleeting. Our ability to operate successfully in cyberspace is a function of streamlined processes, mission readiness, and the trust of our various mission partners.

- Second, USCYBERCOM's partnership with NSA remains the foundation of our success. Working together under one leader again demonstrated the ability of both organizations to operate with speed and agility to achieve outcomes for the nation.

- Third, we enable our foreign allies and partners, just as they remain crucial to our ability to act. Operating with allies and partners allows each to magnify each other's unique strengths. Our efforts over the last year highlight the value of not only operating but training together as well.

USCYBERCOM supported the combatant commands with a wide range of other operational accomplishments over the last year. Counterterrorism operations in cyberspace are continuous, helping to protect the force and prosecute targets in Afghanistan and other regions on behalf of USCENTCOM and USSOCOM. We are also shifting JTF-Ares' focus (though not all of its missions) from counterterrorism toward heightened support to great power competition, particularly in USINDOPACOM's area of responsibility. Finally, we are working across the board to ensure that the data links that our warfighters rely on are protected and resilient.

In recent months our priority has been mitigating the threat to federal systems from malicious cyber actors compromising widely-used SolarWinds software and exposing thousands of public and private systems to targeted exploitation. The U.S. government learned of the compromise in December 2020. As an immediate response to this threat, I directed the creation of a combined USCYBERCOM-NSA team in support of the U.S. government's efforts, through the Unified Coordination Group, to mitigate the compromise. To date, we have yet to identify any compromise of DoD information networks in the unclassified or classified domains.

My teams have provided almost 100 days of continuous support to the whole-of-government mitigation effort. I have organized our efforts across three lines of effort:

1. *Bound the Problem*. Using both automated and manual processes, we worked to determine the scope of SolarWinds Orion software products employed across the DoDIN. Each instance was immediately isolated and disconnected from DoD networks. Meanwhile, NSA worked to understand the adversary's intent and illuminate additional tradecraft and infrastructure to inform threat detection and asset response activities. Finally, we prepared to support and assist other federal departments and the Defense Industrial Base in bounding their respective problems.

2. *Expel the Adversary*. This is a continuous process driven by USCYBERCOM's Joint Force Headquarters-Department of Defense Information Networks (JFHQ-DoDIN), which has directed network administrators to enumerate, isolate, and remediate all affected systems before they are reconnected to the DoDIN. We have yet to find any adversary presence on the DoDIN as a result of the SolarWinds compromise. We continue to work with federal partners to share best practices and expertise to expel the adversary from affected systems.

3. *Impose Cost.* USCYBERCOM and NSA are both planning and informing the whole-of-government response options to the SolarWinds supply-chain compromise and the adversary's associated campaign. Policymakers are considering a range of options, including costs that might be imposed by other elements of our government.

The SolarWinds incident occurred because highly skilled, sophisticated actors inserted a malicious cyber capability into a commercial product that was then downloaded and installed world-wide. The nature of the tradecraft employed by this actor reinforces the imperative for government and industry to collaborate in detecting and responding to malicious cyber activity. We in the U.S. Government, together with our industry partners, must improve our defensive posture to prevent and minimize the impacts and the cost in time and money of remedying such vulnerabilities and incidents, and we must rapidly expose and respond to malicious cyber activity in the future.

Our Focus for 2021

My focus for the coming year is to broaden the foundation for operational progress. In particular, we are building on recent guidance from the Department, seeking to promote sustainable readiness; to improve training; and to attract and retain high-end talent across our military, civilian, active duty, and Reserve workforces.

Cybersecurity and defensive cyberspace operations mean mission assurance for the DoD and thus are integral to our nation's security. For 2021 and the years ahead, there are several areas where USCYBERCOM plans to improve. Our growth to date has highlighted certain misalignments between the responsibilities I have as Commander and the resources and authorities to execute those responsibilities. The following initiatives reflect the Department's guidance to align mission, responsibility, and accountability for the Command:

Accountability: The Secretary of Defense in late 2020 issued a directive emphasizing accountability by aligning cybersecurity efforts with operational risk decisions. USCYBERCOM will improve risk management while also holding commanders and directors accountable for their risk decisions.

Budget Control: USCYBERCOM's FY21 budget is roughly $605 million, which covers the headquarters staff and the Cyber National Mission Force. Meanwhile, 27 different components shape the Department's overall Cyber Activities Budget, which averages about $10 billion a year. USCYBERCOM is working with the Services and the Office of the Secretary of Defense

to direct CMF funding in a more collaborative effort while allowing for informed tradeoffs (across the Services) based on operational needs.

Team Realignment: The CMF's original force structure was set in 2012, and several teams were originally aligned to support the counter-terrorism fight. With the return of great power competition, USCYBERCOM is realigning some teams to focus on key nations.

Force Growth: Recent demand across DoD has demonstrated that the original 133 teams in the CMF are not enough. The strategic environment has changed since the original CMF was designated in 2012. Added forces will ensure USCYBERCOM can fulfill its responsibility as both a supported and a supporting command.

Training: USCYBERCOM is centralizing the provision of advanced training. The Army will serve as the executive agent for advanced cyberspace training. This will ensure that each Service presents well-trained personnel to USCYBERCOM who can contribute to our missions as soon as they arrive in the Command.

Sustainable Readiness: We are improving our ability to monitor the status of forces down to the team, mission element, and even individual levels in order to identify and remedy challenges to gaining and maintaining necessary readiness. We are working to better provide commanders with the situational awareness they require to assess risks and make informed decisions, not just in operations but also in maintaining the force as a whole. I am pleased with the progress here, but more needs to be done.

Domestic and International Partnerships: Such ties collectively are a force multiplier when it comes to cyber operations. USCYBERCOM is enhancing its existing relationships and forging new ones based on U.S. Government priorities. We have been sending teams to "hunt forward" at the invitation of foreign governments, helping them find adversary malware on their governmental systems. Such persistent engagement in cyberspace lets the Command deliver outcomes in competition with adversaries, both by enabling our partners and by acting when called upon.

Realigning Cyber Protection Teams: USCYBERCOM is working with the combatant commands to ensure they have dependable defensive support for their missions while we retain forces to deal with global challenges to the DoDIN.

USCYBERCOM executes its operations employing the Joint Cyber Warfighting Architecture (JCWA), which is a cyber capabilities architecture that enables us to act against our adversaries in competition, crisis, and conflict in cyberspace. When fully realized, JCWA will provide unified capabilities for Cyberspace Operations Forces, integrating the data from offensive and defensive cyberspace operations in ways that help commanders gauge risk, make timely decisions, and act.

To help drive operational needs and capability development, USCYBERCOM activated a JCWA Capability Management Office (JCMO). This promoted unity of effort across the

Command, the Services, and Department in building the many and varied components that together comprise the JCWA. Those components include:

- Improved operational architectures that give our forces the ability to operate at-scale from multiple locations;

- Data sharing and analytics (the Unified Platform) that provide insight for offensive and defensive operations;

- Command and control features that display the readiness of our forces as well as operational status. One tool in this suite, Project IKE (soon to be Joint Cyber Command and Control), has ensured we can measure readiness down to the individual level while informing exercises, training, recruiting, and even retention;

- Tool development capabilities that are responsive to operational needs and increasingly able to focus talents and innovations when and where they are needed most;

- Realistic collective training (via the Persistent Cyber Training Environment, or PCTE) that lets us rehearse missions and even exercise with Reserve Component and foreign partners.

Last year's operational successes would not have been possible without the Department's Total Force, which includes the National Guard and the Reserves. Before the 2020 elections, the Guard provided local connectivity and insight on key events like Super Tuesday. They also played vital roles during the pandemic. For example, the National Guard and Reserve provided cyber forces in response to a Defense Support to Civil Authorities (DSCA) request from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency in support of Operation Warp Speed, providing cybersecurity support to the pharmaceutical industry as it developed COVID-19 vaccines in record time.

Finally, the Reserve Component's ability to hire qualified cyber warriors who decide to leave active duty upon completion of their service commitment has proved invaluable. Members of the National Guard and Reserve have relevant private-sector experience in fields of strong interest to the Department, and many of them work for some of the nation's top-tier technology companies. The Air National Guard, for example, has built both offensive and defensive cyber units in which members departing active duty can transfer to part-time status while they pursue careers in the civilian sector.

As the trailblazer for the DoD's Cyber Excepted Service (CES) personnel authority, the Command benefits from flexible hiring authorities in filling civilian vacancies and recruiting top cyber talent. Even with COVID-19 impacts and security clearance timelines that continue to challenge the whole Department, USCYBERCOM offered competitive compensation and incentives to our best candidates. We are also partnering with the National Security Innovation Network (NSIN), a Defense Innovation Unit program office, to conduct a virtual hire-a-thon that runs through this month. The most recent hire-a-thon garnered more than 260 resumes from

people eager to join our team, and similar events are planned for the future. Civilians continue to play an important role for USCYBERCOM, providing vital continuity in several areas.

Conclusion

USCYBERCOM is actively engaged in addressing the nation's challenges from sophisticated and evolving adversaries in cyberspace. The Command supports other combatant commanders in every geographic and functional area of responsibility, while implementing the Department's Defend Forward strategy and enhancing our capabilities.

For the year to come our priorities are set. We will focus on great power competition through persistent engagement, especially in support of USINDOPACOM, and particularly through improving the efficiency and effectiveness of DoDIN operations and defensive cyberspace missions. To prepare for the approved growth in the CMF, we will enhance our control over resources for the force, improve its readiness (including the metrics we require in doing so), and consolidate CMF training. We will integrate the development efforts ongoing in support of the JCWA. We will also improve recruitment and retention of top military and civilian performers. All of these measures will enhance the proficiency of USCYBERCOM and boost its ability to provide defensive security assurance and options for policymakers and commanders at the senior levels of the government and the Department of Defense.

The men and women at USCYBERCOM are grateful for the support this Committee and Congress in these efforts. I thank you for that support in the important work that we have undertaken together. And now I look forward to your questions.