# POSTURE STATEMENT OF

# GENERAL PAUL M. NAKASONE

# COMMANDER, UNITED STATES CYBER COMMAND

# BEFORE THE 117TH CONGRESS

# SENATE COMMITTEE ON ARMED SERVICES

APRIL 5, 2022

(U) Chairman Reed, Ranking Member Inhofe and distinguished members of the Committee, thank you for your enduring support and the opportunity today to represent the hard working men and women of U.S. Cyber Command (USCYBERCOM). I am honored to be here and testify beside Assistant Secretary of Defense Christopher Maier and General Rich Clarke.

(U) Let me begin by acknowledging the dedicated service of our Service members and civilians at USCYBERCOM. Their mission is to plan and execute global cyber 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. Our three lines of operation are to:

- Provide mission assurance for the Department of Defense by directing the security, operation and defense of Department of Defense Information Network (DODIN), including DoD's critical infrastructure;

- Help deter and defeat strategic threats to the United States and its national interests; and

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

(U) U.S. Cyber Command directs operations through its components. These include the Cyber National Mission Force-Headquarters (CNMF-HQ), Joint Force Headquarters-DoD Information Network (JFHQ-DODIN, the commander for which is dual-hatted as the Director of the Defense Information Systems Agency) and Joint Task Force Ares. They work with our Joint Force headquarters elements, the commanders for which are dual-hatted with one of the Services' cyber components (Army Cyber Command, Marine Corps Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Force Cyber/16th Air Force and Coast Guard Cyber Command). The Command currently comprises 133 teams across the Cyber Mission Force (CMF), approximately 6,000 Service members, including National Guard and Reserve personnel on active duty. The CMF is due to grow by 14 teams over the next five years.

(U) USCYBERCOM is postured to execute its missions and meet both the nation's near-term and enduring strategic challenges in cyberspace. I shall address the Command's role in the crisis caused by Russia's invasion of Ukraine, and then speak to our preparedness for persistent threats and in meeting our long-term pacing challenge, China. As the Commander of USCYBERCOM and Director of the National Security Agency (NSA), I have learned that the Command's linkage with NSA is essential to achieving critical outcomes for the nation in both cyber and intelligence operations. The dual-hatted command relationship improves planning, resource allocation, risk mitigation, and unity of effort. It allows us to operate with speed, agility, and mission effectiveness that we could not achieve without it. This is critical to meeting the strategic challenges of our adversaries as they grow in sophistication, aggressiveness and scope of operations.

*(U) Strategic Challenges*

(U) Russia's invasion of Ukraine demonstrated Moscow's determination to violate Ukraine's sovereignty and territorial integrity, forcibly impose its will on its neighbors and

challenge the North Atlantic Treaty Organization (NATO). Russia's military and intelligence forces are employing a range of cyber capabilities, to include espionage, influence and attack units, to support its invasion and to defend Russian actions with a worldwide propaganda campaign.

(U) U.S. Cyber Command (with NSA) has been integral to the nation's response to this crisis since Russian forces began deploying on Ukraine's borders last fall. We have provided intelligence on the building threat, helped to warn U.S. government and industry to tighten security within critical infrastructure sectors, enhanced resilience on the DODIN (especially in Europe), accelerated efforts against criminal cyber enterprises and, together with interagency members, Allies, and partners, planned for a range of contingencies. Coordinating with the Ukrainians in an effort to help them harden their networks, we deployed a hunt team who sat side-by-side with our partners to gain critical insights that have increased homeland defense for both the United States and Ukraine. In addition, USCYBERCOM is proactively ensuring the security and availability of strategic command and control and other systems across the Department. We have also crafted options for national decision makers and are conducting operations as directed.

(U) When Moscow ordered the invasion in late February, we stepped up an already high operational tempo. We have been conducting additional hunt forward operations to identify network vulnerabilities. These operations have bolstered the resilience of Ukraine and our NATO Allies and partners. We provided remote analytic support to Ukraine and conducted network defense activities aligned to critical networks from outside Ukraine – directly in support of mission partners. In conjunction with interagency, private sector and Allied partners, we are collaborating to mitigate threats to domestic and overseas systems.

(U) These measures were made possible by the patient investments in cyberspace operations capabilities and capacity over the last decade, as well as by the lessons that we as a Department and a nation have learned from operational experience. The current crisis is not over, but I am proud of the response of our people and confident in their ability to deliver results no matter how long it lasts. Their grit and ingenuity have been inspiring.

(U) Shifting to longer-term considerations, I note that our operations are planned and executed in accord with the *Interim National Security Strategic Guidance*. Underpinning our work is Integrated Deterrence. We provide combat-capable forces in cyberspace that engage in active campaigning to disrupt adversary actions, demonstrate capabilities and resolve, shape adversary perceptions and gain warfighting advantages should deterrence fail. Integrated Deterrence is multi-partner, multi-domain, multi-theater and multi-spectrum, requiring us to compete every day in cyberspace against military and intelligence actors seeking to undermine our nation's strength and strategic advantages.

(U) Cyberspace is a dynamic and inter-connected domain where near-peer adversaries seek to exploit gaps and seams between our organizations and authorities. Such adversaries use a variety of cyber means to compromise our systems, distort narratives and disseminate misinformation. These actions threaten our national interests by impairing the safety and security of our citizens, stealing intellectual property and personal information while seeking to

undermine the legitimacy of our institutions. Our adversaries have demonstrated sophisticated cyber-attack capabilities for use in competition, crisis and conflict, but I am confident that USCYBERCOM is well postured to meet those challenges.

(U) China is our pacing challenge, which I see as both a sprint and a marathon. China's military modernization over the past several years threatens to erode deterrence in the western Pacific, which requires immediate steps to redress. At the same time, China is an enduring strategic challenge that is now global in scope. Beijing is exerting influence worldwide through its rising diplomatic, informational, military, and economic power. China is a challenge unlike any other we have faced. I have therefore created a China Outcomes Group under joint USCYBERCOM and NSA leadership to ensure proper focus, resourcing, planning, and operations to meet this challenge. Although we recognize that much of our effort will be in support of U.S. Indo-Pacific Command, China is a global challenge. The success of our efforts will depend in part on the resilience and capabilities of regional and worldwide partners. We are building operating relationships and also dedicating long-term work to enhance their cybersecurity and cyberspace operations forces.

(U) Iran and North Korea are cyber adversaries growing in sophistication and willingness to act. Despite our strengthened focus on China, we are maintaining our ability to counter these threats. Tehran has increased ransomware operations, the targeting of critical infrastructure, and influence campaigns (including in our 2020 elections). We support U.S. Central Command in its efforts against Iranian-backed proxies in Iraq and Syria (as we also did in the withdrawal from Afghanistan last summer). North Korea uses its cyber actors to generate revenue through criminal enterprises, such as hacking-for-hire and theft of cryptocurrency. USCYBERCOM works with the Departments of State and Treasury to stem Pyongyang's campaigns.

(U) The scope, scale and sophistication of these threats is rising. The United States faced major cybersecurity challenges over the last year, beginning with the SolarWinds supply-chain compromise but extending to incidents involving software compromises that affected companies like Colonial Pipeline, Microsoft, JBS, Kaseya, and Apache. In each instance, our Command worked through CNMF and other components to provide insights to our homeland security and law enforcement partners, who are the nation's first line of defense for U.S. systems and networks.

(U) Ransomware can have strategic effects as America saw in the disruption of Colonial Pipeline's systems. CNMF has taken numerous actions over the past year to combat ransomware in close partnership with law enforcement, interagency, industry, and foreign partners to disrupt and degrade the operations of ransomware groups attacking our nation's critical infrastructure. CNMF and NSA enabled whole-of-government actions targeting ransomware actors, passing key insights in near-real time. CNMF was a key partner in the whole-of-government effort to disrupt and impose costs against those who targeted Colonial Pipeline.

(U) USCYBERCOM (with JFHQ-DODIN) also defended the DODIN against cyber threats and helped ensure that disruptions to its systems and data remained inconsequential and brief. We continue to innovate in enhancing DODIN defenses and countering adversary threats; indeed, we must, because our adversaries are agile and adaptive. Key to this effort is building

resilience in our systems and platforms while preparing the Department, the other Combatant Commands and Defense Industrial Base (DIB) companies to operate even in degraded cyber environments.

(U) *U.S. Cyber Command Posture for the Future*

(U) Our success against these growing challenges is a result of sustained efforts and investments, not to mention a lot of hard work. I should add that that work over the last two years took place under COVID-19 mitigations. USCYBERCOM has been on-mission, running operations and exercises with the joint force and domestic and foreign partners throughout the pandemic, with negligible workforce transmission and slight impact to operations. We will continue to prioritize workplace safety, workforce confidence, and mission continuity.

(U) We see 2022 as a year of opportunity to make progress in several areas that will enhance USCYBERCOM's capabilities and contributions to national security. With this in mind, I have established the following priorities for our Command:

- Readiness;
- Operations in Defense of the Nation;
- Integrated Deterrence;
- Recruiting, Retention and Training; and
- Joint Cyber Warfighting Architecture and Enhanced Budget Control

(U) Readiness is priority one. It is foundational to the success of operations in defense of the nation and Integrated Deterrence. USCYBERCOM has made progress despite challenges. We improved our ability to monitor the status of our cyber mission forces down to the team, mission element and individual levels. Across the Department, USCYBERCOM is responsible for setting standards for all of DoD's Cyberspace Operations Forces. We work to provide commanders with the situational awareness they require to assess risks and make informed decisions, not just in operations but in maintaining force readiness as a whole. We will work with the Services this year to ensure the progress we have made over the past year continues.

(U) Second, along with our interagency partners, we defended the nation's recent elections against foreign interference and are preparing to support the defense of this year's midterms through the combined efforts of USCYBERCOM and NSA. We anticipate that our adversaries will continue using their military and intelligence elements to affect our democracy. Thus I appointed a USCYBERCOM general officer and an NSA senior executive to oversee election security in 2022. This is an enduring, no-fail mission for USCYBERCOM.

(U) Interagency partnerships are crucial in these efforts. Working with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has demonstrated that we are much stronger together. Indeed, no single agency can defend the nation on its own. USCYBERCOM imposes costs on threat actors and provides insights to domestic and foreign partners to mitigate and respond to malign activity, enabling each to act under its respective authorities. We will continue to

collaborate with our domestic partners across the federal government and the states to share best practices and expertise.

(U) Our adversaries also target our economy. DIB companies are on the frontlines in cyberspace and are constantly targeted by malicious cyber actors. Over the past year, we have deepened our relationships with private industry through voluntary information sharing. Since the nation's critical infrastructure and systems are largely in private hands, these relationships have directly enhanced our operations, in addition to the security of their commercial systems.

(U) Third, supporting the national priority of Integrated Deterrence means preparing for crisis and conflict while campaigning in competition across the full spectrum of cyber operations. It also means building the strategic partnerships that enable the defense of U.S. systems and networks beyond the DODIN and the DIB. Our foreign partnerships begin with our "Five Eye" Allies – the United Kingdom, Canada, Australia and New Zealand. The circle of partnership has been enlarged in recent years as we enhanced existing relationships with allies and forged new ones with several nations, especially in Europe and the Indo-Pacific region.

(U) Fourth is building a skilled workforce through recruitment, training, and retention. Talent is key to preserving our competitive edge against our adversaries. USCYBERCOM has improved its civilian hiring with the use of its congressionally-granted Cyber Excepted Service (CES) authorities, which allow us to offer competitive compensation packages for high-demand expertise. In addition, a diverse, talented workforce that expands equity and inclusiveness is an enduring goal. To recruit and retain a skilled military workforce, we are also grateful for the authorities Congress has granted the Services to offer flexible promotion and commissioning avenues in support of the CMF.

(U) Partnerships with academia will aid in engaging the future cyber workforce and enriching the strategic dialogue about cyber. Our new Academic Engagement network began last year and comprises 93 institutions, including 10 minority-serving institutions, across 40 states and the District of Columbia, as of March 25, 2022. Interest in partnering with USCYBERCOM is strong and growing.

(U) Training and proficiency are improving through our mission simulation capabilities, particularly the Persistent Cyber Training Environment (PCTE). The PCTE is helping us mature cyber operations tradecraft, enhance individual proficiencies and enable faster attainment of team certification and collective training in maneuvers such as Exercise CYBER FLAG.

(U) The Reserve Component is critical to protecting the nation in cyberspace. As a result of the partnership between USCYBERCOM and the National Guard Bureau during the 2020 election, Guard units could rapidly share information on malicious cyber activity with state and local authorities. Members of the National Guard and Reserve often have private-sector experience in fields of strong interest to USCYBERCOM. In addition, the ability of the National Guard and Reserve to hire cyber talent has been especially helpful in retaining the contributions of Service members who decide to leave active duty upon completion of their commitment; members can transfer to a part-time status.

(U) Our final priority is guiding the Department's investments in cyberspace capability through the Joint Cyber Warfighting Architecture (JCWA) and Enhanced Budget Control. JCWA consolidates and standardizes the Department's cyberspace operations capabilities, enabling us to integrate data from missions and monitoring to help commanders gauge risk, make timely decisions and act against threats at speed and scale. The Department is building JCWA and advancing the Cyber Mission Force's capabilities for conducting the full spectrum of cyberspace operations.

(U) USCYBERCOM is grateful to this Committee and Congress for granting us Enhanced Budget Control over resources dedicated to the Cyber Mission Force. With this authority, USCYBERCOM will improve direction, control and synchronization of investments for cyber operations across the Department of Defense.

(U) *Conclusion*

(U) U.S. Cyber Command views 2022 as a year of significant opportunity for building our capabilities against the five priorities above. Our overarching goal is to build a Command that is ready and capable at providing options and conducting operations in defense of the nation with wider partnerships and world-class talent, all linked through the Joint Cyber Warfighting Architecture. These elements will be essential to our nation's security as it faces an array of adversaries who are expanding the scope, scale and sophistication of their operations against us, and will be critical to developing the right mission posture to meet the unprecedented challenge of China.

(U) The men and women at U.S. Cyber Command are grateful for the support this Committee has given to our Command. We can only succeed with a strong partnership with Congress. Thank you, and now I look forward to your questions.