The Heritage Foundation

BACKGROUNDER
No. 3651 | AUGUST 25, 2021
CENTER FOR NATIONAL DEFENSE

Cybersecurity: Policymakers Need a Consistent Means to Assess Capabilities

James Di Pane

KEY TAKEAWAYS

The United States faces a vast cybersecurity landscape with constantly evolving threats; a robust and capable Cyber Mission Force is a national security imperative.

The cost of under resourcing U.S. Cyber Command could mean failing to deter a catastrophic cyberattack.

The Department of Defense and Congress need to ensure budgets and manpower levels meet U.S. Cyber Command's operational demands.

Two recent cyber hacks, the SolarWinds and the Chinese use of Microsoft products to infiltrate client networks, highlight the fact that sophisticated cyber threats are tangible and immediate.[1] The cost of under-resourcing cyber capability could mean failing to deter a catastrophic cyberattack against U.S. critical infrastructure or operational defeat of American forces in an armed conflict. If offensive cyber capability lags behind the capabilities of likely adversaries, America's policy options will shrink, and its security policy objectives will be undermined. These are high stakes indeed.

When assessing U.S. cyber capabilities, policymakers and Members of Congress should keep a few fundamental questions in mind: Is U.S. Cyber Command adequately staffed to meet the demands put on it? Are its people of sufficiently high quality and

appropriately trained to meet the challenges of today and thwart the threats of tomorrow? Does it have the right organization to be effective? Does it have the most cutting-edge technology available? And are its offensive and defensive capabilities being best utilized in support of U.S. national security?

While the answers to these questions are normally classified as military secrets and normally unavailable to the general public, policymakers should nonetheless press to achieve a full understanding of this most critical area.

U.S. Cyber Command and Its Action Arm: Cyber Mission Forces

U.S. Cyber Command is America's primary military organization for offensive and defensive cyber operations against America's adversaries. Originally created with a focus on defending military networks from cyber espionage, Cyber Command has expanded to cover defending the nation's critical infrastructure, election security, and supporting military cyber objectives with both offensive and defensive operations.[2]

The Cyber Mission Forces (CMF) are the operational units of Cyber Command and provide the backbone for offensive and defensive cyber operations. When the Department of Defense (DOD) stood up the CMF in 2013, it envisioned a force of 133 teams with 6,200 personnel based on the mission requirements at that time. All 133 CMF teams reached full operational capability in 2018.[3]

These teams are broken down into functional areas. There are 13 National Mission Teams that defend the United States against high-impact cyberattacks and provide election security. There are 68 Cyber Protection Teams focusing on defending DOD networks and systems. There are also 27 Combat Mission Teams that support or conduct operations across the globe either in tandem with or independent of other military forces. Additionally, 25 Support Teams provide support with analysis and planning.[4]

In addition, there are about 12,000 personnel outside U.S. Cyber Command who maintain DOD networks under the command of the various services.

Adversary Cyber Capabilities: Growing and Dynamic

As robust as U.S. cyber capabilities are, those of America's adversaries are formidable as well. China, Russia, Iran, North Korea, and non-state actors ranging from international terrorists to criminal organizations are the key

adversaries for the U.S. in cyberspace. According to the most recent Worldwide Threat Assessment published by the Office of the Director of National Intelligence: "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners."[5]

- The Chinese have invested heavily in cyber with the intention of becoming a cyber superpower.[6] It is the most active adversary in cyber espionage, targeting vast amounts of important intellectual data in public and private networks. One example is the Office of Personnel Management hack, detected in 2014, in which the Chinese were able to steal millions of personnel records with sensitive information on individuals holding security clearances.[7] A more recent example is the Microsoft hack this past year, in which Chinese hackers reportedly used flaws in SolarWinds software to infiltrate U.S. government networks as well.[8]

- Russia has extensive cyber capabilities and poses a large threat to U.S. critical infrastructure networks. The Worldwide Threat Assessment contained a stark warning about Russia's cyber capabilities: "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."[9]

- Iran and North Korea are continuing to improve their cyber capabilities. Iran's capabilities for disruptive or destructive cyberattacks are growing, and they have a clear intent to challenge the United States in cyberspace. North Korea has the ability to strike the United States in cyberspace and uses its cyber forces to evade United Nations sanctions.[10]

- Complicating the situation further is the opaque threat landscape in cyber. There are a number of Advanced Persistent Threats that act in concert with or on behalf of nation-states, as well as on their own. In the case of the SolarWinds hack, the hacking group was most likely "Cozy Bear," a group thought to be affiliated with Russian intelligence.[11]

The DOD faces millions of attempted intrusions every day[12]—and this is a *peacetime* level of activity. The observed cyber activity could dramatically increase during wartime in both tempo and severity.

How Much Is Enough?

In March 2020 testimony, the commander of Cyber Command, General Paul Nakasone, acknowledged that the CMF was created before election security and international developments increased its workload.[13] Later in 2021, he stated, "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 [Cyber Command] can fulfill its responsibility as both a supported and a supporting command."[14]

It appears the original organization and manpower levels are insufficient for handling today's missions. But how should policymakers and Members of Congress assess the need for more? Should they just take Nakasone's word for it? And what could the DOD do to ensure that there is ample understanding of the requirement?

For more conventional military forces, this is an easier question to answer: Navies can be measured by ship counts, missile magazines, or tonnage; armies by tanks, soldiers, or artillery. Cyber is more challenging because of the secrecy that surrounds cyber forces and methods, as well as the different character of cyber conflict.

One solution to this problem would be the development of consistent metrics to convey a relative sense of the security of the DOD in cyberspace. These metrics should include quantifiable elements such as manpower levels, budgets, and the numbers of offensive and defensive cyber incidents in addition to assessments of how U.S. cyber forces compare to their adversaries, how effective their offensive and defensive cyber operations are, and whether the current force is able to meet the demands placed on it. Other factors, such as training and partnerships, could also be included.

Financial Metrics

The President's budget request for cybersecurity was $9.7 billion for fiscal year (FY) 2021. The DOD had requested $9.8 billion for cyber, with $3.8 billion of that going toward cyber operations.[15] For FY 2020, the DOD requested $9.6 billion for cyber, $3.7 billion of which was designated for offensive and defensive cyber operations.[16] Cyber Command's budget for

FY 2021 is approximately $605 million;[17] in FY 2020, it was reported to be $596 million.[18]

It is important to highlight that "throwing money at the problem" is not always an effective way of improving U.S. government capabilities. Money can be misallocated or inefficiently spent. The budget request for cybersecurity says nothing about how effectively that money will be spent. However, as higher priorities often see more funding, changes in year-to-year funding are useful as a snapshot of how high of a priority cybersecurity is considered.

Manpower Metrics

Manpower levels are another easy-to-track metric. In the same way that funding levels change from year to year, personnel levels can show if there is more attention going to cyber or less. If the CMF were to be cut in half or doubled, that would say a lot about their institutional priority.

President Biden is reportedly requesting an increase for the CMF of approximately 600 personnel—an increase of around 10 percent—in his FY 2022 budget request.[19]

However, the drawback with assessing people is similar to the issue with tracking money. People can be mismanaged and poorly organized to the point that adding more people will not improve the situation.

For example, defense officials have stated that teams are being reassigned from the counterterrorism mission to the great-power competition mission, a reflection of the growing importance of peer and near-peer competition.[20] This shows that decisions must be made with how best to use the available teams, and more attention to one mission set means less attention to another.

In addition, cyber is an unforgiving domain in which quality is valued over quantity. General Nakasone has stated that the best cyber personnel—such as talented coders—could be 10–20 times more valuable than their peers.[21] This places an imperative on developing and retaining cyber personnel.

Every effort should be made to retain and develop talent. It is not enough to fully staff a sufficiently large cyber force. That force must also be effective to have its intended impact in understanding and countering the adversaries in the cyber domain.

Training, incentives, and allowing individuals to remain in cyber positions for extended periods of time could all help to foster a stronger and more effective cyber workforce.

Successes of Past Operations

Another means of assessing U.S. cyber effectiveness is to judge the effectiveness of particular operations toward achieving their goals. One example is the 2016 cyber war in which the United States used cyber operations to fight the Islamic State's ability to distribute propaganda online and fundraise.[22] Another is Cyber Command activity to deter Russian and Iranian[23] interference in the 2020 U.S. elections. A third example is the cyber retaliation taken against Iran following the downing of the U.S. drone in the Strait of Hormuz in 2019. Reports indicated the U.S. conducted a cyber operation action that actually affected physical hardware in Iran.[24]

The vast majority of these operations are classified, and some may never be made public. This means the available information will always be limited. As in the cyber operations against Iran, press reporting can indicate suspected cyber activity, but they cannot provide a real understanding of how the U.S. cyber forces are doing operationally. In the case of Iran, all our information came from Iranian sources, and they are not known for their truthfulness.

Without access to the classified material, it is also exceedingly difficult to get a sense of the volume of cyber operations, their success or failure rates, or how successful adversaries are in targeting U.S. networks. General Nakasone testified that U.S. Cyber Command launched over two dozen operations in advance of the 2020 elections,[25] but without that testimony, this information would not have come to light.

Cyber officials should ensure that Congress and policymakers are kept adequately informed on the offensive cyber capabilities and options that can be employed to secure U.S. interests. The better informed leaders are on these options, the better able they will be to effectively use these important tools.

But there is also room for the DOD to release more information without giving away vulnerabilities to adversaries. Cyber officials could make a better case for additional resources by releasing more information about the volume and effectiveness of their operations.

Recommendations

The DOD should:

- **Provide more information to the public on the state of cybersecurity.** The need for secrecy regarding America's cyber forces is

critical. However, it must be balanced with the need to make the case for more resources to Congress and the American people.

- **Develop consistent criteria for briefing Congress on the state of the CMF and cybersecurity.** Congress should be able to fully understand the shortfalls in cyber and their impacts in an objective way. The DOD should develop performance metrics based on personnel, technology, and policies and procedures to provide stability and objectivity to congressional briefings.

- **Conduct a force structure assessment on U.S. Cyber Command every three years.** The 133 CMF teams were originally created and sized in 2013 to meet the needs of eight years ago. But since then, the world has changed in significant ways, and election security has been added as a core mission for Cyber Command. Conducting a force structure assessment would help ensure that the military has the right amount of personnel to conduct their vital offensive and defensive missions, taking into account the increased activity from cyber criminals and nation-states.[26]

- **Cultivate a better cyber force by enhancing training, attracting quality talent, and providing a cyber career track.** In 2019, the Government Accountability Office identified a lack of consistency in training protocols for U.S. Cyber Command.[27] The DOD should address this problem.

- **Strengthen public–private partnerships to ensure the CMF have access to cutting-edge technologies.** It is essential for U.S. Cyber Command to have strong relationships with the private sector in order to benefit from technological developments.[28] One way to strengthen these relationships is to increase the amount of threat intelligence given to the private sector.

- **Strengthen partnerships and cyber cooperation with key allies.** Strengthening cyber capabilities among U.S. allies helps to build resilience and enhance deterrence. The United States should actively work with its "Five Eyes" allies—Australia, Canada, New Zealand, and the United Kingdom—to defend against common threats in cyberspace. Cooperation could also expand to other NATO allies and to partners such as India, Japan, and South Korea.

Congress should:

- **Mandate an annual report on the state of the DOD's cybersecurity, with both a classified and unclassified version for release.** This report could serve as the basis for briefing materials and should be based on metrics, especially at the classified level. The unclassified version would educate the public on the broad state of cybersecurity and the possible need for increased funding.

- **Provide sufficient funding for the CMF to handle the new mission set of election security and threats to critical infrastructure.** Congress should support the growth of the CMF to ensure it is adequate to meet the demands required of it. U.S. Cyber Command is currently engaged in a force structure assessment, and Congress should support its findings with resources.

Ensuring the Force Is Capable Against Its Likely Adversaries

A robust and capable CMF is a national security imperative that should be adequately supported. The first step is to ensure the budgets and manpower levels are adequate for U.S. Cyber Command to meet its operational demands. Also, force structure assessments should be done regularly to ensure the CMF keeps up with its dynamic mission set and that its forces are being used to maximum efficiency to cover the most important missions.

The next step is to ensure that the force is as competent and effective as it can be by cultivating and retaining talent. Cyber Command officials have pointed to the success of transitioning cyber personnel from active duty to reserve roles in order to retain them, as well as the contributions provided by National Guard personnel.[29] Other options include increasing performance incentives, extending the time cyber personnel spend in cyber billets, and ensuring there is a clear promotion path within the cyber infrastructure. Training should be standardized in order to foster consistent skills and practices across the services, and policymakers should actively question whether the force is adequately trained.

James Di Pane is Policy Analyst for Defense Policy in the Center for National Defense, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

Endnotes

1. Dustin Volz and Robert McMillan, "Suspected China Hack of Microsoft Shows Signs of Prior Reconnaissance," *Fox Business*, April 7, 2021, https://www.foxbusiness.com/technology/china-cyberattack-microsoft-email-personal-data (accessed June 4, 2021).
2. C. Todd Lopez, "Commander Discusses a Decade of DOD Cyber Power," U.S. Department of Defense, May 21, 2020, https://www.defense.gov/Explore/News/Article/Article/2193130/commander-discusses-a-decade-of-dod-cyber-power/ (accessed June 4, 2021).
3. News release, "Cyber Mission Force Achieves Full Operational Capability," U.S. Department of Defense, May 17, 2018, https://www.defense.gov/Explore/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/ (accessed June 4, 2021).
4. Office of the Under Secretary of Defense, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request*, February 2018, pp. 3–11, https://dod.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf (August 11, 2021).
5. Daniel R. Coats, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," statement for the record before the Select Committee on Intelligence, January 29, 2019, p. 5, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (accessed June 4, 2021).
6. International Institute for Strategic Studies, *Asia Pacific Regional Security Assessment 2019*, 2019, pp. 77–90, https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5 (accessed August 11, 2021).
7. Brendan I. Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (accessed June 4, 2021).
8. Christopher Bing et al., "Exclusive: Suspected Chinese Hackers Used SolarWinds Bug to Spy on U.S. Payroll Agency—Sources," Reuters, February 2, 2021, https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8 (accessed June 4, 2021).
9. Coats, "Worldwide Threat Assessment of the US Intelligence Community," p. 6.
10. Gen. Paul M. Nakasone, "Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command," posture statement before the Armed Services Committee, U.S. Senate, March 25, 2021, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf (accessed June 4, 2021). See also Bruce Klingner, "North Korean Cyberattacks Pose Threat to U.S.," Heritage Foundation *Commentary*, June 3, 2021, https://www.heritage.org/cybersecurity/commentary/north-korean-cyberattacks-pose-threat-us.
11. David E. Sanger, Nicole Perlroth, and Eric Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit," *New York Times*, December 15, 2020, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html (accessed June 4, 2021).
12. Mark Pomerleau and Joe Gould, "Which Cyber Priorities Didn't Appear in the Pentagon's Budget," *Defense News*, February 21, 2020, https://www.defensenews.com/dod/cybercom/2020/02/21/which-cyber-priorities-didnt-appear-in-the-pentagons-budget/ (accessed June 4, 2021).
13. Paul M. Nakasone and Kenneth P. Rapuano, "The Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cyberspace," hearing before the Subcommittee on Intelligence and Emerging Threats and Capabilities, March 4, 2020, https://armedservices.house.gov/2020/3/subcommittee-on-intelligence-and-emerging-threats-and-capabilities-hearing-the-fiscal-year-2021-budget-request-for-u-s-cyber-command-and-operations-in-cyberspace (accessed June 4, 2021).
14. Nakasone, "Posture Statement of General Paul M. Nakasone."
15. News release, "DOD Releases Fiscal Year 2021 Budget Proposal," U.S. Department of Defense, February 10, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/ (accessed June 4, 2021).
16. News release, "DOD Releases Fiscal Year 2020 Budget Proposal," U.S. Department of Defense, March 12, 2019, https://www.defense.gov/Newsroom/Releases/Release/Article/1782623/dod-releases-fiscal-year-2020-budget-proposal/ (accessed June 4, 2021).
17. Nakasone, "Posture Statement of General Paul M. Nakasone."
18. Nakasone, "Statement of Paul M. Nakasone."
19. Martin Matishak and Lara Seligman, "Biden Budget to Seek Boost to the Military's Cyber Force," *Politico*, May 26, 2021, https://www.politico.com/news/2021/05/26/biden-budget-military-cyber-force-490965 (accessed August 16, 2021).
20. Mark Pomerleau, "Cyber Command Shifts Counterterrorism Task Force to Focus on Higher-Priority Threats," C4ISRNET, May 4, 2021, https://www.c4isrnet.com/cyber/2021/05/04/cyber-command-shifts-counterterrorism-task-force-to-focus-on-higher-priority-threats/ (accessed August 11, 2021).
21. "An Interview with Paul M. Nakasone," *Joint Force Quarterly*, Vol. 92 (1st Quarter 2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf (accessed June 4, 2021).
22. Dina Temple-Raston, "How the U.S. Hacked ISIS," NPR, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis (accessed June 4, 2021).
23. Ellen Nakashima, "U.S. Undertook Cyber Operation Against Iran as Part of Effort to Secure the 2020 Election," *Washington Post*, https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html 9 (accessed May 28, 2021).

24. Idrees Ali and Phil Stewart, "Exclusive: U.S. Carried Out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials," Reuters, October 16, 2019, https://www.reuters.com/article/us-usa-iran-military-cyber- exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK (accessed June 4, 2021).
25. Nakasone, "Posture Statement of General Paul M. Nakasone."
26. U.S. Cyberspace Solarium Commission, *Final Report*, March 2020, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view (accessed June 4, 2021).
27. U.S. Government Accountability Office, *U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO–19–362, March 2019, https://www.gao.gov/assets/gao-19-362.pdf (accessed June 4, 2021).
28. Mark Pomerleau, "US Cyber Command's Top General Makes Case for Partnering with Tech Firms," C4ISRNET, August 25, 2020, https://www.c4isrnet.com/cyber/2020/08/25/us-cyber-commands-top-general-makes-case-for-partnering-with-tech-firms/ (accessed June 4, 2021).
29. Nakasone, "Posture Statement of General Paul M. Nakasone."