Cyber Warfare and U.S. Cyber Command

James Di Pane

The world of cyber operations is notoriously secretive. Nevertheless, even a rudimentary understanding of the domain, the threats and opportunities associated with it, and the ability of the Department of Defense (DOD) to protect the U.S. from cyberattack and enable military operations against enemies is of the greatest importance. To supplement the concise overview of military cyber capabilities provided in this chapter, more detailed discussions of the characteristics of cyber warfare can be found in "National Defense and the Cyber Domain"[1] and "The Reality of Cyber Conflict: Warfare in the Modern Age."[2] These essays, published in previous editions of the *Index of U.S. Military Strength*, provide a wealth of information about the cyber domain and how it fits into the world of national defense.

Cybersecurity has been very much in the forefront of public attention this year, with several large cyber incidents from foreign actors drawing considerable public attention. The Solar Winds hack and the Colonial Pipeline and other notable ransomware attacks demonstrate the potential threat to the homeland from malicious cyber actors and provide a window into the types of threats the U.S. could face on a broader scale during wartime. They also demonstrate the link between private networks and public networks, as well as the broad approach that is necessary to ensure cybersecurity.

The vulnerability of allies and the private sector has an indirect effect on military affairs because the compromise of just one can lead to complications for the military services. In the words of Kenneth P. Rapuano, former Assistant Secretary of Defense for Homeland Defense and Global Security:

> Their vulnerability means that adversaries could disrupt military operations without actually targeting military networks and systems themselves.... To address these challenges, we are strengthening alliances and attracting new partners to take a whole-of-society approach to enabling better security and resilience of key assets.[3]

Because of this, cybersecurity for the military is very expansive and goes beyond the Department of Defense alone.

The use of cyber as a military tool to target enemy forces and capabilities falls into categories similar to those of other military operations. Cyber tools can be used in the form of conventional operations, like the operations against the Islamic State that were used to disrupt command and control nodes and the group's ability to distribute propaganda.[4] In this type of campaign, cyber accompanies the other military capabilities as a way to target enemy forces.

Or they can take the form of special operations–type activity like the Stuxnet cyber operation against Iran, which could be compared to the U.S. Navy SEAL raid to kill Osama Bin Laden.[5] In these operations, cyber is used to achieve targeted goals, sometimes in a covert way that, like special operations, falls below the threshold of traditional armed conflict.

In conventional operations, cyber is used to support forces and commanders by ensuring that they can operate uninhibited in cyberspace or by disrupting the enemy's ability to operate in order to achieve necessary objectives more effectively. In this way, cyber is used to gain an advantage over an adversary similar to the way advantage is sought in the other domains.[6] This is similar to the use of naval forces to restrict the enemy's ability to use the seas to achieve strategic ends.

Like naval power, cyber is an important means with which to maximize one's own access and effectiveness while restricting the opponent's access and effectiveness. However, it differs from other domains in the sense that time and space are incredibly compressed. A cyber force can launch an attack from anywhere in the world and strike very quickly, unlike more traditional forces that take time to move and launch attacks.

U.S. Cyber Command

U.S. Cyber Command (USCYBERCOM) is a capability-based Unified Combatant Command similar to U.S. Special Operations Command and is the military's primary organization for both offensive and defensive cyber activity. It is currently commanded by General Paul Nakasone, who serves simultaneously as Director of the National Security Agency (NSA). The two organizations have a close cooperative relationship: The NSA and Cyber Command operate, respectively, under Title 50 and Title 10 of the U.S. Code, the sections that govern intelligence and military affairs.[7]

U.S. Cyber Command was founded in 2010 as a sub-unified command under U.S. Strategic Command. In 2018, the Trump Administration elevated it to full Unified Combatant Command status, and it reached full operational capability in that same year.[8] Over the past approximately 11 years, Cyber Command has grown from a very small organization that was largely dependent on the NSA for personnel and resources into the much more robust and independent organization that exists today.

Missions

U.S. Cyber Command has a wide range of missions, from offensive and defensive cyber operations to monitoring DOD networks and assisting with the defense of critical infrastructure. Its primary role is to ensure the DOD's ability to operate in a world that is increasingly dependent on cyber. To this end, according to General Nakasone:

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.[9]

These "lines of operation" are critical to ensuring the success of the military enterprise and national defense, as any compromise in the ability to communicate or operate could jeopardize the full range of U.S. military activities.

The types of operations that Cyber Command is tasked with performing encompass defensive cyber activity coupled with offensive options to impose costs on an adversary. For example, USCYBERCOM is helping to lead the government's response to the SolarWinds hack.

Discovered in December 2020, the Solar Winds hack was one of the most significant breaches of computer networks in history, and its effects are still being felt because of the number of organizations affected and the sophistication of the hackers. A Russia-aligned hacking organization known as Cozy Bear was most likely behind the breach. Thousands of private-sector organizations, as well as government agencies like the Departments of the Treasury, Commerce, and Homeland Security, were compromised following the corruption

of the widely used Orion software. Cyber Command has worked to search for compromise within networks and expel the adversary when found, and it will provide options to policymakers for imposing costs on the attacker.

With respect to election security, U.S. Cyber Command conducted a number of operations aimed at preventing meddling in the 2020 presidential election. Another example was the 2018 targeting of the Russian Internet Research Agency (IRA), "a troll farm that led the effort to spread disinformation around the 2016 presidential election and 2018 midterm elections."[10] USCYBERCOM proactively shut down the organization's Internet access to prevent it from engaging in influence operations against the United States.

In 2021, Cyber Command has also continued to support the ongoing counterterrorism fight, including force protection and target prosecution in Afghanistan in support of U.S. Central Command. These efforts are continuous and extend to other regions as well, including support for U.S. Special Operations Command. Cyber is used to disrupt terrorist organizations' financing and ability to communicate in addition to intelligence collection and targeting.

A key part of these missions is the concept of "defending forward." As described in the 2018 DOD Cyber Strategy, "[t]his includes working with the private sector and our foreign allies and partners to contest cyber activity that could threaten Joint Force missions and to counter the exfiltration of sensitive DoD information."[11]

Defending forward means operating as close to the origins of the cyber threat as possible before it reaches critical networks in the U.S. with the goal of collecting threat intelligence or disrupting attacks. This is contrasted with passive defense, which involves monitoring within U.S. networks for intrusions. Cyber compresses time and space in the battlespace by its very nature, and attacks can emanate from anywhere in the world with similar speed. U.S. forces must therefore engage adversaries in their networks and work to disrupt attacks in their early stages because it is often too late once the networks have been compromised.

Budget

Analyzing the budget for cybersecurity is difficult because of the large degree of classification involved, but there are some data that can be tracked with respect to USCYBERCOM and the broader Department of Defense. President Joseph Biden's FY 2022 DOD budget request includes $10.4 billion for cyberspace.[12] This is slightly higher than the $9.8 billion requested for FY 2021.[13]

General Nakasone has testified that U.S. Cyber Command alone executed a budget of $605 million in FY 2021.[14] This was $9 million over the reported executed budget for FY 2020, which was $596 million.[15]

Capacity

The Cyber Mission Force is the operational arm of U.S. Cyber Command, and CMF teams are distributed across various mission sets. In 2013, a force of 133 teams with 6,200 personnel was envisioned based on the mission requirements at that time. All 133 CMF teams reached full operational capability in 2018.[16] These teams are distributed across functional areas. Specifically, there are:

- 13 National Mission Teams that defend the U.S. against high-impact cyberattacks and provide for election security;
- 68 Cyber Protection Teams that are focused on defending DOD networks and systems and ensuring that the department is not compromised by a hack;
- 27 Combat Mission Teams that support the combatant commands with integrated cyber effects in various theaters across the globe, either in tandem with or independent of other military forces, and ensure that the Combatant Commanders have cyber tools at their disposal; and
- 25 Support Teams that support the national mission and combat teams with analysis and planning.[17]

The teams are supported by four service components: Army Cyber Command (ARCYBER); Air Force Cyber Command (AFCYBER); Navy Fleet Cyber Command (FLTCYBER); and Marine Corps Forces Cyberspace Command (MARFORCYBER). These four commands, created at the same time that U.S. Cyber Command was created, provide the operational forces that make up the teams.

- ARCYBER supplies 41 teams to the CMF;[18]
- AFCYBER supplies 39 teams;[19]
- FLTCYBER supplies 40 teams, which reached full operational capability a year ahead of schedule in 2017;[20] and
- MARFORCYBER provides 13 teams.[21]

As of January 2021, according to General Nakasone, Cyber Command had "roughly 6,000 service members and civilians out of an authorized total of 6,187 positions."[22] The Biden Administration is proposing a 10 percent increase to expand the CMF by approximately 600 personnel to meet its growing demands for FY 2022.[23]

In addition, there are about 12,000 personnel outside of U.S. Cyber Command who maintain DOD networks and fall under the command of the various services. Asked by House Armed Services Committee Chairman James Langevin (D–RI) to specify "how many people will be part of the new Cyber Operations Force," General Paul Nakasone, Commander of U.S. Cyber Command and Director of the National Security Agency, testified that "I would say the 6,187 that are part of our Cyber Mission Force. And then I would say probably double that with regards to our cybersecurity service providers across all four services."[24]

The recruiting and retaining of cyber talent is one of the key challenges for U.S. Cyber Command, which has invested in retention and incentive programs in an effort to keep the talent it cultivates. The high demand for cyber personnel in the private sector makes this a difficult challenge.

Capability

Due to the nature of cyber and the classification of methods, analyzing USCYBERCOM's capability as reflected in open-source (i.e., unclassified) literature is nearly impossible. However, the United States is considered to be one of the world's most capable cyber actors, an assessment that is based on its wide range of infrastructure and strategies and the advanced technologies that the U.S. is known to employ.[25]

Readiness

Because of the lack of open-source reporting, it is also nearly impossible to assess the readiness of America's cyber forces. The U.S. Government Accountability Office has identified some issues of training consistency in the past.[26] Standardizing and improving training is one of the main priorities for U.S. Cyber Command, along with retaining its talent, and both are critical to maintaining readiness.

Conclusion

Cyber is a key domain for the U.S. military. It also is increasingly important and expansive in the modern world generally. As seen in the various breaches and ransomware attacks that have come to light, cybersecurity for defense extends well beyond the Department of Defense. For the Joint Force, cyber supports military capabilities both by ensuring that U.S. forces can operate in cyberspace without disruption and as a tool on its own to achieve goals.

U.S. Cyber Command is the primary organization for the full spectrum of military cyber operations, and it has grown as an organization, reaching full operating capability in 2018. Now that USCYBERCOM has reached its authorized manning levels, the emphasis has shifted to training the force to ensure that in the coming years, it will be as capable as possible in helping to advance and protect the nation's interests.

Endnotes

1. G. Alexander Crowther, "National Defense and the Cyber Domain," in *2018 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2018), pp. 83–97, https://www.heritage.org/sites/default/files/2017-10/2018_IndexOfUSMilitaryStrength-2.pdf.
2. Paul Rosenzweig, "The Reality of Cyber Conflict: Warfare in the Modern Age," in *2017 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2016), pp. 31–40, https://ims-2017.s3.amazonaws.com/2017_Index_of_Military_Strength_WEB.pdf.
3. Terri Moon Cronk, "DOD's Cyber Strategy of Past Year Outlined Before Congress," U.S. Department of Defense, March 6, 2020, https://www.defense.gov/Explore/News/Article/Article/2103843/dods-cyber-strategy-of-past-year-outlined-before-congress/ (accessed June 17, 2021).
4. 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 17, 2021).
5. Crowther, "National Defense and the Cyber Domain," *2018 Index of U.S. Military Strength*, p. 88.
6. U.S. Department of Defense, Joint Chiefs of Staff, Joint Publication 3-12, *Cyberspace Operations*, June 8, 2018, p. I-8, https://www.marforcyber.marines.mil/Portals/215/Docs/JP%203-12.pdf?ver=2019-03-20-110123-190 (accessed June 17, 2021).
7. See U.S. Code Title 50, https://www.law.cornell.edu/uscode/text/50 (accessed June 19, 2021), and U.S. Code Title 10, https://www.law.cornell.edu/uscode/text/10 (accessed June 19, 2021).
8. U.S. Cyber Command, "About: Our History," https://www.cybercom.mil/About/History/ (accessed June 17, 2021).
9. General Paul M. Nakasone, Commander, United States Cyber Command, posture statement before the Committee on Armed Services, U.S. Senate, March 25, 2021, p. 1, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf (accessed June 17, 2021).
10. Maggie Miller, "Trump Confirms 2018 US Cyberattack on Russian Troll Farm," *The Hill*, July 10, 2020, https://thehill.com/policy/cybersecurity/506865-trump-confirms-2018-us-cyberattack-on-russian-troll-farm (accessed June 17, 2021).
11. U.S. Department of Defense, "Summary: Department of Defense Cyber Strategy, 2018," p. 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed June 17, 2021).
12. News release, "The Department of Defense Releases the President's Fiscal Year 2022 Defense Budget," U.S. Department of Defense, May 28, 2021, https://www.defense.gov/Newsroom/Releases/Release/Article/2638711/the-department-of-defense-releases-the-presidents-fiscal-year-2022-defense-budg/ (accessed June 17, 2021).
13. 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 17, 2021).
14. Nakasone, posture statement before Senate Armed Services Committee, p. 4.
15. General Paul M. Nakasone, Commander, United States Cyberspace Command, statement before the Subcommittee on Intelligence and Emerging Threats and Capabilities, Committee on Armed Services, U.S. House of Representatives, March 4, 2020, p. 2, https://docs.house.gov/meetings/AS/AS26/20200304/110592/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf (accessed June 17, 2021).
16. 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 17, 2021).
17. U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *United States Department of Defense Fiscal Year 2019 Budget Request: Defense Budget Overview*, February 2018, p. 3-11, https://dod.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf (accessed June 17, 2021).
18. U.S. Army Cyber Command, "DOD Fact Sheet: Cyber Mission Force," February 10, 2020, https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/ (accessed June 17, 2021).
19. Tech. Sgt. R. J. Biermann, "Air Force Cyber Mission Force Teams Reach 'Full Operational Capability,'" Joint Base San Antonio, May 16, 2018, https://www.jbsa.mil/News/News/Article/1524859/air-force-cyber-mission-force-teams-reach-full-operational-capability/ (accessed June 19, 2021).
20. Petty Officer 1st Class Samuel Souvannason, "Navy Cyber Mission Force Teams Achieve Full Operational Capability," U.S. Department of Defense, November 2, 2017, https://www.defense.gov/Explore/News/Article/Article/1361059/navy-cyber-mission-force-teams-achieve-full-operational-capability/ (accessed June 19, 2021).

21. Biermann, "Air Force Cyber Mission Force Teams Reach 'Full Operational Capability.'"
22. Nakasone, posture statement before Senate Armed Services Committee, p. 1.
23. 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 June 17, 2021).
24. Testimony of General Paul M. Nakasone, Commander, U.S. Cyber Command, and Director, National Security Agency, in hearing, *The Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cyberspace*, Subcommittee on Intelligence and Emerging Threats and Capabilities, Committee on Armed Services, U.S. House of Representatives, 116th Cong., 2nd Sess., March 4, 2020, p. 8, https://www.congress.gov/116/chrg/CHRG-116hhrg40605/CHRG-116hhrg40605.pdf (accessed July 19, 2021).
25. International Institute for Strategic Studies, *The Military Balance 2021: The Annual Assessment of Global Military Capabilities and Defence Economics* (London: Routledge, 2021), pp. 503–506.
26. U.S. Government Accountability Office, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362, March 6, 2019, https://www.gao.gov/assets/gao-19-362.pdf (accessed June 17, 2021).