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 discussion, two essays, "National Defense and the Cyber Domain" and "The Reality of Cyber Conflict: Warfare in the Modern Age," from 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.[1]

The vulnerability of allies and the private sector to cyberattacks can lead to complications for the military services that negatively affect the ability of the United States to sustain a war effort, thereby compromising our national security. But the need for cybersecurity goes beyond the Department of Defense alone. In the words of Kenneth P. Rapuano, former Assistant Secretary of Defense for Homeland Defense and Global Security:

> The increasingly provocative activities of key competitors, such as the NotPetya cyber operation conducted by Russia in February 2018, demonstrate how vulnerable the Department is to attacks against the many non-DoD-owned assets that are nevertheless critical to our ability to execute our missions. These assets include civilian ports, airfields, energy systems, and other critical infrastructure. Vulnerabilities in these areas will likely be targeted by our adversaries to disrupt military command and control, financial operations, the functioning of operationally critical contractors, logistics operations, and military power projection, all without ever targeting the comparatively well-protected DoD Information Network. Any large-scale disruption or degradation of national critical infrastructure represents a significant national security threat.
>
> To address these challenges, the DoD Cyber Strategy directs DoD to strengthen alliances and attract new partners to ensure that we are taking a whole-of-society approach and to enable better security and resilience of key assets....[2]

The use of cyber as a military tool to target enemy forces and capabilities falls into categories that are 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.[3] In this type of campaign, cyber supplements other military capabilities as a way to target enemy forces.

Cyber also 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.[4] 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 in much the same way advantage is sought in the other domains[5] (for example, when naval forces 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 a very important respect: In cyber operations, time and space are incredibly compressed. A cyber force can launch an attack from anywhere in the world and strike very quickly, whereas more traditional forces need time to move, are affected by terrain and weather, and must physically position themselves to 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, U.S. Army, 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.[6]

U.S. Cyber Command was founded in 2010 as a sub-unified command under U.S. Strategic Command. The Trump Administration elevated it to full Unified Combatant Command status in 2018, and it reached full operational capability in the same year.[7] Over the past approximately 12 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 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, Cyber Command has three "enduring lines of operation":

- 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.[8]

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.

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."[9]

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. As noted, 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. U.S. Cyber Command physically deploys teams abroad to work alongside the cyber forces of partner nations to operate in selected networks.[10]

Cyber and the War in Ukraine

Russia's invasion of Ukraine is significant for cyber because it shows how cyber can be used in conjunction with conventional military assets. While it was largely overshadowed by other aspects of Russia's invasion like the movements of armor units and use of artillery, the Russians utilized cyber throughout as part of their overall war plan. This includes some notable operations that had effects beyond Ukraine. For example:

- The Russians targeted Viasat, an American satellite communications company that provided support to the Ukrainian military, with malware designed to erase its data before disabling it. The Russians did not limit the malware's scope, and it ended up affecting other ground satellite components, causing hundreds of thousands of people outside of Ukraine to lose electrical power and their connection to the Internet.[11]

- A cyberattack against the City Council of Odessa, a major Ukrainian port city situated on the Black Sea, was timed to coincide with a cruise missile attack that was meant to disrupt Ukraine's response to Russian forces attacking in the south.[12]

- Cyberattacks have also been launched against many parts of Ukraine's infrastructure and government and civilian networks, including hospitals.[13]

These actions show that cyber operations are not limited to the military forces of the combatants and, like World War II strategic bombing efforts, often extend to strike at infrastructure and areas of economic significance.

U.S. Cyber Command has provided analytic support and has sought additional ways to support Ukraine. It has deployed cyber teams to support both Ukraine and NATO allies, and those efforts have proved critical to protecting U.S. networks and critical infrastructure as well as those of NATO allies. Specifically, according to General Nakasone:

> 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 [Department of Defense Information Networks] (especially in Europe), accelerated efforts against criminal cyber enterprises and, together with interagency members, Allies, and partners, planned for a range of contingencies.[14]

Budget

Analyzing the budget for cybersecurity is difficult because of the degree of classification involved, but some data can be tracked with respect to USCYBERCOM and the broader Department of Defense. President Joseph Biden's FY 2023 budget includes $11.2 billion for "Cyberspace Activities."[15] This is $800 million more than the FY 2022 DOD budget request, which included $10.4 billion for cyberspace.[16]

General Nakasone testified in March 2021 that "USCYBERCOM's FY21 budget [was] roughly $605 million, which covers the headquarters staff and the Cyber National Mission Force," and that "27 different components shape the Department's overall Cyber Activities Budget, which averages about $10 billion a year."[17]

Capacity

The Cyber Mission Force (CMF) 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.[18]

These teams are distributed across functional areas. Specifically, there currently are:

- "13 National Mission Teams to defend the United States and its interests against cyber attacks";

- "68 Cyber Protection Teams to defend DoD networks and systems against rapidly evolving-threats and technologies in cyberspace";

- "27 Combat Mission Teams to provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations";

- "25 Support Teams to provide analytic and planning support to National Mission and Combat Mission teams"; and

- "14 new CMF Teams created in FY 2022 and FY 2023 to support the Combatant Commanders in Space Operations and for countering cyber influence."[19]

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;[20]
- AFCYBER supplies 39 teams;[21]
- FLTCYBER supplies 40 teams, which reached full operational capability a year ahead of schedule in 2017;[22] and
- MARFORCYBER provides 13 teams.[23]

As of April 2022, according to General Nakasone, Cyber Command had "approximately 6,000 Service members, including National Guard and Reserve personnel on active duty," within its 133 teams" and was expecting to "grow by 14 teams over the next five years."[24]

Recruiting and retaining 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

As noted at the outset of this discussion, the world of cyber operations is notoriously secretive, and much is classified. Thus, analyzing USCYBERCOM's capability as reflected in open-source (unclassified) literature is nearly impossible. However, the United States is viewed as 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 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 by ensuring that U.S. forces can operate in cyberspace without disruption, by making it difficult for enemies to conduct their own operations, and by conducting independent operations against targets as directed to achieve specified goals.

Within DOD, U.S. Cyber Command bears the primary responsibility for the full spectrum of military cyber operations. Having reached its authorized manning levels, USCYBERCOM has shifted its focus to training the force to ensure that it will be as capable as possible in helping to advance and protect the nation's interests.

Endnotes

1. See 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, and 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.
2. Kenneth Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor, statement before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. House of Representatives, March 4, 2020, p. 13, https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-RapuanoK-20200304.pdf (accessed July 26, 2022).
3. 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 July 26, 2022).
4. Crowther, "National Defense and the Cyber Domain," *2018 Index of U.S. Military Strength*, p. 88.
5. 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 July 26, 2022).
6. 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 July 26, 2022).
7. U.S. Cyber Command, "About: Our History," https://www.cybercom.mil/About/History/ (accessed July 26, 2022).
8. 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 July 26, 2022).
9. 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 July 26, 2022).
10. News release, "U.S. Conducts First Hunt Forward Operation in Lithuania," U.S. Cyber Command, Cyber National Mission Force, May 4, 2022, https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/ (accessed July 26, 2022).
11. Stavros Atlamazoglou, "Cyberattacks Quietly Launched by Russia Before Its Invasion of Ukraine May Have Been More Damaging than Intended," *Business Insider*, May 18, 2022, https://www.businessinsider.com/russian-cyberattacks-on-ukraine-may-have-gotten-out-of-hand-2022-5 (accessed July 26, 2022).
12. Yurii Shchyhol, "Vladimir Putin's Ukraine Invasion Is the World's First Full-Scale Cyberwar," Atlantic Council *Ukraine Alert*, June 15, 2022, https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/ accessed July 27, 2022).
13. Ibid.
14. General Paul M. Nakasone, Commander, United States Cyber Command, posture statement before the Committee on Armed Services, U.S. Senate, April 5, 2022, p. 3, https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf (accessed July 26, 2022).
15. U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), *United States Department of Defense Fiscal Year 2023 Budget Request: Defense Budget Overview*, April 2022, p. 2-10, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf (accessed July 26, 2022).
16. U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), *United States Department of Defense Fiscal Year 2022 Budget Request: Defense Budget Overview*, May 2021, p. 3-4, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_Budget_Request_Overview_Book.pdf (accessed July 26, 2022).
17. Nakasone, posture statement before Senate Armed Services Committee, March 25, 2021, p. 4.
18. 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 July 26, 2022).
19. U.S. Department of Defense, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *United States Department of Defense Fiscal Year 2023 Budget Request: Defense Budget Overview*, p. 2-13. Punctuation as in original.
20. 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 July 26, 2022).
21. Tech. Sgt. R. J. Biermann, "Air Force Cyber Mission Force Teams Reach 'Full Operational Capability,'" U.S. Department of Defense, 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 July 26, 2022).
22. 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 July 26, 2022).
23. Biermann, "Air Force Cyber Mission Force Teams Reach 'Full Operational Capability.'"

24. Nakasone, posture statement before Senate Armed Services Committee, April 5, 2022, p. 2.
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 2019, https://www.gao.gov/assets/gao-19-362.pdf (accessed July 26, 2022).