LAWFARE

Cybersecurity & Tech

Cyber Command Needs New Acquisition Authorities

Erica D. Lonergan

Tuesday, May 12, 2020, 8:00 AM

A major force program will help solve the problem.

Personnel of the 624th Operations Center conduct cyber operations in support of the command and control of Air Force network operations and the joint requirements of the Air Force component of Cyber Command. (U.S. Air Force/William Belcher)

In fiscal 2016, Congress granted limited acquisition authorities to U.S. Cyber Command, which sunset in 2021. Given the dynamic nature of the cyberspace environment, the rapidly changing pace of technological development, and the speed at which adversaries operate, Congress should accept the recommendation in the Cyberspace Solarium Commission's March 2020 report to create a major force program (MFP) category for cyberspace as part of the fiscal 2021 National Defense Authorization Act (NDAA). This was among the number of issues I worked on as a senior director on the commission.

The Department of Defense acquisitions process drives how the military builds and equips its fighting forces to achieve strategic priorities set by national leadership, and it is a central element of how the military determines planning, budgeting and procurement. The overall projected budget planning process, called the Future Years Defense Program (FYDP), takes place in five-year intervals and is organized into 12 different MFP categories, each of which represents a combination of the personnel, forces and appropriated funding that together constitute a Defense Department program to achieve certain objectives. How the MFP categories are defined and organized, and which elements within the Pentagon manage the acquisition authorities associated with each MFP category, is important: These issues shape what kinds of capabilities the department can acquire for different missions and purposes.

MFP categories can provide Defense Department entities with enhanced flexibility in acquisitions to meet emergent and unanticipated needs—as well as a seat at the table in working with the services. This is why, in the past, Congress created two distinct MFP categories for special operations and space. These entities currently have independent acquisition authority to acquire goods and services that are unique to their needs. However, for cyberspace, acquisition authorities remain limited.

Major Force Programs Over Time

The MFP concept was originally conceived of in the early 1960s by then-Secretary of Defense Robert McNamara and the "whiz kids" at the Office of the Secretary of Defense. Initially, the Pentagon created 10 MFP categories, ranging from "Research and Development" to "Training, Medical, and Other General Personnel Activities." Since the 1960s, only two additional categories have been created: MFP-11 for U.S. Special Operations Command (SOCOM) in 1987, and MFP-12 for National Security Space in 2016.

When Congress established SOCOM, it established an MFP category for the new unified combatant command as well, granting SOCOM acquisition authorities specific to special operations. Providing SOCOM with acquisition authorities that were independent from the military services effectively made it "service-like"

without creating a new service. It also gave SOCOM greater flexibility and an ability to react rapidly to emergent situations, a particularly important capability for a command operating in environments where unexpected contingencies are likely to arise. SOCOM could directly control resources that were unique to its specific needs—including the capabilities and systems designed for use by special operations forces rather than the services, tailored modifications to capabilities that were originally created for use by the services, or goods and services urgently needed for some developing situation. SOCOM's acquisition authorities became particularly important in the post-9/11 era as the military grew to rely heavily on SOCOM for overseas contingency operations.

The government did not reassess the MFP construct until decades later,when the Commission to Assess United States National Security, Space Management and Organization—established in the 2000 NDAA—recommended the creation of an MFP for space. Initially, the Pentagon used a "virtual" MFP to more easily track space funding—essentially, aggregating program elements related to space—until Congress created MFP-12 for national security space in the fiscal 2016 NDAA. This decision stemmed from a growing concern that nation-state adversaries, particularly Russia and China, were seeking to exploit the U.S. military's reliance on space-based systems. Lawmakers also sought to address concerns about a lack of transparency within Defense Department budgeting for space programs, including the Air Force shifting funds from space to other air power programs. However, while Congress simultaneously established an MFP and a unified combatant command for special operations in the 1980s, the MFP for space *preceded* the creation of the Space Force and U.S. Space Command, which occurred in the fiscal 2020 NDAA.

It is relatively easy to define what resources are peculiar to special operations—like the MH-47G Chinook special operations helicopter, a modified version of the CH-47 Chinook, or the AC-130U gunship, a modified C-130 gunship. But there are inherent challenges associated with defining what "counts" as space-peculiar, as well as cyber-peculiar, goods and services. Space-related assets and functions—such as satellite-based communications or precision navigation and timing systems—are widely dispersed across the services and integrated into numerous military capabilities and systems. The same is true for cyber capabilities. The Defense Department has acknowledged this challenge for space, noting that scoping budgeting in this area "is complicated due to the various classifications and categories." For instance, the fiscal 2020 budget request for MFP-12 does not contain the full scope of space-specific funding, such as funding for personnel.

Moreover, SOCOM usually aims to rely on service-common equipment, modifying capabilities that the services are already acquiring and adapting them to suit their specific needs. However, space and cyber are areas with minimal overlap between service and space- or cyber-specific weapons platforms. It is difficult to imagine

Space Command or Cyber Command defining a need for a hypothetical "modified F-35" for space or cyber missions. This makes appropriations for space- and cyber-peculiar capabilities more difficult. Cyber acquisitions in particular may also not benefit from the economies of scale that come with special forces, service, or even space acquisitions because cyber-peculiar capabilities are unlikely to translate into bulk purchases from contractors. For example, rather than acquiring large numbers of aircraft, cyber acquisitions are likely to involve specific tools and capabilities for defined purposes that cannot necessarily be reused across different target sets and that may become irrelevant as technology changes or the target adapts. Despite these challenges, U.S. Cyber Command would benefit from cyber-peculiar acquisition authorities. The Defense Department's 2018 Cyber Strategy requires an agile and adaptive cyber force that can respond to the dynamic cyber environment and the operational pace of U.S. adversaries. This is in large part what drove Congress to define cyber operations as traditional military activities under Title 10 of the U.S. Code, and the Trump administration to make policy more responsive to offensive cyber operations under National Security Presidential Memorandum-13. The missing piece, however, is comparable flexibility for acquisitions. As with special operations, in cyberspace unanticipated opportunities are likely to arise that may generate requirements for new cyber capabilities or personnel, and the current budgeting process does not have the speed necessary for the acquisitions required.

Current Cyber Acquisition Authorities

While Space Command and the Space Force were established *after* an MFP was created for space, acquisition authorities for cyberspace have lagged behind the organizational maturation of the force. In the fiscal 2015 NDAA, Congress requested that the secretary of defense submit a budget justification display that would include an MFP category for the Cyber Mission Force (CMF), Cyber Command's "action arm." At the time, Cyber Command was a subunified combatant command under U.S. Strategic Command (it was not elevated to a unified combatant command until 2018). Despite this request, in the following year's NDAA—the same act that created a new MFP category for national security space—Congress granted limited acquisition authorities to U.S. Cyber Command. The idea was to first provide Cyber Command with "training wheels"—$75 million in limited acquisition authority through 2021, rather than a blanket MFP—and then assess whether the organization was sufficiently mature to warrant a real MFP.

In 2017 testimony before the House Armed Services Committee, then-Commander of U.S. Cyber Command and Director of the National Security Agency (NSA) Adm. Michael Rogers acknowledged that Cyber Command had not yet used its limited acquisition authorities. Cyber Command's first priority, Rogers testified, was forming partnerships with the private sector—which Cyber Command would

use to acquire defensive capabilities to support the cyber protection teams responsible for defending the Defense Department's networks and, when authorized, critical infrastructure.

In 2018, the Defense Department shifted its strategy to "defend forward." Defend forward posits that to disrupt, deny, and degrade malicious adversary cyber operations and campaigns (particularly in routine competition, below the level of armed attack), ideally before they reach their intended targets, the U.S. must position its cyber forces forward and maneuver where the adversary operates. Following this shift, it is not clear the extent to which Cyber Command has leveraged its new acquisition authorities to acquire offensive capabilities. In March 2019 testimony, Commander of U.S. Cyber Command and Director of the NSA Gen. Paul Nakasone noted that Cyber Command had not managed to completely spend even the relatively small amount of money Congress authorized. At that point, Cyber Command had executed only $44 million of the $75 million appropriated to it and was projected to execute $60-65 million by the end of that fiscal year. It had also filled only six of the 10 personnel positions created to execute these acquisitions.

Cyber Command currently lacks the full acquisition authorities of Space Command, which would make it "service-like." But the NSA serves important "service-like" functions because it possesses an independent ability to acquire goods and services. Under the dual-hat structure, the NSA and Cyber Command are jointly headed by the same individual; what is more, the NSA plays the role of combat support agency. This allows Cyber Command to benefit *indirectly* from the NSA's independent ability to acquire tools, capabilities, infrastructure and personnel—even though neither organization can use its own funds to support the other.

Nevertheless, this relationship may not last forever. Congress has tasked the Defense Department with providing updates on whether specific benchmarks have been met that would warrant splitting the dual-hat structure (although it is not clear if or when this will occur). If the objective is to cultivate Cyber Command to become a more robust, mature and, ultimately, independent organization such that it can safely be separated from the NSA, then granting Cyber Command cyber-peculiar acquisition authorities is an important component of that process.

Creating an MFP-13 for U.S. Cyber Command

With the sunsetting of Cyber Command's limited acquisition authorities in 2021, the time is ripe to establish an MFP. Creating an MFP for Cyber Command would enable the organization to more rapidly field and acquire cutting-edge capabilities, consistent with the operational demands posed by implementing a strategy of defend forward and the evolving nature of the cyber domain. At the most basic level, an MFP would allow Cyber Command to quickly meet emergent needs for

novel tools and capabilities, even for relatively small purchase quantities. Unlike special forces, which typically relies on modifications to capabilities the services are already acquiring, Cyber Command would likely seek to rapidly acquire new and innovative capabilities—including commercial off-the-shelf capabilities outside of traditional acquisitions sources—as well as the development of interoperable toolkits across the services. Furthermore, capabilities may include not only pure "cyber tools" but also the broader set of capabilities that support offensive and defensive missions, such as personas, infrastructure, and licensing (for example, host-based cloud services), as well as investment in research and development.

This more comprehensive conception is consistent with how Nakasone defined "cyber-peculiar" goods and services in his 2019 testimony. According to Cyber Command, such goods and services include "[a]ny acquisition effort that supports or facilitates any of the three Cyberspace Missions as defined in Joint Pub 3-12; Offensive Cyber Operations, Defensive Cyber Operations, or Department of Defense Information Network operation."

These acquisition authorities could also support unanticipated costs that emerge from "hunt forward" efforts—that is, threat hunting on allied and partner networks to enable early warning and assist host nations with local defensive efforts. This could include, for instance, providing resources to deploy sensors or harden network defenses of allies and partners at the geographically forward edge of the defend forward strategy.

Cyber-peculiar acquisition authorities would also extend beyond capabilities to include services and personnel, similar to the MFPs for special forces and space (notwithstanding the fact that the 2020 budget request for space did not include military personnel). There is already a growing recognition that the CMF may not be appropriately sized and organized to implement the diverse set of missions for which it is responsible. For this reason, the Cyberspace Solarium Commission recommended that Congress should direct the Defense Department to conduct a force structure assessment of the CMF. An MFP category for Cyber Command, which the commission also recommended, complements the force structure assessment recommendation: It could facilitate Cyber Command in contracting to fill gaps in specialty skills, consulting services and staff augmentation.

Finally, these acquisition authorities would give Cyber Command a seat at the table in resolving funding disputes with the services. Cyber Command already relies on the services to a significant extent because a hefty portion of its funding collectively stems from the individual services, whose components feed into the 133 CMF teams. Nakasone testified in 2019 that, from the $9.6 billion for cyber

included in the president's 2020 budget request to Congress, only 6 percent was allocated to U.S. Cyber Command headquarters, and, of the $1.9 billion requested for infrastructure, 87 percent was allocated to the services.

Establishing an MFP funding category for Cyber Command would be a significant undertaking. Perhaps the most obvious question to ask before beginning this work is why Congress should establish an MFP for Cyber Command when the command has not demonstrated convincingly that it has fully taken advantage of even limited acquisition authorities. There is an intuitive logic to taking a "crawl, walk, run" approach to granting acquisition authorities—but such a narrowly scoped and constrained "test" should not be held up as a validation of how Cyber Command would perform with a true MFP category. Space, for instance, was not "tested" in the same fashion, despite the organizational infrastructure being far less mature than cyber—although it did take nearly 16 years for the formal creation of an MFP category for national security space.

More importantly, the United States needs to match its strategic and operational objectives with the appropriate organizations, resources, processes and authorities to implement them. If the strategy of defend forward demands an agile force that can maneuver and adapt in a fast-paced environment (in terms of both evolving adversary approaches as well as changing technology), then that force needs to be able to acquire goods and services to fulfill those requirements.

That said, Cyber Command will need to substantially grow its acquisitions organization and staff to effectively implement this, just as Special Operations Command had to do. An additional challenge will be clearly defining what constitutes "cyber-peculiar" versus "service-common" goods and services—a challenge that is similarly salient for space.

While the Cyberspace Solarium Commission, following its remit from Congress, focused on the more specific issue of an MFP for Cyber Command, it is also worth assessing the extent to which the broader MFP construct—hardly altered since the 1960s—should be reexamined in terms of its appropriateness for the contemporary needs of the military. For instance, some of the 12 different MFP categories may appear antiquated or mismatched to the current organization of U.S. forces. While Special Operations Command, which is only a single combatant command, has a separately defined MFP category, the entirety of the services fall under one MFP (termed MFP-2 "General Purpose Forces"). In another example, the MFP-3 category encompasses "Command, Control, Communications, Intelligence, and Space"; yet, with the newly created MFP-12 for national security space, defining the distinctions among these components is ambiguous on its face. Adapting the acquisitions process for current and anticipated future strategic needs, particularly for highly technical environments, is essential for sustaining the modern military force.

Erica D. Lonergan

@eborghard

Read More

Dr. Erica Lonergan (nee Borghard) is an Assistant Professor in the Army Cyber Institute. She is also a Research Scholar in the Saltzman Institute of War and Peace Studies at Columbia University. Prior to that, she held positions as a senior fellow at the Carnegie Endowment for International Peace and the Atlantic Council. Previously, Erica served as a Senior Director on the U.S. Cyberspace Solarium Commission. Erica also held an appointment as a Council on Foreign Relations International Affairs Fellow, with placement at JPMorgan Chase and US Cyber Command, and has served as an Assistant Professor and Executive Director of the Rupert H. Johnson Grand Strategy Program in the Department of Social Sciences at West Point. Erica received her PhD in Political Science from Columbia University. She is a term member at the Council on Foreign Relations. The views expressed are personal and do not reflect the policy or position of any U.S. government organization or entity.