Financial Stewardship in the Land of "1's and 0's"

Brigadier General Kenneth D. Hubbard
Major Jared Nystrom

ABSTRACT

Budget processes supporting cyberspace operations are uniquely challenged due to their dispersal within Department of Defense (DoD) Services and agencies. This budgetary structure fails to provide the visibility needed to analyze and report on cyberspace investments. Furthermore, this structure fails to provide the resolution, with a high level of confidence, on how the DoD executes money in support of cyberspace operations. Establishing a budgetary process similar to that employed by special operations would synchronize and integrate funding activities to operational functions and tasks. This includes the creation of a cyberspace Major Force Program (MFP) that would provide cyberspace budget lines throughout the department. These proposals would create a budgetary structure that could best serve the unique requirements demanded in cyberspace. Doing so would act to acknowledge the cyberspace domain as a separate environment integrated across all Services.

The diffuse nature of the military cyber budget presents the Department of Defense (DoD) with a challenge for effective budgetary management; DoD must develop a new method for managing cross-program funding to improve mission effectiveness and achieve management efficiencies.[1] Cyberspace is not unique among warfighting domains in that operational readiness is dependent upon the timely execution of a balanced program of resources tied to valid requirements. The DoD budgetary structures have kept pace with the explosive growth in cyberspace; however, the resulting system fails to provide the visibility needed to analyze and report on cyberspace investments. Aligning cyberspace budgetary processes to better support operations would provide increased transparency and improve force readiness by synchronizing capability development across the DoD.

Brigadier General Kenneth D. Hubbard currently serves as Director of Resource Management for 3rd Army ARCENT G8, and previously served as the Director, Capability and Resource Integration J8, United States Cyber Command. He is the son of a career Army officer and a 1986 graduate of the South Carolina State Army ROTC Program. His assignments include the Director for Resource Management (G8), IMCOM; the Director of the Army Budget's Operations and Support Directorate; USFOR-A J8 while assigned as the V Corps G8, Operation Enduring Freedom, Afghanistan; Division G8 (Comptroller) for 1st Infantry Division; MNSTC-I G8, Operation Iraqi Freedom, Iraq; Contingency Operations Budget Analyst, Army Budget Office; and Defense Resource Manager, J8, Joint Chiefs of Staff. BG Hubbard is a graduate of the Industrial College of the Armed Forces and Air Command and Staff College. He holds graduate degrees from Syracuse University and the National Defense University.

Every DoD Service and agency submits an annual budget estimate in order to build the overall DoD budget, which is then provided as part of the President's Budget (PB) request to Congress.[2] This budget is a detailed forecast of the next two-year's financial execution developed in accordance with fiscal programming guidelines, as well as assessments of on-going programs.[3] It aligns with Congressional appropriations, and includes justifications to provide transparency regarding the investment of taxpayer dollars in defense programs. Programs within the defense budget are organized into Major Force Programs (MFP), which aggregate program elements that reflect a force or support mission and contain the resources necessary to achieve an objective or plan.[4] Currently, cyberspace operations are not organized within an MFP, with budget lines diffused within the financial records of individual Services and agencies. Budget analysts and staffers must manually correlate cyberspace efforts across multiple, disparate budget estimates to gain a basic understanding of how funds are being invested.

The lack of oversight of cyberspace resource planning, programming and budgeting have consistently been a contentious issue since the establishment of U.S. Cyber Command (USCYBERCOM) as a sub-unified command. During the 2010 confirenate Armed Services Committee characterized this lack of oversight as well-known within the Federal Government.[5] Furthermore, the Congressional language during this time-period describes the issue as fragmented within the DoD, the executive branch as a whole, and within Congress.[6] Initial attempts to provide a unified budget drew upon authorities granted to the DoD Chief Information Officer (CIO) within the Information Technology Management Reform Act. Also known as the Clinger-Cohen Act,

Major Jared Nystrom is an Operations Research and Systems Analyst (ORSA) Officer assigned to J8, United States Cyber Command. He is a graduate of Tulane University ROTC where he received Bachelor's Degrees in Economics and Psychology and commissioned into Military Intelligence (MI) detailed to Armor. He previously served in both the 2nd and 14th Cavalry Regiments and commanded B Company, 532nd MI Battalion, Republic of Korea. He holds a Master's degree from the Air Force Institute of Technology (AFIT) and will return this fall to pursue a Ph.D. in Operations Research.

this legislation was signed into law as part of the 1996 National Defense Authorization Act (NDAA).[7] This law improved the methods used by all Federal agencies to acquire, use, and dispose of Information Technology (IT) by leveraging enterprise solutions,[8] and was later established in policy through the Office of Management and Budget Circular A-11.[9] The Clinger-Cohen Act charges the DoD CIO with the responsibility for reviewing and providing recommendations to the Secretary of Defense (SecDef) on budget requirements for IT and national security systems.[10] Although initially conceived to handle business operations IT, the authorities granted in the Clinger-Cohen Act were later attributed to cyberspace operations to include both offensive and defensive capabilities.[11] The current budgetary framework developed organically through this process. This extrapolation of authorities from business support IT to operational cyber mission forces results in a system ineffective in developing and providing oversight of a cyberspace budget across the Services and Joint Forces. This introduces potential risk to force readiness due to a lack of synchronization of development amongst Services, and the inability to function as a combined joint force.

A brief history of the US special operations offers insight into the effective application of military operations resourcing within a nascent command. The U.S. Special Operations Command (SOCOM) possesses unique Service-like authorities for funding and accounting. To explain this unprecedented authority, Charles G. Cogan provides a contemporary perspective as chief of the Near East and South Asia Division in the Directorate of Operations of the Central Intelligence Agency between mid-1979 and mid-1984.[12] Cogan assesses the capability gaps following the failure at "Desert

One" as well as the articulation of intent behind the Cohen-Nunn Act that consolidated Special Operations under SOCOM.[13] In April 1980, the United States military suffered a humiliating defeat during the failed attempt to rescue 53 Americans during the Iranian hostage crisis. The multiple setbacks at Dasht-e-Kavir, also known as "Desert One"[14] resulted in the failure of Operation *Eagle Claw,* and tragically the death of eight American service members.[15]

Following an internal investigation, chaired by Admiral James L. Holloway, the DoD established a Counterterrorist Joint Task Force (CTJTF) in 1980 as a field agency of the Joint Chiefs of Staff (JCS) to consolidate advocacy for special operations.[16] Congress later took a more significant role in the organization of Special Operations, culminating with the passage of Public Law (PL) 99-661 in 1986.[17] Section 1311 of this legislation adds Section 167, Title 10, which formally established SOCOM as a four-star unified command tasked to prepare special operations forces to carry out assigned missions.[18] Furthermore, this legislation directed the SecDef to appoint an Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD(SOLIC)), and create a new major force program (MFP) category 11 for the DoD Five-Year Defense Plan.[19] The Congress tasked the ASD(SO/LIC) to prepare and justify program recommendations for the newly minted MFP, and restricted the authority to the SecDef for any reprogramming of special forces operations.[20] Comparatively, the cyberspace domain requires this level of oversight and authority to properly execute resources.

The establishment of Special Operations Forces (SOF) MFP 11, managed by the AS (SO/LIC), provides clear traceability of resources from the Congress directly to the SOF community. Programs organized under an MFP allow a more precise articulation of investments, facilitating immediate identification of resources assigned to a particular activity or capability regardless of Service. Through this system, Congress can control funding to individual MFPs, allowing prioritization and preservation of joint capability and capacity during periods of budget scarcity.

The DoD should seek to optimize resourcing of cyberspace operations, versus the current CIO-driven model where each Service and agency resources and manages cyber capabilities independently. This current model results in a 'cottage industry' of cyberspace capabilities not only hindered by redundant efforts but also results in unaddressed capability gaps. The responsibilities given to DoD CIO to budget cybersecurity do not provide the controls or necessary authority to manage cyber resources. This responsibility results in DoD CIO attempting to report on what they believe the Services and agencies are spending on cybersecurity based upon loose reporting guidance and layers of independent organizational staff providing budget justifications.

The Office of the Under Secretary of Defense Comptroller (OUSD(C)) and the Office of the Secretary of Defense Cost Assessment and Program Evaluation (CAPE) are the two

primary offices at the OSD level for providing oversight of the DoD budget and the Program Objective Memorandum (POM). The OUSD(C) provides support to the DoD CIO through the Office of Investment Programs Directorate. This directorate oversees billion-dollar programs, but cyberspace requires funding for million-dollar programs, an order of magnitude less, making oversight of these programs a lower priority for the Investment Programs Directorate and OUSD(C). The CAPE has limited personnel dedicated to a cyberspace program across the five-year Fiscal Year Defense Program (FYDP). A dedicated office with a focus on relatively small appropriations may provide greater efficiencies. A more robust effort would assist DoD in long-range planning and programming of cyber requirements. In conjunction with the Principal Cyber Advisor (PCA), OSD Policy, CAPE could better align cyber functions, increase transparency, and synchronize efforts amongst the Services and optimize acquisition processes. This effort will create efficiencies and improve mission effectiveness.

This article offers the following recommendations towards improving cyberspace operations budgetary processes and management.

- Creation of a cyberspace MFP to ensure required resourcing is available to execute critical domain-specific missions, similar to the recognition of special operations. An MFP allows proper pairing of resources to requirements, facilitating a rapid pace of capability development required within cyberspace. An MFP provides the necessary transparency in cyberspace investments to Congress. Furthermore, an MFP protects resources intended for critical cyberspace capability and capacity during periods of budget scarcity, rather than risk diversion of those resources towards priorities internal to Services and agencies.
- Elevate the PCA to a comparable position to the Assistant Secretary of Defense in line with the roles and authorities for the ASD(SOLIC). The PCA should develop the annual and long-range strategic plan for cyberspace development. This also facilitates proper implementation and oversight of a cyber MFP, consolidated within an office armed with proper resource management and acquisition expertise. An elevated PCA also enables DoD CIO to focus exclusively on DoD's information enterprise and business IT solutions versus cyberspace operational capability, as was the original intent behind current policies.
- Cyberspace operations require a dedicated Joint Staff element to ensure the personnel readiness, policy, planning, and training of the Cyber Mission Force. This Joint Staff element would also act in a military advisory capacity for the PCA. Placing this capability within the Joint Staff facilitates coordination across all combatant commands, and allow better integration of cyberspace forces in support of Chairman of the Joint Chiefs of Staff priorities.

Under the current model, the DoD does not have the resolution to provide, with a high level of confidence, how money is being executed in support of cyberspace operations. We recommend creating a budgetary oversight process outside of CIO to improve clarity and control. If implemented, the recommendations in this paper would produce a budgetary structure that could best serve the unique requirements demanded in cyberspace. Doing so would acknowledge the cyberspace domain as a separate environment that is integrated across all Services. The ability to focus resources on the most critical cyber threats and provide the optimum solutions across all Services is necessary to derail future hazards.

NOTES

1. Ashton Carter, The Department of Defense Cyber Strategy. Washington D.C.: Department of Defense, 2015.

2. DoD Directive 7045.14. "The Planning, Programming, Budgeting, and Execution (PPBE) Process." Washington D.C.: Government Printing Office, 2013.

3. Ibid.

4. Defense Acquisition University. n.d., April 9, 2018, https://dap.dau.mil/glossary/pages/2192.aspx.

5. U.S. Senate. (2010). Nominations before the Senate Armed Services Committee, Second Session, 111th Congress. Washington D.C.: Government Publishing Office.

6. Ibid.

7. U.S. Congress. (1996). Clinger Cohen Act of 1996. Washington D.C.: Government Publishing Office.

8. Ibid.

9. Office of Management and Budget (OMB) (2000). Circular A-11. Washington D.C.: Government Publishing Office.

10. U.S. Congress. (1996). Clinger Cohen Act of 1996. Washington D.C.: Government Publishing Office.

11. DoD Manual 7000.14-R. (2015). DoD Financial Management Regulation Volume 2B. Washington D.C.: Government Publishing Office.

12. Charles Cogan, "Desert One and its disorders." The Journal of Military History 67, no. 1 (2003), 201.

13. Ibid.

14. Ibid., 211.

15. Ibid., 211.

16. Ibid., 214.

17. Ibid., 2151.

18. U.S. Congress. (1996). Clinger Cohen Act of 1996. Washington D.C.: Government Publishing Office.

19. Ibid.

20. Ibid.