Beyond Binaries: Cyber Force Generation and the SOCOM-like Model

Description

This article is part of Project Cyber, which explores and characterizes the myriad threats facing the United States and its allies in cyberspace, the information environment, and conventional and irregular spaces. Please contact us if you would like to propose an article, podcast, or event environment. We invite you to contribute to the discussion, explore the difficult questions, and help.

United States Cyber Commandâ??s need to identify, train, and retain personnel has grown alongside its mission set, which includes everything from ransomware defense and election security to preparing for potential contingencies with Americaâ??s â??pacing threat.â?• Yet, Cyber Command does not control the recruitment, professional development, or retention incentives of the military service members selected to fight in the cyber domain. Instead, the individual military services (Army, Navy, Marines, Air Force, and Space Force) are responsible for force generation and readiness. Over time, as General (Retired) Paul N. Nakasone stated, US Cyber Command has tried to â??build its authorities much in the same way Special Operations Command did.â?• More recently, the Pentagonâ??s inaugural Assistant Secretary of Defense for Cyber Policy, Honorable Michael Sulmeyer, testified that â??a range of options should be consideredâ?• to address current cyber force readiness challenges, â??including extending aspects of the US Special Operations Command [(SOCOM)] model to US Cyber Command.â?• This perspective reflects a consensus among several senior leaders that special operations should inform how the US military organizes itself to generate forcesâ??the process of recruiting, training, and retaining personnelâ??for cyberspace operations. As far back as 2016, senior leaders have drawn similarities between cyber and special operations, noting how success in both types of operations requires prioritizing a highly specialized workforce. However, the cyber-special operations analogy is problematic, largely because it is rooted in uninterrogated assumptions.

Despite the popularity of modeling Cyber Command after Special Operations Command among senior leaders, there is no consensus on what a â??SOCOM-like modelâ?• is or how it could solve the problems plaguing the cyber mission force. Cyber Command has not formally defined the â??SOCOM-like modelâ?• concept or explained why it considers that model superior to alternative organizational structures for force generation in cyberspace, like establishing an independent service. Despite lacking a coherent and consistent definition, proponents of adopting a SOCOM-like model for cyberspace insist that it is more effective, more efficient, simpler to implement, and less disruptive than creating a

Cyber Service. However, policymakers should not forge ahead with implementing a SOCOM-like model before evaluating its implications for cyberspace. Moreover, unexplored solutions, such as a hybrid approach to force generation combining elements of an independent service with implementing a SOCOM-like model, may yield the best and most realistic approach to improve cyber readiness. Regardless, the conversation surrounding Cyber Commandâ??s force structure is too immature to become anchored on any given solution.

https://irregularwarfareinsider.podbean.com/

We aim to further the discussion on force generation for the cyber domain in two ways: first, by presenting likely manning practices and their associated challenges that may arise within a SOCOM-like model, and second, by highlighting why the choice between a SOCOM-like model and a Cyber Service is a false binary. We do not attempt to authoritatively define or comprehensively analyze what a SOCOM-like model is, nor advocate for one approach over another. Instead, we focus on defining possible implementations of a SOCOM-like model for cyberspace to illuminate assumptions that may be false, inaccurate, or under-analyzed. Ultimately, our analysis shows the need to advance the conversation surrounding cyber force generation beyond theory to discuss implementation *before* fully embracing any one model. Only then can we understand the implications of a force generation model for the cyber domain, discover creative solutions, and move forward on a course grounded in realistic and informed assumptions.

What is a SOCOM-like Model?

To evaluate a SOCOM-like model for cyber force generation, we need to start from a common understanding of the force generation process for special operations personnel. For Special Operations Command, force generation begins with the individual services, each responsible for recruiting personnel and providing them with initial entry training. Then, the services assess, select, and train prospective special operators through extensive service-specific courses like the Armyâ??s Special Forces Qualification Course or the Navyâ??s Basic Underwater Demolitions/SEAL training. Special Operations Command conducts specialized training and then presents these highly-trained units to the Geographic Combatant Commands. For the most part, special operations personnel remain managed by their respective services, but in some cases Special Operations Command may provide unique administrative support structures. For example, the Command may provide further advanced training beyond the initial training provided by the services, which is designed to support the distinct needs of the special operations community and mission.

It is reasonable to assume that Cyber Command already relies on a SOCOM-like model for force generation. Similar to Special Operations Command, Cyber Command depends upon each of the services to generate and present forces to the command. However, that assumption is false. Senior leaders have indicated the Department of Defense is still evaluating the suitability of a SOCOM-like model for Cyber Command, implying that such a model has not yet been fully implemented. Additionally, Cyber Commandâ??s service like authorities regarding the cyber mission forcesâ??such as elevation to Combatant Command, enhanced budgetary control, the creation of an Assistant Secretary of Defense for Cyber Policy, and updating the Unified Command Plan to name Cyber Command as the Joint Force Provider and Joint Force Trainerâ??are only now coming into effect. Even though Cyber Command has yet to publicly define how it will use many of its new authorities, leaders have alluded to policies regarding personnel and assignments that draw from the SOCOM model.

Critically, the assumption that Cyber Command already uses a SOCOM-like model raises a second related assumption: that Cyber Command has already completed the analysis to support the implementation of a SOCOM-like model. Unfortunately, inconsistent or unspecified definitions of what a SOCOM-like model entails, coupled with the assumption that the model is an effective approach to force generation, have undermined any meaningful analysis of the model itself and stymied productive conversations about what cyber force generation could and should look like. In reality, Special Operations Command is far from perfect and faces several similar force generation challenges and inefficiencies that Cyber Command is trying to overcome. For example, because special operations forces, like cyber forces, are segregated in their training and resourcing and have a distinct chain of command, it remains challenging to integrate special operations with other military operations. Ultimately, leaders are advocating for the SOCOM-like model *before* it has been evaluated for effectiveness and without any analysis of its outcomes or how it will improve Cyber Commandâ??s overall force readiness.

Challenges with the SOCOM-like Model

The significant challenges associated with the SOCOM model itself are often overlooked when comparing cyberspace and special operations. For example, a 2020 review of Special Operations Command revealed a number of force generation challenges and potentially incompatible practices that also occur in Cyber Command. First, Special Operations Command units consistently sustain a high operational tempo, which places force readiness at risk. The result is that already undermanned formations often experience increased medical, training, and retention problems. Second, service members in Special Operations Command are still beholden to industrial era Departmental policies and service behaviors. Individuals are promoted by and receive incentive pay from their respective military services, meaning a soldier and sailor of equivalent rank and skill could be promoted differently, receive different incentive pay for their service or have different retention bonus options. Service members assigned to Cyber Command experience similar talent management problems, such as incentive and retention pay discrepancies between servicesâ??or even within a single service. Moreover, the service components and Special Operations Command do not always agree on priorities, leading to tensions that can impact service members and their careers. Similar practices have also proven inadequate and inequitable for the cyber force. Consequently, Special Operations Command struggles with maintaining high standards and service fundamentals in its selection and training pipelinesâ??an issue that Cyber Command confronts.

That said, the SOCOM-like model presents some positive practices relevant to cyberspace. One example is implementing a selection process. Special Operations Command relies on the services to uphold a rigorous and highly selective assessment process to maintain the quality of special operations personnel. Meanwhile, the services currently assign personnel to units and positions in Cyber Command without an assessment process or qualification course. The result is Cyber Commandâ??s ongoing struggle with the quality, consistency, and operational effectiveness of the forces it receives from the services.

However, if Cyber Command were to implement a SOCOM-like assessment and selection process, it would have to accept the necessary attrition rate such a process would inevitably incurâ??which could be up to 75% for some special forces training and qualification courses, resulting in an overall average 52% attrition rate across all of its elements, or approximately 80% when assessing individuals prior to completing their initial military training. Assuming these attrition rates and consistent quality of recruits, one service must attract five recruits to fill a single special forces billet. Extending this logic to cyberspace, for Cyber Command to adopt a SOCOM-like model, it should expect similar or greater attrition rates and, therefore, require a significant increase in recruits. Given the recruitment challenges the services already face in cyberspace (not to mention more broadly), it is unclear how they would fulfill an even greater recruitment demand. Furthermore, each service would have to adjust its recruitment practices, goals, and training pipelines to meet Cyber Commandâ??s needs. Importantly, unlike Special Operations Command, whose ideal recruit profile (i.e., physically fit, leadership attributes, and mental agility, among others) is also an ideal candidate for the conventional force, Cyber Commandâ??s ideal recruit profile may not align with what the services need to perform their domain-specific warfighting functions and tasks. Education in, or a deep affinity for, computer science and engineering are not necessary for a person to fire a rifle but are fundamental requirements to become an interactive on-net operator. The question then becomes how the services could, or should, adjust their recruiting practices and initial entry requirements to meet the unique demands of Cyber Command and if they would even be willing to do so. Regardless, there is the possibility that each service would be faced with making drastic and disruptive changes, on the one hand, or risk continuing to fail to meet their force generation obligations and leaving the cyber mission forces hollow, on the other hand.

Ultimately, implementing any new force generation model will pose challenges. However, the perceived effectiveness of the SOCOM model should not immediately qualify it as the optimal solution for Cyber Command. Some of the challenges associated with a SOCOM-like model could exacerbate existing cyber force generation issues rather than solve them.

Moving Past False Dichotomies

Another common assumption is that the SOCOM-like model and the creation of a new, independent service to generate forces for cyberspace are mutually exclusive courses of action. However, this is a false binary. Many of the changes necessary to generate cyber forces of sufficient quality and quantity will distract or place a significant burden on the services. It would be more efficient and less disruptive if each service only provided Cyber Command with personnel whose work roles also have value in their organic service formations. In that case, a SOCOM-like model would necessitate a new or existing service focused on cyberspace, which would be established or designated to generate forces for Cyber Command and the remaining cyber-related work roles that do not align with the existing servicesâ?? needs. This action would allow the existing services to avoid the training and doctrinal burdens of providing forces unique to Cyber Command-aligned units. It would also guard the services from compromising standards or sacrificing cyber competencies in pursuit of efficiency. Furthermore, it would enable Cyber Command to uphold a high standard and more freely evolve its requirements without necessitating changes from all services. Although rarely discussed, this option could avoid the near-term disruptions of a new cyber service without hindering a strategy for long-term domain dominance.

Looking Ahead

For the Cyber Mission Force to meet growing demands and compete with China and Russia in the cyber domain, it must be developed and institutionalized to protect it from becoming a marginalized asset. Special operations forces escaped becoming marginalized by the conventional forces and broader US military community, and an analogy with the evolution of Special Operations Command does offer a possible (though not necessarily complete) model for the future of cyber force generation. Special Operations Command succeeded with a new organizational home, high-level advocacy, and secure funding. These three elements would also be extremely beneficial in overcoming the challenges now faced by Cyber Command. However, while those lessons are important, the cries for Cyber

Command to adopt a SOCOM-like model for force generation rely on the perceived successes of Special Operations Command while ignoring its shortcomingsâ??both the SOCOM model itself and its application to cyberspace. In many ways, operational outcomes and mission accomplishments have overshadowed or allowed the force generation issues within the special operations community to be overlooked and underappreciated. Like any organization, Cyber Command tries to succeed and protect its equities and has also sought to highlight its high operational tempo as an operational achievementâ??if the command is busy, it must mean it is doing something right. But showcasing busy teams is a diversion from Cyber Commandâ??s manning shortfalls, training backlogs, and dismal force readiness levels.

Cyber Command is reaching an inflection point in force generation. Chinese cyber actors are actively compromising US critical infrastructure to preposition capabilities in the event of a crisis or contingency involving the United States, potentially over Taiwan. Congress has granted Cyber Command significant service-like authorities to counteract such threats. Meanwhile, the debate about the best path to improve cyber force generation has largely become reified between a yet-to-be-defined SOCOM-informed solution or the standup of an entirely new service. The essential role cyberspace plays as an independent domain of warfare and a warfighting enabler across other domains means that how the United States generates cyber forces will have significant national security implications. Now is the time to take bold, impactful actions and consider significant improvements to improve the cyber forcesâ?? readiness to face potential adversaries. Cyber Command needs to drive this process by defining the characteristics and practices it seeks to adopt or avoid. More importantly, the Command should define its force generation goals and specify how they will enable the United States to deter or, if necessary, defeat its pacing threat. Fundamentally, a SOCOM-like model should not be assumed to be the easiest, most effective, most efficient, or least disruptive solution until properly defined. Paradoxically, the model will likely be defined by its implementation plan. Therefore, the conversation must progress toward specific changes and analysis of their second and third-order effects. For proponents of a SOCOM-like model, an independent cyber service, or some combination of the two, uncovering what the *CYBERCOM-like model* is will require putting in the work.

MAJ Skylar Onken spent 11 years active duty conducting intelligence and offensive cyber operations. He is now a U.S. Army Reservist and co-founder at Twenty.

MAJ Nick Starck is an active duty U.S. Army cyber officer with a background in defensive cyber operations. He has served in operational roles as a signal and cyber officer and researcher at the Army Cyber Institute at West Point.

MAJ JC Fernandes is an active duty US Army cyber officer and researcher at the Army Cyber Institute at West Point who has experience conducting defensive cyber operations. He was initially *commissioned as an infantry officer and served with the 173rd IBCT(A).*

Erica D. Lonergan, Ph.D. is an Assistant Professor in the School of International and Public Affairs at the Columbia University. She previously served as a Senior Director on the Cyberspace Solarium Commission.

MAJ Maggie Smith, Ph.D. is an active duty U.S. Army cyber officer with a background in offensive cyber operations. She is currently the Co-Director of IWIâ??s Cyber Project and is a Senior Nonresident Fellow at the Atlantic Council.

LTC Todd Arnold, Ph.D. is an active duty U.S. Army cyber officer and currently serves as a research team lead at the Army Cyber Institute at West Point.

The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

Main Image: Sgt. James Hyman, Expeditionary CEMA operator for the 11th Cyber Battalionâ??s Expeditionary Cyber-Electromagnetic Activities Team-01 (photo by Steven Stover)

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Date Created
2024/11/07