Chance and Necessity: Evolving the Supporting Role of SOF to Cyber Operations

Description

Introduction

> â??Evolution is driven by chance and necessity.â?•

This was the mantra of Nobel Prize winner Jacques Monod. While Monod was primarily known for his work as a French biologist and philosopher, he also served as Chief of Staff for Operations for the French resistance organization, the Forces FranÃ§aises de lâ??Interieur, during the Second World War. A true Renaissance man, he was equally adept at both exploring the field of enzymology and conducting railroad bombings. Monodâ??s evolutionary principle applies seamlessly to both protein enzymes and irregular warfare, as it offers a useful analytical lens for understanding the adaptation of military organizations to the evolving character of warfare.

The most obvious recent example of chance and necessity colliding on the battlefield is the explosive expansion of attritable drones in the Ukrainian conflict. The Ukrainian civilian sectorâ??s ability to rapidly develop, produce, integrate, and field swarms of quadcopters and other unmanned systems was met with the necessity of defending its sovereignty against Russian aggression.

However, a less observable, but equally significant aspect of this combat evolution was the role that cyber operations played in the opening days of the invasion, blunting the effectiveness of Russian tactics. American companies, including Microsoft and Palo Alto Networks, provided vital cyber defense capabilities. These efforts protected critical infrastructure from Russian hackers and enabled greater command and control (C2) of the Ukrainian counteroffensive. Simultaneously, Starlink has fielded over 50,000 high-speed, resilient satellite data terminals to the Ukrainian front lines, providing unparalleled data transport capabilities that even Russian forces cannot rival. Starlinkâ??s capabilities have been so effective that it has been called â??â?¦the essential backbone of communicationsâ?• for the Ukrainian Ministry of Defense. Ukrainian tactical units have even adapted the Low Earth Orbit technology to control attack drones. These successes make evident the importance of cyber capabilities and technology to achieve strategic security objectives.

Concurrently, United States Special Operations Command (USSOCOM) now finds itself at a similar inflection point following decades focused on counterterrorism. Indeed, in 2022, Lt Gen Jim Slife, former Air Force Special Operations Command (AFSOC) Commander, stated, â??AFSOC is at its third strategic inflection point. We have toâ?¦ respond to crises on behalf of the nation on short notice anywhere around the globe and maintain pressure on counter-violent extremist organizations. We have to be prepared for conflict with peer adversaries in contested environments, and we have to compete strategically with global competitorsâ?¦â?•

Against this backdrop, what should the next evolution of SOF become? Where can USSOF be most relevant in strategic competition? The cyberspace domain provides opportunities for SOF to apply its problem solving and innovation in new ways, and Microsoft, Palo Alto Networks, and Starlinkâ??s successes in Ukraine demonstrate an opportunity for a significantly high return on investment.

Background: The Current State of Cyberspace

The Department of War continues to face longstanding deficiencies in cyberspace. According to *War on the Rocks*, United States Cyber Command (USCYBERCOM) has encountered difficulties in developing and retaining qualified cyberspace operators, hindering its ability to sustain force generation. In â??*The Sad and Sorry Tale of Cyber Commandâ??s Seven-Year Failure*,â?• Aden McGee explains that this failure is attributable to organizational confusion, service parochialism, and deficiencies in processes and culture. Ultimately, this situation results in the deployment of significantly fewer offensive and defensive cyberspace operation forces than necessary, thereby impairing the overall effectiveness of US forces in cyberspace.

Recognizing that in the modern era, cyberspace operations serve as both a prerequisite for and an enabler of follow-on kinetic operations, USSOF are uniquely positioned to address certain aspects of network operations that have proven difficult for conventional forces. These aspects might include gaining physical access to isolated networks, bolstering the network defense capabilities of allies and partners in politically sensitive areas, or simply increasing data-centric C2 capabilities for partner forces across all domains.

Integration of cyberspace operations within USSOF is not unprecedented. LTG Braga, then United States Army Special Operations Command (USASOC) Commanding General, and now commanding Joint Special Operations Command, introduced the SOF-Space-Cyber triad as one of USASOCâ??s key priorities for future modernization efforts. He described the triadâ??s relationship between special operations, the space domain, and the cyber domain as â??a convergence of trans-regional, multi-domain, and joint capabilities to exponentially increase the holistic strategic effects of each capability across the spectrum of conflict now and in the future.â?• This convergence is the result of both necessity and chanceâ??the necessity of integrating non-kinetic capabilities to remain effective below the threshold of open conflict and the chance to exploit unique opportunities in domains where conventional forces face structural constraints.

SOF Support to Cyber Operations

As USSOCOMâ??s evolution reaches an inflection point, adding support to cyber operations as a core activity becomes important to enhance the effectiveness of integrating cyber and technology in national power. Support to cyber could consist of four distinct pursuits: strengthening relationships with industry; streamlining coordination with interagency cyber counterparts; modernizing security assistance to include cyber operations; and leveraging SOF as a testbed for cyber technology for the wider force. This approach shows how SOF can support cyber and also integrate it into traditional SOF mission sets.

Firstly, USSOCOM must strengthen its relationships and efforts in the cyber domain, specifically with civilian commercial and non-military organizations. The SOF community already enjoys organizational relationships with USCYBERCOM, the intelligence community, and other government agencies that exceed what conventional military forces possess. But enhancing these connections is necessary to integrate different departments and agenciesâ?? efforts in cyberspace, synchronize disparate targeting data, and streamline communications.

Collaboration with industry leaders is necessary to maintain access to the cutting edge. SOF are uniquely positioned to maximize impact through their natural team building and creating purpose-built coalitions. By partnering with US companies, USSOF can increase the â??valueâ?• of alliesâ?? and partnersâ?? engagement with US cyber and space-focused training entities. Widespread adoption of Microsoftâ??s technology has created a global infrastructure ecosystem, one where product utilization increases productivity and international relevance. The ability to include these industry-standard partners in foreign military sales or security forces assistance (SFA) activities may persuade uncertain countries to partner with the United States, thereby increasing US reach in strategic locales.

USSOCOM must also embrace cyber and space as fundamental aspects of SFA activities. Doctrinally, SFA is defined as activities based on organizing, training, equipping, rebuilding, and advising various components of foreign security forces. Typically, these activities are aligned with country-specific combat arms functions, such as providing training to conduct area defense or seizing key terrain. However, the necessity of defending national cyber infrastructure now rivals the importance of holding physical terrain.

American network defense capabilities are world-renowned, and information technology equipment and training are often more politically acceptable to allies and partners than receiving military equipment. For instance, in addition to donating approximately $400 million in digital infrastructure and support to Ukraine, Microsoft also provides cybersecurity training to 28 countries globally. Microsoft Vice President Kate Behncken states, â??These countries have an elevated cyber threat risk, coupled with a significant gap in their cybersecurity workforcesâ?¦â?• Consequently, the inclusion of defense cyber operations and network development and operations into SFA activities would influence additional nations to partner with USSOF, bolstering the partner nationâ??s capabilities, expanding access and placement in areas previously deemed politically too sensitive, and ultimately advancing US national policy objectives.

Lastly, USSOCOM must utilize its SOF-peculiar authorities to confront challenges in cyberspace. As the conventional services struggle to implement tactical effects within the cyber domain, USSOCOM is uniquely capable of performing a pathfinder role and providing lessons learned on organization, training, and equipment for DoW-wide implementation. Furthermore, USSOCOM entities, such as Special Operations Forces Acquisition, Technology, and Logistics (SOF AT&L) and SOFWERX, can rapidly develop, test, and field cyber capabilities tailored to specific battlefield needsâ??and improve commercially procured equipment for cyber and space-related SFA activities. Additionally, USCYBERCOM currently struggles with the accession, training, and follow-on retention of personnel as members rotate through assignments and back to individual services. Aligning a portion of Cyber Commandâ??s billets with USSOCOMâ??s selective manning model, following a selectively manned precedent similar to that used by the AFSOC Special Operations Surgical Teams, would eliminate this issue and allow for increased continuity of operations for highly specialized personnel, which is vital to the success of slow-burning cyber operations. Admittedly, utilization of SOF-peculiar authorities is a temporary solution to broader organizational issues within the US cyber milieu. However, these authorities allow for rapid adaptation to an ever-changing digital landscape, which is necessary for continued global relevance as a premier technological leader.

USSOF initiatives within this domain should not be conducted in isolation or separate from those undertaken by USCYBERCOM, the Department of State, and other interagency partners. Strict cross-agency coordination is required to ensure these operational means align with national security strategic ends. Doctrinally, USSOF must maintain a supporting force posture, allowing for the technical expertise of cyberspace professionals to leverage the access, placement, and SOF-specific authorities that only USSOF can provide. Furthermore, these cyber-focused efforts would not be done at the expense of other SOF core activities. If implemented correctly, the organic inclusion of cyberspace activities will increase the effectiveness of all future USSOF missions, as well as the missions of other combatant commands.

Conclusion

Monodâ??s observation about the interconnectedness of necessity and chance underscores that evolution is never arbitrary. For Ukraine, necessity demanded resilience against Russian aggression, while chance enabled the rapid adoption of drones and commercial communications. USSOCOM now faces its own evolutionary inflection point. By employing cyber capabilities and cutting-edge US technology as an effective instrument of national power, USSOCOM can ensure that its supporting role in non-kinetic operations not only enhances the effectiveness of all USSOF but also secures enduring relevance in the broader strategic competition. In this way, USSOCOMâ??s future role will likely exemplify Monodâ??s dictum: military evolution, like biological evolution, is driven by the twin forces of chance and necessity.

Ben Soltisz is an IWI Nonresident Fellow and an active-duty US Air Force expeditionary communications officer with extensive Special Operations experience. A graduate of the US Air Force Academy, he also holds a Master of Science degree from Oklahoma State and a Master of Military Studies degree from the US Marine Corps Command and Staff College. Currently, Ben attends Georgetown University through the USAF McConn Strategy Fellowship, where he is earning a Master of Policy Management degree. Professionally, he is heavily focused on the role of Irregular Warfare in future conflict and has deployed numerous times throughout the Middle East, Central/South America, and Asia. The opinions presented in this article are his own and do not represent the official positions of the US Air Force or the Department of War.

Main Image: 1SFG with SDN. Courtesy of DVIDS.

The views expressed are those of the author 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.

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
2025/11/21