Expeditionary Cyberspace Operations

Paul Schuh

ABSTRACT

As the pace of change in cyberspace operations and the nature of cyberspace forces continues to increase, the demand for innovative solutions to warfighters' needs and improved lethality of the joint force shows no signs of slacking, and the concepts and frameworks established just a few years ago to meet these needs have evolved to keep pace. The Cyber Mission Force is tasked to handle national and combatant commander priorities, working from garrison or deployed when necessary. As the Cyber Mission Force reached full mission capacity, including concomitant changes to their alignment and command and control, additional capability and capacity were required, including, ultimately, calls for additional types of cyberspace forces. In particular, there is a growing need for cyberspace forces that deploy within the physical domains. This article introduces and defines the term Expeditionary Cyberspace Operations (ECO) to standardize terminology for these tactical maneuver units operating across the competition continuum.

THESIS

The conduct of military cyberspace operations (CO) is both enabled and restricted by the nature of the domain, particularly the interconnectivity afforded by the Internet and other global, regional, and local networks. Although cyberspace forces can gain remote access to many targets in and through cyberspace, some targets with military utility are difficult to access from a distance and require maneuver in one of the physical domains to achieve close access of some form. And some systems to which cyberspace forces require close access are not targets at all.

Paul Schuh is the Technical Director of the Policy, Doctrine, & Strategy Division of U.S. Cyber Command (USCYBERCOM), the command Joint Doctrine Lead, and the command terminologist. He served for 20 years in the U.S. Navy as a Surface Warfare Officer and a Cryptologist. After retiring from the Navy, he was a Lead Associate at Booz-Allen Hamilton, supporting all the predecessor organizations of USCYBERCOM, and then transitioned to a DoD civilian position. He helped develop DoD's technical assurance evaluation standard for cyberspace capabilities and became the command's subject-matter expert for technical policy and doctrine. He authored the first detailed Cyber Lexicon in DoD, which became the foundation for portions of joint doctrine for cyberspace operations, for which he is currently the Lead Agent (pwschuh@cybercom.mil). Education: BS Computer Science, The Ohio State University, MS Computer Science, US Naval Postgraduate School, and MS Systems Technology-Joint C3, US Naval Postgraduate School.

In addition to personnel deployed from Cyber Mission Force (CMF) teams, a variety of additional units exist or are being developed that could conduct these close-access missions. The Services are conceiving, resourcing, and fielding elements to conduct CO in support of combatant commands (CCMDs), particularly including U.S. Special Operations Command (USSOCOM), beyond the operations of the 133 CMF teams under the combatant command (COCOM) authority of U.S. Cyber Command (USCYBERCOM). ***But what term should we use to refer to operations where cyberspace forces are required to deploy within the physical domains?*** "Tactical cyberspace operations" has been used colloquially to refer to this activity, but is that the correct term? This article examines the terminology, opportunities, and challenges in the development, deployment, and operations of the cyberspace forces that the Services and USSOCOM are proposing to meet. Additionally, this article introduces the related roles and responsibilities, command and control (C2), training, infrastructure, data, authorities, and capabilities issues.

BACKGROUND

The cyberspace challenges facing the United States (US) have evolved significantly since 2010, when USCYBERCOM was initially established as a subordinate unified command; in 2012, when the Department of Defense (DoD) decided to create the 133 teams of the CMF; in the 2018 elevation of USCYBERCOM to a unified combatant command; and the 2022 elevation of the Cyber National Mission Force Headquarters to a subordinate unified command. USCYBERCOM initially deployed small "expeditionary cyber support elements" forward to Afghanistan and Iraq to facilitate operations against extremists operating in cyberspace and to support physical domain tactical operations while at the same time overseeing the newly assigned and overwhelming task of securing and defending the Department of Defense Information Network (DODIN). The scope of

the USCYBERCOM mission, the number and complexity of its operations, and the policies and authorities under which it operates have grown tremendously since that time. Today, USCYBERCOM conducts operations to execute the following missions:

- Defend forward through persistent engagement to compete with and counter adversaries in competition below the level of armed conflict.
- Execute global operations under various Presidential determinations.
- Provide CO support to CCMDs and forces deployed in crisis response and contingencies.
- Protect the DODIN and support protection of the defense industrial base.
- Counter malign influence, including protecting US elections.
- Acquire and develop CO infrastructure and capabilities,
- Train and exercise the CMF in preparation for wartime operations,
- Execute the Presidentially assigned responsibilities of joint force provider and trainer.

Over the past eleven years, the pace and scope of USCYBERCOM's operations have steadily increased, as did DoD's recognition of both the critical need and growing promise of CO to meet the challenge posed by the Nation's most concerning nation-state threats and other malign actors, including the malicious activities of criminal, individual, and non-state origin in cyberspace. Meanwhile, the demand for tactical CO capacity and operations continued to grow, with increasing CCMD appetite for CO, particularly those integrated with physical domain maneuver forces.

OPPORTUNITIES

With over eleven years of operating experience under expanded responsibilities and authorities, there is potential of CO to better bear in competition below the level of traditional armed conflict and better prepare for its use in crisis, conflict, and war. This opportunity is accompanied by the inexorable convergence of CO, signals intelligence (SIGINT), electromagnetic warfare (EW), military information support operations (MISO), and other operations in the information environment, and by the concomitant need to organize and equip our forces. We must ensure our efforts are well coordinated from a resource perspective and informed by sound development and standardized operating principles. This effort requires a common understanding among the Office of the Secretary of Defense (OSD), the Services, CCMDs, and USCYBERCOM of the terminology and responsibilities that apply to our collective initiatives.

As cyberspace forces are developed and fielded by the Services and deployed by the Services and USSOCOM, we must standardize the associated terminology, examine authorities, develop processes, and clearly assign responsibilities between USCYBERCOM, the Services, and the CCMDs so that CO are conducted under proper authorities; effective C2; sufficient technical

control; and necessary coordination, deconfliction, and synchronization of tactical, operational, and strategic operations. We must ensure initiatives to build new teams of cyberspace forces are mutually informed to meet requirements while avoiding duplication and inefficiency in training, infrastructure and capabilities development, and concepts for effective force employment. This is particularly critical in cyberspace, where any specific operation can have significant impacts on the efficacy and viability of tactics, techniques, and capabilities across the entire joint force and intelligence enterprise and can significantly affect the viability and effectiveness of CO worldwide.

THE CHALLENGE

The goal of any cyberspace operation is maximum effectiveness in achieving its desired objective while protecting against secondary consequences to infrastructure, capabilities, and other operations. This means striking the right balance between distributed CO planning and execution by units under the Services, CCMDs, and maneuver commanders; and the centralized/delegated tasking authorities and technical control essential to enabling and protecting the effectiveness of the Nation's cyberspace forces and capabilities overall.

This challenge has two parts: defining and administering standards for training, qualifications, capabilities development, tradecraft, and operations, and then distributing operating responsibilities in a inherently interconnected domain that overlaps with the physical domains and in which many operations may have global implications for the joint force's overall operating effectiveness. These characteristics are unique to cyberspace. In the physical domains, the employment of a specific weapon or tactic in one area of operations (AO) against a specific target has few immediate implications for the viability of employing it in other AO's against different targets. In cyberspace, using a particular infrastructure, capability, or technique may risk or foreclose its effectiveness across the entire force as adversaries recognize and close exploited vulnerabilities. This means we must apply consistent approaches to ensure that tactical, operational, and strategic CO are effective and responsive to the commander's needs and yet conducted under appropriate authorities and effective technical control to ensure the protection of other operations and the overall capability of the force, and prevent or mitigate unintentional effects.

ISSUES

As understanding and experience in CO continue to evolve, and as the Services and USSOCOM invest in and deploy additional cyberspace force elements, several things must be done:

- Clarify the terminology related to CO support to tactical maneuver elements in the physical domains (this article).
- Clearly understand USCYBERCOM's role and authority in conducting CO at all levels of warfare.

- Better synchronize diverse force, capability, infrastructure, and training initiatives.
- Delineate responsibilities among USCYBERCOM, the Services, USSOCOM, and executing commands.

TERMINOLOGY

DoD joint doctrine, in Joint Publication 1, *Joint Warfighting*, describes three levels of warfare:

- **The tactical level of warfare** is where battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. (Note that this definition is focused on the units involved and the objectives sought, not on the unit's location.)
- **The operational level of warfare** is where campaigns and major operations are planned, conducted, and sustained to achieve strategic effects within a theater or another operational area.
- **The strategic level of warfare** is where a nation or group of nations uses national resources to achieve national or multinational strategic objectives.

Based on these definitions, a "tactical cyberspace operation" would be "a cyberspace operation conducted by tactical cyberspace forces units to achieve tactical effect." But that doesn't limit the scope of the term to only those tactical units that deploy with physical domain maneuver units. A combat mission team (CMT) operating remotely from the US will fit the same definition if it achieves tactical-level objectives, even if it is maneuvering to the target virtually, not physically. The distinction between operational and strategic CO depends upon the level of the intended objective. Similarly, strategic cyberspace operations could be defined as "cyberspace operations conducted using national resources and infrastructure to achieve national or multinational strategic objectives to gain advantage in competition and establish conditions to prevail in war." Like tactical CO, strategic CO can be conducted from any location, access permitting.

USE CASES

Consider a CO to support a particular maneuver engagement against an enemy's weapons systems or units within a particular geographic AO; in close proximity to physical domain forces in contact; using the organic resources of a locally deployed CO unit; with effects limited in duration and conducted for tactical impact. This is easily recognized as a tactical CO. Now consider a different example – a CO against a particular network or entity for a local tactical effect, but the execution of which depends on national assets, data, infrastructure, and capabilities; executed remotely across infrastructure far removed from the supported tactical operation; to create effects against a key node geographically far removed from the theater of the

desired tactical outcome. This is also a tactical CO but would require authorities not held by a local command, capabilities not directly available to the local commander, and execution under policy and technical control factors beyond tactical considerations. Conversely, an operational or strategic CO might involve dispersed global or localized operations that leverage forward-deployed forces in close physical proximity to an access point. The bottom line is that the location of the operation does not determine the level of the operation.

This spectrum of operations means that a unit of an Army Cyber Warfare Battalion or an Air Force Mission Defense Team must train to meet both the deployment and sustainment standards of their Service, as well as the CO technical, policy, and interoperability standards specified by CDRUSCYBERCOM. A unit of the Navy's Fleet Offensive Cyber Teams or a Marine Corps cyber mission element (CME) must carry equipment compatible with shipboard installation and maintenance and follow procedures that are fully consistent with tactics, techniques, and procedures specified by CDRUSCYBERCOM for gaining, maintaining, and sharing target accesses, which may have continued utility beyond the scope of the Team's deployment for later operations at the tactical, operational, or strategic level.

To the extent that units of the CMF are fully tasked with theater-level and national-level objectives, these units of cyberspace forces manned, retained, and/or fielded by the Services and USSOCOM will increasingly fulfill roles requiring deployment within the physical domains. Examples include deploying for the following objectives:

- Gain access through a low-power, point-to-point radio frequency (RF) link.
- Gain access through physical connection (tapping) to wired communications links.
- Gain access through hands-on keyboards or the insertion of portable media.
- Hunt for cyber threats on allied/partner networks.

PROPOSED DEFINITION

To summarize, the opposite of remote operations is not tactical operations. The opposite of remote is "proximal" or better "close access" or even better "expeditionary." To specify the training, equipping, and qualification standards required for units of cyberspace forces to deploy with forces maneuvering in the physical domains, as well as the policies and procedures required to standardize their tasking and their mission reporting, a more specific term than tactical is required: one that evokes its intended meaning.

The proper term for this type of deployed, "on-site" CO support, whether accompanying physical domain maneuver units or as stand-alone cyberspace forces, is ***expeditionary cyberspace operations (ECO)***. This term more precisely captures the essence of this activity, which is not just tactical and may even be strategic. In the DOD Dictionary of Military and Associated

Terms, the term expeditionary force is described as "organized to achieve a specific objective in a foreign country." Note that this term originated when forces had to be physically present in a foreign country to achieve their objectives. Still, its meaning endures to this day and captures the spirit and intent of the missions these CO units are intended to undertake.

Therefore, the *definition of expeditionary cyberspace operations* should be "cyberspace operations conducted by personnel or units of cyberspace forces deployed within the physical domains." ECO can describe not just external CO missions, i.e., offensive cyberspace operations (OCO) and defensive cyberspace operations response actions (DCO-RA), but also internal CO missions (defensive cyberspace operations-internal defensive measures (DCO-IDM) and DODIN operations. In fact, DCO-IDM hunt forward operations (HFO) are usually expeditionary.

MANNING FOR ECO

Any sufficiently trained, qualified, equipped, and appropriately ordered unit (or individual), including portions of the CMF, could undertake ECO. But because operational and strategic level taskings consume most of the CMF capability and capacity, units from groups 7 and 10 from the December 2019 SecDef *Cyberspace Operations Forces* (COF) Memo are the cyberspace forces likely to undertake many of these missions. These "non-COF" cyberspace forces are being developed specifically to undertake ECO and are manned by Service-retained (group 7) or USSOCOM-assigned (group 10) personnel. C2 of specific forces doing ECO will not be one-size-fits-all but will depend upon their assigned mission, including who has operational control (OPCON), tactical control (TACON), and the type of physical domain maneuver element they support.

TRAINING FOR ECO

As with other warfighting disciplines, effectiveness in the highly technical CO field is a direct function of individual and collective skills and training. USCYBERCOM will develop and direct training standards for all cyberspace forces, including standards guiding the training of cyberspace forces for ECO. USCYBERCOM will work with the Services and OSD to identify opportunities to gain efficiency in developing and administering CO training across the force. To maintain the capability to conduct Presidentially directed joint force trainer duties, CDRUSCYBERCOM must be able to establish, maintain, inspect, and certify minimum training standards for all cyberspace forces conducting ECO. This is done based on the position-specific qualifications documented in the Joint Cyberspace Training and Certification Standards (JCT&CS) used for the CMF. Units assigned to conduct ECO may propose and contribute to developing new, ECO-specific JCT&CS standards. Whenever possible, proposed new standards should be universal to all ECO missions, not specific to one Service or CCMD.

EQUIPPING FOR ECO

There have already been interoperability issues between CO capabilities procured by the Services for similar missions and effects. The Joint Cyber Warfighting Architecture (JCWA) Program is creating standards for Service- and USSOCOM-developed deployable cyberspace capabilities. Various JCWA portfolio interface control documents (ICDs) will establish interoperability requirements for cyberspace capabilities used for ECO, including data exchange formats. Capabilities like the deployable mission support system (DMSS) kits for cyberspace protection teams (CPTs) have already begun this standardization. The Services should procure infrastructure to support ECO under standards and policies defined in conjunction with USCYBERCOM, who will be DoD's lead and approval authority. USCYBERCOM, in conjunction with the Services, will define data standards, governing policies, and cyberspace capability development policies. Decentralized development of cyberspace capabilities to support ongoing operations will be the norm, but it will be subject to technical control and governance of USCYBERCOM.

EXISTING AUTHORITIES

Conduct of ECO, like any military operation, falls to those units with an assigned ECO mission and an execute order (EXORD) to undertake a specific operation. Their specific tasking may be covered inside a larger, all-domain operational order (OPORD) or in a stand-alone order to conduct CO in support of another named operation. In general, ECO are subject to the same constraints and restraints as other CO. This includes national policy, DoD policy, and Chairman's EXORDS that apply to all CCDRs. Further, external mission ECO remain subject to the requirement for interagency deconfliction for cyberspace attack and exploitation actions.

All ECO-capable units derive their authority to operate from their operational chain of command. Any combatant commander can conduct CO under specific circumstances. However, only CDRUSCYBERCOM is assigned specific responsibilities for CO in the Unified Command Plan (UCP); represents DoD in the interagency deconfliction process; is under order to secure, operate, and defend the DODIN; and routinely deploys forces to defend non-DODIN blue cyberspace. Consequently, the US military must consider how to best characterize and assign responsibilities and C2 for tactical, operational, and strategic CO to ensure maximum effectiveness while avoiding unintended consequences.

NEW AUTHORITIES

As the Services continue to develop cyberspace forces that fall under the "non-COF" designation, USCYBERCOM should maintain centralized tasking authority for all CO, including ECO, to maintain cyberspace situational awareness and to aid in required operational deconfliction. In the same manner that National Security Agency (NSA) delegates SIGINT operational tasking authority (SOTA), CDRUSCYBERCOM could delegate *cyberspace operations tasking authority* ("COTA") to tactical commanders in a manner that focuses their activities on mission-relevant

targets and limits risk to other similar or associated CO. COTA would be the authority for a military commander to operationally direct, and levy CO requirements on, designated units.

Likewise, in the same way that NSA exercises SIGINT technical control (SIGINT TECHCON), CDRUSCYBERCOM could exercise "*CO TECHCON*." This control over the policies and standards that underpin the CO would not be delegated. CDRUSCYBERCOM should retain control over the uniform techniques, standards, and support mechanisms by which CO, including ECO, are conducted, by which CO operational and mission reporting is produced, and how mission-relevant information is collected, processed, and disseminated.

SUMMARY

Expeditionary Cyberspace Operations are happening now and will occur more in the future. Establishing the correct terminology and providing its definition are just two short steps on a long journey to make the expeditionary operations of cyberspace forces part of a comprehensive framework of fully deconflicted, mutually supporting, and globally integrated CO.

DISCLAIMER

The views expressed are those of the author and do not reflect the official policy or position of U.S. Cyber Command, the Department of Defense, or the U.S. Government.