The JSOU Quick Look is intended to provide a brief overview of a complex topic.

For more in-depth JSOU Press products, visit *https://jsou.libguides.com/jsoupublications*

JSOU Quick Look

Cyber Fundamentals for SOF

What is cyber?

Variations of the word cyber can describe both things and activities. In terms of things, joint doctrine identifies cyberspace as “the domain within the information environment that consists of the interdependent network of information technology infrastructures and resident data.” Conversely, cyber activities include cyberspace operations (CO) which are “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”[1] These terms appear clear, but practical use can be difficult when commanders and planners are seeking approvals or authorizations as the distinction between the domain (cyberspace) and the activity (CO) will result in differences for operational considerations and processes.

In fact, disagreement remains regarding CO, information operations, and a variety of overlapping disciplines.[2] The after-action reviews from Joint Task Force (JTF)-ARES Operation Glowing Symphony (OGS), discussed below, indicate that even though it was a successful operation, military and interagency planners disagreed on terms, authorities, and processes.[3] Yet, doctrinal or operational disagreements should not prevent the rest of Special Operations Forces (SOF) from gaining a usable framework to understand cyber.

In 2018, Congress clarified the authority for U.S. Cyber Command (CYBERCOM) to operate in cyberspace and for the military to execute cyberspace operations as a traditional military activity.[4] Accordingly, CYBERCOM uses a concept of persistent engagement to guide U.S. military actions in cyberspace. Under this concept, cyber capabilities are no longer only employed under certain circumstances. The U.S. is prepared to engage adversaries with constant contact, rather than waiting to defend against attacks, and U.S. military forces are prepared both to act themselves and enable actions by interagency and international partners.[5]

What makes up the cyberspace domain?

The *physical network layer* represents the tangible objects that enable information to be entered, processed, stored, or transmitted. Examples include laptop computers, hard drives, fiber optic cables, routers or any technology device one can touch. This could include something a person carries like a mobile phone, all the way up to massive data centers full of servers or mainframe computers. Objects in this layer exist in the physical world someplace, are owned by someone, and need to be protected from unauthorized physical access.

The *logical network layer* can be more challenging to visualize because it includes nearly everything except the physical devices. This layer is made up of the data that resides in the technology, the computer code that processes the data, and the addresses that enable the data to travel from one place to another. It encompasses what you would consider typical functions of a computer such as to run an operating system, open a software program, or display information. The only way to access what is on this layer is through the use of technology devices and computer code.

Finally, the *cyber-persona layer* is the collection of who exists in the cyber world. This can range from logon accounts assigned to real people, the records associated with a business entity, or identities like webpage addresses that are not necessarily related to a specific person or company. This can also include a person's social media account, the logon to a desktop computer, or a team's use of a shared identity to logon to a system. Linking a persona to a real-world individual, entity, or specific device may require extensive collection and expertise.

What actions do friendly and adversary actors undertake in cyberspace?

Joint doctrine categorizes cyberspace actions according to the effects the actions are intended to achieve.[6] *Cyberspace security* encompasses the tactical actions that proactively protect and harden information and systems. It also refers to the improvement of detection measures and resolution of known vulnerabilities. The addition of a network sensor or antivirus program would serve this purpose. *Cyberspace defense* actions describe how units defeat an adversary following an intrusion into networks operated or protected by military entities. However, these measures cannot cause effects to systems or information outside the networks they are assigned to protect. Cyberspace security and defense occur in friendly (blue) space.

Cyberspace exploitation actions represent steps using cyber capabilities to prepare for future military operations. These can include collection of information about the enemy as intelligence or operational preparation of the environment. It can involve targeting, finding weaknesses, or identifying enemy key cyber terrain. Similarly, exploitation can position cyber capabilities in preparation for anticipated future operations, cyber, or otherwise. An example would be installing a device or code to capture network traffic. Exploitation happens in neutral (gray) or enemy (red) space.

Cyberspace attack consists of measures—deny or manipulate—to make a targeted system or information unusable for its expected function. The result, temporary or permanent, may appear only in cyberspace or can impact the physical world. *Deny* can take three different forms: degrade, disrupt, and destroy. *Degrade* makes something less useful, but still functioning for a specified period of time. An example could be a ship's engine that only can produce half its rated power output. *Disrupt* causes something to be completely inaccessible or unusable for some amount of time. This would occur if a website were temporarily inaccessible to users. *Destroy* renders something irreparably unusable. This could be the case if a computer fan stopped working causing the processor to melt.

In contrast to deny, an attacker can *manipulate* a system or information to change how it works or underlying data used by the system. An example would be if a shipment of fuel were sent to the wrong port by changing the specified destination. Manipulation can be subtle so that the targeted system functions normally but dependent systems do not.

JTF-ARES

In October 2014, the United States established a military construct, Combined Joint Task Force-Operation Inherent Resolve (CJTF-OIR), to counter the Islamic State of Iraq and Syria (ISIS). CJTF-OIR, with the support of coalition partners, pursued ISIS using air and ground forces, along with training and assistance to local forces and opposition groups.[7] SOF played a counterterrorism (CT) role in this mission.[8] CJTF-OIR generated a model for the future of multi-domain warfare.

There is now public recognition that the coalition later pursued a much different type of warfare. JTF-ARES was authorized in May 2016 to counter ISIS in cyberspace by planning and executing cyberspace operations as a subordinate to CYBERCOM, and thereby not under the control of U.S. Central Command or CJTF-OIR.[9] Instead, the commander of U.S. Strategic Command signed an execute order in November 2016 to authorize "offensive cyberspace operations" under OGS to act against ISIS targets.[10]

ISIS effectively used the internet to recruit, radicalize, threaten, and intimidate. The group also used the internet to maintain global reach—a capability that CJTF-OIR could not disrupt solely using air or ground forces. OGS objectives against ISIS media framework and functions included effects against network services and applications, email, domains, media products, virtual private servers, social media, and webpages.[11]

In the fall of 2016, OGS changed how the U.S. military operated against ISIS in cyberspace. Previous activities were sporadic and generally limited in geographic scope. OGS started a continuous set of actions to counter ISIS in cyberspace by taking down accounts, websites, and infrastructure used to create and distribute propaganda. It also disrupted internal communication across ISIS leaders and followers, and gravely disrupted an ISIS publication which never resumed operations.[12]

The OGS Concept of Operations mentioned the role of on-net operators, along with the involvement of the National Security Agency, Federal Bureau of Investigation, and United Kingdom and Australian intelligence entities.[13] This interagency and partner input prevented unintentional interference in their existing operations while bringing to bear additional authorities, capabilities, and accesses. Assessments after OGS execution deemed it a success because it "escalate[d] operations to damage and destroy Islamic State of Iraq and Syria networks."[14] Further, OGS showed the importance of executing operations both within and outside of designated combat areas, and how activities against an adversary outside the combat zone builds military combat capability.

Three noteworthy takeaways for SOF, listed below, came out of OGS.

(1) The objectives OGS successfully targeted were otherwise nearly unreachable by kinetic effects. As such, public knowledge of OGS and the U.S. capabilities in cyberspace compels adversaries to consider that their infrastructure is also at risk of attack by cyber operations.
(2) The leadership of JTF-ARES, under CYBERCOM, with partner organizations brought new capabilities beyond what traditional CT brings to the fight. The use of cyber operations expanded coalition CT capabilities.
(3) U.S. Special Operations Command (USSOCOM) has broad responsibility as the coordinating authority for the counter violent extremist organization mission. The USSOCOM commander described it as the responsibility to craft a single, coherent CT global framework for action. OGS bridged the USSOCOM role with CYBERCOM capabilities.

Why do cyberspace operations matter to SOF?

SOF by its very nature are different from conventional forces because of its capability to achieve strategic effects in all phases of conflict with speed, flexibility, and a relatively small footprint.[17] These characteristics are similar to what can be achieved in cyberspace.

Cyberspace operations extend the reach, agility, pace and effectiveness of SOF when fully integrated into doctrine, training, planning and execution. For example, foreign internal defense requires cyber-enabled operation off the grid and detection of adversary activity to enable partner response. In contrast, unconventional warfare needs ways for resistance movements to make its own equipment and that can happen with cyber-enabled 3-D printing.[18] All SOF core activities can be cyber enabled. However, for each core activity SOF needs different cyber-enabled capabilities to secure these benefits.

The USSOCOM commander identified influence as the key task for how SOF will execute great power competition (GPC) against Russia and China. Even in the CT space, the commander found that SOF leaders are already spending much of their time on the information environment, of which cyberspace is a part. This information can exist in cyberspace, a physical domain, or a combination of the two. The commander went so far as to say that a cyber operator may be the most important SOF team member on future missions.[19]

Why SOF and Cyber Matters

Cyber operations can support or enhance SOF missions on the ground, while also forcing the adversary to consider more ways that friendly forces can attack its organization. Coalition actions during OGS showed the criticality and value of cyberspace operations in support of the on-going CT mission. Kinetic actions, typically executed by SOF, could not have countered ISIS use of the internet, particularly when the presence extends outside the defined area of hostilities. Likewise, CO would not have been effective if executed agnostic of supporting kinetic activities executed by SOF.

The shift to GPC further highlights the usefulness of cyber operations. Friendly forces generally cannot physically deploy forces in areas controlled by China and Russia during the current state of competition. Even operations in neutral countries can be difficult to enable if perceived actions directly counter a nation-state adversary. Cyber operations can present options to policy makers and military leaders to influence through the information environment or, if needed, create effects against critical infrastructure in the physical environment. Ultimately, SOF can use a foundational understanding of CO as both a planning consideration for force protection and operational enhancement to present opportunities to execute core mission areas. ■

Endnotes

[1] Joint Chiefs of Staff, *Cyberspace Operations,* Joint Publication 3-12 (Washington, D.C.: Joint Chiefs of Staff, 2018), I-1, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[2] Herb Lin, "Doctrinal Confusion and Cultural Dysfunction in the DoD," *The Cyber Defense Review 5,* no. 2 (2020): 89-108.

[3] Michael Martelle, ed., "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY," National Security Archive, 21 January 2020, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

[4] Robert Chesney, "Covert Military Information Operations and the New NDAA: The Law of the Gray Zone Evolves," *Lawfare,* 10 December 2019, https://www.lawfareblog.com/covert-military-information-operations-and-new-ndaa-law-gray-zone-evolves.

[5] "An Interview with Paul M. Nakasone," *Joint Forces Quarterly* 92 (1st Quarter 2019): 4-9, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf.

[6] Joint Chiefs of Staff, *Cyberspace Operations,* I-5 to I-7.

[7] "History," Combined Joint Task Force Operation Inherent Resolve, 22 July 2017, https://www.inherentresolve.mil/Portals/14/Documents/Mission/HISTORY_17OCT2014-JUL2017.pdf?ver=2017-07-22-095806-793.

[8] Micah Zenko, "What Obama Really Meant by 'No Boots on the Ground,'" *The Atlantic,* 3 December 2015, https://www.theatlantic.com/international/archive/2015/12/obama-boots-on-the-ground/418635/.

[9] U.S. Cyber Command, "USCYBERCOM FRAGORD 01 TO TASKORD 16-0063 to Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyberspace," U.S. Cyber Command, 25 May 2016, https://assets.documentcloud.org/documents/3678213/Document-07-USCYBERCOM-to-CDRUSACYBER-Subj.pdf.

[10] U.S. Strategic Command, "FRAGORD 06 TO USSTRATCOM OPORD 8000-17: Authorization to Conduct Operation GLOWING SYMPHONY," 8 November 2016, https://nsarchive2.gwu.edu/dc.html?doc=4638023-USSTRATCOM-Subj-FRAGORD-06-to-USSTRATCOM-OPORD.

[11] U.S. Cyber Command, "United States Cyber Command Concept of Operations (CONOP) OPERATION GLOWING SYMPHONY," 13 September 2016, https://nsarchive2.gwu.edu/dc.html?doc=4638018-USCYBERCOM-JTF-ARES-United-States-Cyber-Command.

[12] Dina Temple-Raston, "How the U.S. Hacked ISIS," NPR, 26 September 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

[13] Michael Martelle ed., "Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL," *National Security Archive,* 13 August 2018, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isis.

[14] Martelle, "Joint Task Force ARES."

[15] Mark Pomerleau, "What Cyber Command's ISIS Operations Means for the Future of Information Warfare," C4ISRNET, 18 June 2020, https://www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/.

[16] Raymond A. Thomas III, "Statement of General Raymond A. Thomas, III, U.S. Army, Commander, United States Special Operations Command," Senate Armed Services Committee, 4 May 2017, https://www.socom.mil/pages/posture-statement-sasc.aspx.

[17] Patrick Michael Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Forces Quarterly* 79 (4th Quarter 2015), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_46-53_Duggan.pdf.

[18] Patrick Duggan, "Man, Computer, and Special Warfare," *Small Wars Journal*, 4 January 2016, https://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare.

[19] Jim Garamone, "Special Ops Will Remain Integral to Strategy, USSOCOM Commander Says," U.S. Army, 18 May 2020, https://www.army.mil/article/235667/special_ops_will_remain_integral_to_strategy_ussocom_commander_says.

AUTHOR: U.S. ARMY LIEUTENANT COLONEL MITCHELL WANDER. CONTACT INFORMATION: MITCHELL.WANDER@SOCOM.MIL.

THE VIEWS EXPRESSED IN THIS PUBLICATION ARE ENTIRELY THOSE OF THE AUTHOR AND DO NOT NECESSARILY REFLECT THE VIEWS, POLICY, OR POSITION OF THE UNITED STATES GOVERNMENT, DEPARTMENT OF DEFENSE, UNITED STATES SPECIAL OPERATIONS COMMAND, OR THE JOINT SPECIAL OPERATIONS UNIVERSITY.

JOINT SPECIAL OPERATIONS UNIVERSITY
Department of Strategic Studies
7701 Tampa Point Blvd., Bldg. 5200, MacDill AFB, FL 33621
socom.mil/jsou