On Cyber Force Employment

Setting conditions for SIF employment

by Col Jamel Neville & Maj Joel Chapman

>Col Neville is the Commander of the Marine Corps Cyberspace Warfare Group. He has led Marine and joint cyber forces to conduct defensive and offensive cyber and information operations in support of national objectives and coordinated kinetic and non-kinetic fires and effects in combat.

>>Maj Chapman has served in several capacities in the Cyber Mission Forces and has deployed in support of combatant commander priorities.

As witnessed in the contemporary operating environment, cyberspace has become a pivotal warfighting domain, generating insights, opportunities, and options across the competition continuum. This article explores the strategic considerations surrounding the MAGTF and the Joint Force's utilization of offensive cyber capabilities within the information warfighting function. Despite the range of options cyberspace presents, it is a complex domain with myriad technical and administrative challenges, including target development and authorities. These challenges necessitate a model of employment reserving strategic cyberspace reconnaissance and attack operations for the higher end of the competition continuum. By prioritizing cyber targets that best enable maneuver forces during times of crisis and armed conflict, cyberspace operations can deter adversary aggression and escalation in competition while setting conditions for the Marine Corps' globally positioned stand-in forces' (SIF) role in enabling the Joint Force to fight and win the Nation's wars should deterrence fail.

Background: The Information Environment and Its Challenges

The *information environment* is the global competitive space that spans the warfighting domains. It is where information is stored, moved, and communicated and is the linchpin of Marine Corps operations—*both deployed and in garrison*.[1] Cyberspace is the sector of the information environment comprised of interdependent networks of information technology infrastructures and data.[2] Electromagnetic pathways, guided and unguided, interconnect physical nodes, and certain elements—including data, applications, and network processes—can be abstracted logically beyond any single point in the physical domain.[3] Cyber operations forces tactically and technically maneuver through this logical layer, regardless of its physical medium,[4] to generate or counter systems overmatch—creating fires, intelligence, mobility, logistics, or command and control advantages for their supported forces.[5] Offensive cyberspace attacks are activities executed in and through cyberspace that create denial or manipulation effects and are considered a form of fires.[6] Thus, *effects* are the primary focus of MAGTF and Joint Force commanders' requests for cyber support and operational objectives.

... cyberspace operations can deter adversary aggression ...

Target development in cyberspace is complicated. Each target is unique and requires bespoke solutions to engage due to technical configurations, running software, and administrator actions. Gaining initial access to a network while remaining undetected requires significant time and effort. Further, maturing access into a viable position for launching a cyberspace attack presents even more challenges. Even relatively simple attacks require a detailed understanding of the specific environment for effective employment, necessitating detailed technical targeting data before exploitation. Like a hardened facility in a physical domain, *hard targets* in cyberspace are defended in depth with multiple overlapping cybersecurity solutions, imposing significant costs in time and resources to overcome.[7] In the period between gaining access and executing a cyberspace attack, cyber forces are at risk of discovery, and changes to the network environment can cause forces to lose access without warning. Once employed, cyberspace capabilities are at risk of exposure and can be seized and employed by our adversaries against friendly forces.[8] Concealed activity and non-detection are key—critical vulnerabilities the Joint Force must guard against.

Another major hurdle for cyberspace operations is authorities. Offensive cyberspace operations require an ap-

proval process that can reach as high as the President of the United States.[9] Speaking at an Armed Forces Communications and Electronics Association event in December 2016, former Undersecretary of Defense for Policy (Cyber) retired MajGen Burke "Ed" Wilson highlighted that it is challenging to be "able to gain the authorities and delegate that down so [cyber forces] can move at the speed of the kinetic fight." The high level of approval required for cyberspace operations could reduce the flexibility of cyber forces and the timeliness of cyberspace operations concerning evolving tactical situations in the other four warfighting domains.

The information age has ushered in the rapid integration of cyber fires from the tactical to strategic level in the contemporary operating environment.

As highlighted by these challenges, a critical difference between traditional and cyberspace fires is flexibility against different target sets. Cyber forces require significantly more time to become familiar with adversary terrain and generate combat power. For this reason, cyberspace operations do not naturally lend themselves to crisis response activities. However, by focusing cyberspace operations on key adversaries, it is feasible to optimize the employment of cyber forces and employ them effectively across the continuum of conflict. By orienting cyber forces against threats to national security during Phase 0 (zero) operations, cyber forces can take the necessary actions to prepare the battlespace in support of the MAGTF and Joint Force, providing deterrence to mitigate the risks of competition escalating into crisis and conflict.

Setting Conditions

By preparing the operating environment, cyberspace operations can enable Marine Corps SIF operations, activities, and investments while leveraging their geographic placement and access. During the prelude to its 2008 invasion of Georgia, Russia launched numerous cyberspace attacks against Georgian computer systems. Though limited in scope (e.g., shutdown of public-facing Georgian government websites), these attacks effectively prevented the Georgian government from rapidly disseminating information to its population. More recently, in the prelude to the 2022 Russian Invasion, Ukraine experienced several waves of cyberspace attacks consisting primarily of website defacement and destructive malware campaigns intended to disrupt the Ukrainian government and local organizations.[10] Malware also spread through Viasat's KA-SAT network, disrupting the modems of 50,000 European users, including Ukrainian military units.[11]

The information age has ushered in the rapid integration of cyber fires from the tactical to strategic level in the contemporary operating environment. Cyberspace attacks have enabled military operations by disrupting adversary command and control, injecting uncertainty into government communications, and, at the higher end, disrupting critical technologies ranging from industrial infrastructure to military systems. Cyber fires supplement and expand upon traditional deep fires, functioning similarly to the air campaign to reduce Iraqi command and control in the lead-up to the First Gulf War. However, unlike kinetic fires, cyber fires can be temporary and reversible. Thus, planning and synchronizing the desired effects of cyber fires throughout MAGTF and Joint Force commanders' campaigns and operational schemes of maneuver are crucial.

High Payoff Targets

As the Joint Staff and Combatant Commanders assess principal threats and gain an understanding of adversary force structure and capabilities, they reveal critical vulnerabilities that are potentially susceptible to offensive cyberspace operations. These high payoff targets are usually well-defended, imposing significant costs to preparing the information environment for a cyberspace attack. However, by holding these targets at risk, offensive cyber forces could rapidly degrade adversary capabilities if executed during crisis and armed conflict. In other words, identifying and assessing vulnerabilities within a particular system, network, or infrastructure that could be exploited to achieve military objectives or disrupt an adversary's operations at the time, speed, and tempo of commanders' choosing.

Given the difficulty of rapidly reorienting and scaling cyber forces against new target sets during a crisis, focusing on these high payoff targets provides a preferred alternative for forces to prepare the battlespace. During Phase 0 operations, cyber forces can take deliberate steps, supported by joint, intergovernmental, interagency, and multinational partners, to identify, target, gain access, and generate effects against adversary high payoff targets should competition escalate to crisis and conflict. Should that escalation occur, cyber forces could provide deep fires in support of maneuver forces' operational schemes of maneuver, significantly affecting adversary capabilities in areas not accessible to conventional kinetic fires.

Deterrence

If postured to support the MAGTF and joint forces by preparing the battlespace and holding high-risk payoff targets at risk, offensive cyber forces could simultaneously provide a deterrent effect against aggressive action by our adversaries. The challenge in achieving deterrence through clandestine means was succinctly captured in the Stanley Kubrick film *Dr. Strangelove*, when the titular character remarks, "Of course, the whole point of a doomsday machine is lost if you keep it secret!" However, effectively *signaling* capabilities to adversaries without revealing tactics and techniques can be achieved, as exemplified by the 2019

National Public Radio report on Operation GLOWING SYMPHONY, Joint Task Force Ares' efforts to defeat ISIS. GEN Paul Nakasone, the former Commander USCYBERCOM, highlighted the effect of signaling his testimony to the House Select Committee on the Chinese Communist Party in January 2024. He said of USCYBERCOM's offensive capabilities, "We communicate it in many different ways - from our policymakers who have these discussions to the exercises that we conduct to the real-world examples that we do with a series of different partners."[12]

petition continuum. It will continue to be a critical component of future competition and conflict. The unique challenges of target development and the authorities to conduct cyberspace operations necessitate novel approaches rather than the traditional direct support fires model.

Cyber forces are uniquely capable of setting conditions during Phase 0 operations to posture for potential crises and armed conflict with offensive cyberspace capabilities. Cyber forces could conduct reconnaissance to gain access to adversary networks and posture to

Cyber forces are uniquely capable of setting conditions during Phase 0 operations to posture for potential crises and armed conflict with offensive cyberspace capabilities.

By demonstrating capability through public statements, partnership engagements, and selected declassified reports, cyber forces possess the potential to present unsolvable dilemmas to adversaries. When potential vulnerabilities are exposed, adversaries expend resources to search for evidence of intrusion on their critical systems. The best a defensive cyber team can do is to find no evidence of intrusion, it is impossible to prove that no intrusion has occurred. This challenge in defending networks will further support the potential deterrent effect of cyber forces, as the adversary is left to guess where and how deeply they are compromised and what impact that could have should they seek to act in contravention of U.S. interests. This cognitive effect provides the most potential value to the larger joint force, as it seeks to prevent the necessity of employing kinetic forces by preventing, rather than responding to, crisis and conflict.

Conclusion

Cyberspace operations offer opportunities to support the Marine Corps' globally-positioned SIF and Joint Force operational objectives across the competition continuum. Cyber forces are uniquely capable of setting conditions during Phase 0 operations to posture for potential crises and armed conflict with offensive cyberspace capabilities. Cyber forces could conduct reconnaissance to gain access to adversary networks and posture to hold at risk high payoff targets that, if attacked, could reduce an adversary's ability to generate combat power and respond to Marine Corps SIF and Joint Force actions in the physical domain. The capability to provide this support during conflict could deter escalation in competition by generating uncertainty amongst adversaries as they second-guess their critical capabilities.

This model for employing cyber forces seeks to address the challenges of conducting cyberspace operations during armed conflict. Setting expectations for MAGTF and Joint Force commanders on how cyberspace operations can best support their operational schemes of maneuver enables them to set conditions more effectively in competition and fight and win in conflict.

Notes

1. Headquarters Marine Corps, *MCDP 8, Information*, (Washington, DC: 2022).

2. Office of the Joint Chiefs of Staff, *JP 3-12, Joint Cyberspace Operations* (Washington DC: 2022).

3. Ibid.

4. Definition of "Department of Defense Cyberspace Operations Forces (DOD COF)" according to SecDef Memorandum, December 12, 2019.

5. *MCDP-8.*

6. JP 3-12.

7. CISA, "2022 Top Routinely Exploited Vulnerabilities," *CISA*, August 3, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a.

8. Lily Hay Newman, "The Leaked NSA Spy Tool That Hacked the World," *WIRED,* March 7, 2018, https://www.wired.com/story/eternal-blue-leaked-nsa-spy-tool-hacked-world.

9. *JP 3-12;* and Mark Pomerleau, "Authorities Complicate Use of Cyber Capabilities." *C4ISR Net,* January 9, 2017, https://www.c4isrnet.com/home/2017/01/09/authorities-complicate-the-use-of-cyber-capabilities.

10. Sharon Rollins, "Defensive Cyber Warfare Lessons from Inside Ukraine," *Proceedings*, June 2023, https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine.

11. Staff, "War in Space Is No Longer Science Fiction," *The Economist*, January 31, 2024, https://www.economist.com/international/2024/01/31/america-china-and-russia-are-locked-in-a-new-struggle-over-space.

12. C. Todd Lopez, "U.S. Can Respond Decisively to Cyber Threat Posed by China," *U.S. Dept of Defense*, February 1, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3663799/us-can-respond-decisively-to-cyber-threat-posed-by-china. Additional information is available at https://selectcommitteeontheccp.house.gov/media/press-releases/media-package-select-committee-ccp-holds-hearing-ccp-cyber-threat-american.