REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
04-05-2018	FINAL	Nov 2017 - May 2018

4. TITLE AND SUBTITLE

Effective Cyberspace Operations Intelligence and Planning Support to the Joint Task Force

5a. CONTRACT NUMBER

N/A

5b. GRANT NUMBER

N/A

5c. PROGRAM ELEMENT NUMBER

N/A

6. AUTHOR(S)

LCDR Kurt Shulkitas

5d. PROJECT NUMBER

N/A

5e. TASK NUMBER

N/A

5f. WORK UNIT NUMBER

N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

N/A

15. SUBJECT TERMS

Joint Task Force, Cyberspace Operations, Intelligence, Operations Planning

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			LCDR Kurt Shulkitas
U		U			**19b. TELEPHONE NUMBER** *(Include area code)*
					(206) 512-5821

NAVAL WAR COLLEGE
Newport, R.I.

TITLE: Effective Cyberspace Operations Intelligence and Planning Support to the Joint Task Force

Kurt Shulkitas

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy

INTRODUCTION

Thanks to the Goldwater-Nichols Department of Defense Reorganization Act of October 4, 1986, the United States joint force evolved from individual services competing for precious resources and conducting planning and operations in service stovepipes to the current Unified Command Plan construct. It reorganized geographic combatant commands and created functional combatant commands responsible for overseeing all military planning and operations in their respective area of responsibilities (AOR). The overarching motivation for these reforms was to attempt to correct unity of effort failings experienced in the Korean War and Vietnam War.[1] Combatant Command authority allows these commanders to dynamically organize their forces to maximize operational effectiveness, particularly through the establishment of Joint Task Forces (JTFs) or Sub-Unified Commands.

The operational application of unity of command and achievement of unity of effort are but two of ten command and control (C2) tenets the Joint Force Commander (JFC) must deftly manipulate to ensure their JTF or Sub-Unified Command achieves maximum operational effectiveness. Additionally, a JFC's ability to make timely decisions and implement effective coordination mechanisms both internal to the JTF or Sub-Unified Command and with external organizations is critical to meeting challenges posed by adversaries or potential adversaries.[2] Nothing is more important to the JFC than unity of command and unity of effort.

The U.S. military is practiced at operating within the four physical domains – air, land, maritime, and space – but falls woefully short at achieving unity of command and unity of effort

[1] Edward J. Cole et al, "History of the Unified Command Plan 1946-2012," (Joint History Office, Washington D.C., 2013), 4-5.
[2] Joint Military Operations Reference Guide, *Forces/Capabilities Handbook*, (Naval War College, Newport, RI, 2018), 193.

within the information environment and electromagnetic spectrum. One principle of effective military operations is the ability to mass force at a place and time of the commander's choosing, which brings to bear all necessary means at her or his disposal to achieve an operational objective. Cyberspace operations – "a global domain within the information environment" – is rarely able to reliably achieve this synchronization with operations occurring in the physical domains.[3] This shortfall is a critical capability gap largely of our own making. The JFC and their staffs often do not fully understand what cyberspace operations, particularly offensively-oriented capabilities, can provide or the process required to request and attain the appropriate approvals and authorities at the appropriate level of command to support execution. The massive intelligence requirements to execute cyberspace operations are largely undertaken by organizations without an established command relationship with the JTF. The JTF is entirely beholden to those outside organizations and their internal priorities to provide intelligence and operations support because the JFC likely will not have personnel resident to the staff with the requisite expertise and system accesses.

At its very core, fighting and winning the nation's wars with supporting fires through the information environment demands a mindset shift from the kinetic conflicts and physical operations synchronization the joint force is accustomed to one that acknowledges the ubiquitous nature of the information environment. More specifically, the JFC needs to become the master of their information domain and retain, at a minimum, tactical control (TACON), and preferably operational control (OPCON) of trained, certified, and regionally experienced cyberspace operations forces familiar with the operating environment and the unique challenges of maneuvering within a constantly evolving domain. This includes intelligence professionals with the training and experience to integrate cyber-specific data into the intelligence preparation of

[3] JOINT CHIEFS OF STAFF WASHINGTON DC, *Joint Publication 6-0 Joint Communication Systems*, 2017, I-6.

the battlefield (IPB) and joint intelligence preparation of operating environment (JIPOE) and cyberspace operations planners specialized in integrating cyberspace operations into planning at the operational level-of-war.

Intelligence Support to Cyberspace Operations

There is an oft-cited mantra in the U.S. military that intelligence drives operations. Intelligence impacts everything from the grand decision to embark upon war to determining which building a special operations team on the ground will raid. A carrier strike group will plan their defensive screen based on the perceived threat resident in the area of operations (AO). The intelligence needs of the JFC and their planners are insatiable, and as combat conditions in the AOR evolve the side that recognizes changes in the operating environment or the intent of the adversary and reacts first has a marked advantage.

Cyberspace operations are no different. The need to recognize and aggregate the right data into operationally relevant intelligence for use by the JTF and subordinate warfighters is still a crucial facet of conflict, but not enough is being done to ensure the right analysts get relevant training and are appropriately distributed across the intelligence enterprise. The primary Navy contribution to joint intelligence is Sailors trained as intelligence specialists. Following 13 weeks of primary "A" school training, most Navy intelligence specialists will obtain one of six navy enlisted codes (NECs). These NECs include 3910 – Imagery Intelligence Analyst, 3912 – Expeditionary Warfare Intelligence Analyst, 3913 – Navy Tactical Counter-Intelligence and Human Intelligence Specialist, 3923 – Strike Warfare Intelligence Analyst, 3924 – Operational Intelligence (OPINTEL) Analyst, or 3927 – Advanced Strike and Tomahawk Land Attack

Missile Mensuration Analyst.[4] While these six advanced schools represent the sort of experience intelligence specialists will bring to their various assignments, only OPINTEL includes any topics on cyberspace operations, and those topics are not considered a required core competency.

Thankfully, the various cyberspace operations forces recognize this shortfall and are seeking to correct these deficiencies. Commander, U.S. Cyber Command ordered each service to take the lead on some aspect of cyberspace operations training and execution. The U.S. Navy was assigned the all-source intelligence analyst work role to develop analysts knowledgeable in the unique requirements of cyberspace operations. Additionally, four of the previously non-core cyber competencies will be shifted to core competencies and tested during the semi-annual enlisted advancement exams. A request is pending to create an additional NEC to track this expertise, as well.[5] The course is expected to reach initial operational capability (IOC) on 1 October, 2018.

While this represents a monumental leap forward in training the intelligence personnel in supporting cyberspace operations, the next hurdle will be how to ensure the training remains current. After the training courses are established, the primary complication to ensuring this deep cyber intelligence expertise can be relevant to the JTF is the current billet assignment model the Navy utilizes. Analysts are expected to be familiar with and take assignments conducting a variety of intelligence disciplines. Also, the intelligence specialist rating is primarily a sea-going rate, so Sailors and their promotion potential will still be tied to superior performance at sea and adherence to the usual sea-shore duty rotation. While this system provides unique broadening opportunities, it hinders most from developing the deepest possible

[4] NAVY LEARNING AND DEVELOPMENT ROADMAP, *Intelligence Specialist (IS)*, 2018, 5.

technical and tactical acumen. The result of this assignments model is any experience working on cyber-related intelligence and/or targeting will atrophy to the point of irrelevance before another opportunity to use cyber-specific knowledge and expertise presents itself.

For the JTF, this presents some risks. Intelligence personnel familiar with more traditional all-source analysis attached to the JTF will likely not understand what products the cyber planners require or how to develop them. Reporting will be limited to existing serialized reporting, and access to raw data will be severely limited due to how cyber-related information is often protected. Even if a demonstrated need can be established and approval received, the process of gaining access to the raw data will not be swift. While traditional intelligence analysts integrate reporting and imagery into planning and the kinetic targeting cycle, the analysts devoted to cyberspace operations are immediately at risk of becoming irrelevant to the JFC because constructing a comprehensive picture of the information environment is decidedly more complicated and more time consuming due to the complex interactions with the traditional domains. This is particularly egregious in AORs without strong national intelligence prioritization. In these instances, the intelligence specialist supporting cyberspace operations will be the lead coordinator between the JTF J2, cyber planners resident on the JTF staff, and interagencies supporting cyberspace operations planning and execution.

Supporters of the current intelligence support model for cyberspace operations will argue that as a high-demand, low-density asset, the best way to ensure operations are adequately triaged and supported is by concentrating the preponderance of intelligence analytic capability at a few key locations. By concentrating the expertise in a small number of locations, leaders can identify the highest priorities targets and allocate the most capable analysts accordingly.

---

[5] ISC Nancy Grant (active duty U.S. Navy Intelligence Specialist involved with testing and curriculum development) in discussion with the author, April 2018.

Particularly difficult targets may receive more analytic capability, while lower priority targets may receive fewer resources or less experienced analysts.

While this model represents how Admiral Michael Rogers, Commander U.S. Cyber Command, intends to achieve his stated goal of operational "speed and agility" in the cyberspace domain, it takes a utilitarian approach to developing and employing the expertise required to meet military requirements.[6] The highest priorities receive the majority of competent expertise, leaving lower-level intelligence collection and production requirements undermanned or completely unmet. Worse still, most JTF analysts focused on intelligence support to cyberspace operations planning and execution rely entirely upon national collection and reporting, which is annually reallocated through the process delineated in Intelligence Community Directive (ICD) 204, *Roles and Responsibilities for the National Intelligence Priorities Framework* and overseen by the Director of National Intelligence.[7] The Department of Defense is but one intelligence community customer, and therefore competes for resources like any other organization.

Cyberspace Operations Planning

Presuming sufficient intelligence collection and analytic resources exist to support the JTF's cyberspace operations, the next challenge is how that intelligence supports planning and drives operations. U.S. Cyber Command aptly claims that existing planning doctrine can be readily leveraged with few significant adaptations to support cyberspace operations; however, the planners need to be provided specialized training from which a foundation of relevant

[6] Admiral Mike Rogers, "Inside the Wire: American Security and Cyber Warfare," (speech, 58th Annual Academy Assembly at the U.S. Air Force Academy, USAF Academy, CO, March 15, 2017).
[7] Intelligence Community Directive 204, *Roles and Responsibilities for the National Intelligence Priorities Framework*, (Director of National Intelligence, Washington D.C., January 2, 2015).

experience can be built. Most importantly, those trained and experienced planners must be fully integrated into the JFC's operations planning teams (OPTs) and build the trust and relationships with senior JTF leadership that only time and direct access to the JFC can achieve.

While joint doctrine and the joint operation planning process (JOPP) can support cyberspace operations planning, there are critical challenges in the cyber domain that require attention. First, the cyber domain is very different from the four traditional physical domains. Additionally, there are persistent misunderstandings regarding what effects cyberspace operations can achieve and the phase 0 prerequisites to ensure those effects have a reasonable chance of success. Finally, a general lack of cyberspace operations expertise outside of U.S. Cyber Command and their components limits the effectiveness of often precludes early cyberspace effects integration into JTF planning.

Integrating cyberspace effects within JTF plans in support of the joint force component commanders is complicated by the unique characteristics of the cyberspace domain. The Department of Defense (DoD) describes cyberspace as "a global domain within the information environment … [consisting] of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[8] Unlike the physical domains, the very characteristics by which an operating area might be defined can evolve. Cyber-savvy intelligence personnel may locate a potential target, pass that information to planners, and find the next day that a change in network topography or physical infrastructure renders all previous intelligence, surveillance, and reconnaissance useless. A smart adversary may utilize this to their advantage – regularly reorganizing network segments, shifting operating systems or changing their physical infrastructure. While costly and generally untenable, even small changes may complicate

planning at the operational and tactical levels of war. It is therefore reasonable to conclude that planning within the maritime, air, and space domains is simplified to a degree by consistent physical properties and predictable operational factors interactions, while the opposite is true for cyberspace.

The natural interaction between domains hints at another complexity with cyberspace operations. In the physical domains, it is generally understood that extra care must be taken in planning and execution where domains interact. Close air support operations occur in the air domain, but directly impact the land domain. Sea control in the maritime domain could be directly challenged by land-based aircraft or coastal defense cruise missile sites. These interactions add a measure of complexity, but – apart from weather – are generally predictable because they are threat-based. Cyberspace is unique in that it extends entirely across all physical domains, impacting operations throughout rather than just on the periphery. An effect residing only within the cyber domain does not exist because all effects eventually manifest themselves in a physical domain, even if the effect is slowing the decision-making capability of an individual. This requires planners to consider operational factors and their interactions differently. One example of the unique interactions of operational factors is the space and force interaction. No other domain contends with an operational environment that can fundamentally change instantaneously. Access developed in a target network to posture for the future delivery of a cyber effect may be suddenly lost without warning. This concept upends how military planners have notionally considered the operating space. The force's ability to mass combat power in cyberspace – a principle of war clearly applied in traditional physical domains – may unexpectedly fail, which will require the friendly force to swiftly adapt.

---

[8] JOINT CHIEFS OF STAFF WASHINGTON DC, *Joint Publication 3-0 Joint Operations*, 2017, IV-2.

To operate effectively and meet the challenges posed by the unique characteristics of the cyber domain, the JTF needs competent cyber operations planners assigned to the staff who deeply understand their specific operating environment. At the order of then-Secretary of Defense Leon Panetta, all geographic combatant commands (GCCs) established Joint Cyber Centers (JCC) to address the growing need to integrate cyberspace operations into theater missions.[9] The purpose was threefold: to improve situational awareness, enhance network defense, and establish a single clearinghouse responsible to the combatant commander for incident response, recovery, and coordination.[10] Should the need to establish a JTF arise, the combatant commander (CCDR) has the authority to organize the unit to best face the specific threat. Most likely, the cyber forces most familiar with the target and unique domain characteristics in theater will reside within the GCC's JCC, which makes it a viable option to temporarily fulfill the cyberspace operations planning requirements for the newly established JFC. While this could be effective in the short-term, the JCC assumes significant risk to other missions while a portion of its staff is assigned to support the JTF.

Unfortunately, liaison officers from U.S. Cyber Command, cyber service-components, and cyber-related fly-away support teams will also fall short of meeting the JFC's cyberspace planning requirements. Fly-away support teams, such as those provided by U.S. Transportation Command's Joint Enabling Capabilities Command (JECC), can effectively assist newly established JTFs in traditional physical domain operations and organization, but do not scale appropriately in cyberspace.[11] The cyber domain does not lend itself to "plug and play" fly-away support because, unlike the inherently stable characteristics displayed in physical domains,

[9] Thomas Doscher, "NORAD, USNORTHCOM Joint Cyber Center Stands Up," (Department of Defense, Peterson Air Force Base, Colorado, 2012), http://www.northcom.mil/Newsroom/Article/563711/norad-usnorthcom-joint-cyber-center-stands-up/.
[10] Ibid.

the cyber domain is dynamic both in terms of the threat and the characteristics of the domain itself. Consider that telecommunication networks, computer networks, internet service providers, supervisory control and data acquisition (SCADA) systems, weapons systems, sensors, and all associated underlying infrastructures vary wildly in hardware, software configuration, vulnerabilities mitigated, and zero-day vulnerabilities still present. Additionally, threat actors could be operating within this same maneuver space with or without our knowledge, further hindering operations. Achieving JTF objectives within cyberspace requires target expertise developed over time and in-depth knowledge of the threats specific to the operating area.

The only way for the JFC to meet the threat in cyberspace and project power in the cyberspace domain is by requesting and receiving dedicated cyberspace operations planners with adequate cyberspace analyst intelligence support staff. These planners would have area familiarity, know the telecommunications and associated networks, and have coordinated with the execution forces to ensure they were postured to support Title 10 cyberspace effects operations, if required. U.S. Cyber Command does not have the capacity to adequately meet all mission requirements in all AORs, a fact reiterated by ADM Michael Rogers in his 27 February 2018 testimony before Congress. When pressed about why U.S. Cyber Command does not do more, he ADM Rogers asserted "… the challenge for us is about prioritization, aligning mission with resources…".[12] CCDRs need to advocate for adequate cyberspace operations planning and intelligence expertise focused on the operational and strategic levels-of-war as a way to grow the type of area and threat expertise necessary to successfully establish a JTF in their AOR with the

---

[11] JOINT CHIEFS OF STAFF WASHINGTON DC, *Joint Publication 3-33 Joint Task Force Headquarters*, 2017, II-4.

[12] Derek Johnson, "Rogers: CyberCom Lacks Authority, Resources to Defend All of Cyberspace," *FCW*, 27 Feb 2018, last modified February 2018, https://fcw.com/articles/2018/02/27/rogers-congress-sasc-nsa.aspx.

ability to operate within the cyberspace domain. Retaining this expertise also insulates the command from an overreliance on a support relationship with U.S. Cyber Command, which has its own priority missions and will not always have the capacity to provide adequate support.

The final requirement for the successful application of cyberspace effects in support of the JTF's objectives is to retain a force capable of conducting Title 10 effects-based operations. The current model notionally requires the establishment of a support relationship between U.S. Cyber Command and the requisite GCC via an order. Once the support relationship is established, U.S. Cyber Command will assess how the additional requirements may impact risk to existing missions, determine what level of support, if any, the JTF will receive, and internally task a combat mission team (CMT) or a portion of a CMT to support. Ideally, this CMT will have an existing relationship with GCC's JCC and already be familiar with the target's cyberspace domain within the information environment.[13]

A problem arises when it is determined that the level of support will be minimal or notional because the risk to higher level missions would be too great to provide adequate support to the emerging operation. Because of how aggressively U.S. Cyber Command retains control of service cyber forces, fewer forces are available for assignment to and tasking by GCCs. This lack of available OPCON or TACON cyber forces necessitates the JTF to coordinate all operations through the GCC's JCC for cyber mission approval and execution. This extra level of coordination obfuscates the relative cyber combat potential available to the JFC, as well as muddles mission synchronization and execution – impacting unity of effort. In addition, unity of command complications can quickly develop because the executing cyberspace operations forces are not formally assigned to the JTF or necessarily operating under the JFC's authority.

[13] Lt. Col. James Austin (Chief, U.S. Africa Command Joint Cyber Center) in discussions with the author, October 2017.

CONCLUSION

A fair question must be addressed, which is how does a JTF organized to face a difficult task/challenge compete for resources in an ad hoc manner to meet an emerging threat or task? The answer is with difficulty, which underpins the critical requirement for the JFC to obtain and retain competent intelligence analysts and planners.

The current support model relies upon support relationships at the CCMD level. Even with direct liaison authority, all requests for assistance and reprioritization of missions would need to be sent from the JTF to U.S. Cyber Command through the JTF's appropriate GCC. Subsequent support would come only if the mission aligns with established U.S. Cyber Command priorities and assumes higher priority missions do not fully exhaust U.S. Cyber Command's support capacity. As the global synchronizer for all DoD cyberspace operations, U.S. Cyber Command's list of tasks and objectives is significant, and any support provided to the JTF will come at the detriment of another mission. The JFC cannot assume cyberspace operations intelligence support and planning capability will exist or be prepared to deliver effects within the time and space constraints required by the pace of traditional military operations.

The only way GCC CCDRs and their staffs can be prepared to support the planning and execution of the full range of military operations is by retaining the capabilities and capacity to effectively conduct those missions. This necessitates a full evaluation of how cyberspace operations intelligence and planning support is conducted, who retains control of both those forces and the executing forces, and how any request for forces can be filled through the traditional global force management processes. The best place for an analyst to gain experience

and familiarity with threats relevant to a battlespace is by focusing on that AOR over time. Until a baseline level of knowledge is constructed, it is impossible to determine what is new or unusual. That level of fidelity in the information environment, and in particular the cyberspace domain, does not exist in most AORs. This represents a critical vulnerability that could be partially mitigated through specialized training and a new approach to how the Navy allocates those forces.

BIBLIOGRAPHY

Cole, Edward, et. al. “History of the Unified Command Plan 1946-2012.” (Joint History Office, Washington D.C., 2013). Retrieved from http://www.jcs.mil/Portals/36/Documents/History/Institutional/ Command_Plan.pdf.

Doscher, Thomas. “NORAD, USNORTHCOM Joint Cyber Center Stands Up.” (Department of Defense, Peterson Air Force Base, Colorado, 2012). Retrieved from http://www.northcom.mil/Newsroom/Article/563711/norad-usnorthcom-joint-cyber-center-stands-up/.

Intelligence Community Directive 204, *Roles and Responsibilities for the National Intelligence Priorities Framework*, (Director of National Intelligence, Washington D.C., January 2, 2015). Retrieved from https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

Johnson, Derek. “Rogers: CyberCom Lacks Authority, Resources to Defend All of Cyberspace.” *FCW*, 27 Feb 2018. Retrieved from https://fcw.com/articles/2018/02/27/rogers-congress-sasc-nsa.aspx.

Joint Military Operations Reference Guide. *Forces/Capabilities Handbook*. (Naval War College, Newport R.I., 2018).

Joint Chiefs of Staff Washington D.C. *Joint Publication 3-0 Joint Communications Operations*. 2017.

Joint Chiefs of Staff Washington D.C. *Joint Publication 3-33 Joint Task Force Headquarters*. 2017.

Joint Chiefs of Staff Washington D.C. *Joint Publication 6-0 Joint Communications Systems*. 2017.

NAVY LEARNING AND DEVELOPMENT ROADMAP. *Intelligence Specialist (IS)*. 2018. Retrieved from https://www.cool.navy.mil/usn/LaDR/is_e1_e9.pdf.

Rogers, Michael. “Inside the Wire: American Security and Cyber Warfare.” (Speech, 58th Annual Academy Assembly at the U.S. Air Force Academy, USAF Academy, CO, March 15, 2017).