JTF-ARES as a Model of a Persistent, Joint Cyber Task Force

Charlie Donnelly[1] and Marcel Stolz[2]
[1]University of Chicago, Chicago IL, USA
[2]University of Oxford, Oxford, UK

csdonnelly@uchicago.edu
marcel.stolz@univ.ox.ac.uk

Abstract: Military involvement in cyberspace has traditionally been limited to operations in service of "kinetic," or physical, missions. Military cyberoperations are therefore usually described using traditional "kinetic" descriptors and rarely articulate cyber-related goals that are independent of kinetic operations. Recently, the concepts of "persistence" and "jointness" have been increasingly used by the U.S. Cyber Command to describe cyberoperations. Persistence describes operations that focus on a target over time (in contrast to the episodic "response" concepts articulated in kinetic warfare). "Jointness" describes working across group or agency lines. This paper will investigate the effectiveness of "persistent" and "joint" task forces in accomplishing cyber-related goals by means of a case study of Joint Task Force – ARES ("JTF-ARES"). JTF-ARES was set up as a task force by the U.S. Cyber Command to disrupt ISIS cyberoperations – a singularly cyber (as opposed to kinetic) goal. By contrasting the approach of JTF-ARES with the existing history of US operations in cyberspace, militaries can apply JTF-ARES' successful approach to accomplish future cyber-related goals that are independent of kinetic military units. After discussing a brief history of the U.S. Cyber Command and defining the terms "persistence" and "jointness," the paper discusses JTF-ARES' successful operation and contributing factors, most notably its organization within the U.S. Cyber Command. Next, it explores a counterfactual organization of JTF-ARES, suggesting that alternative organizational structures would likely have ended in failure and highlighting factors that may have influenced its success. Furthermore, the paper discusses the administrative challenges associated with creating a JTF, which include administration hurdles as well as collaboration and training requirements specific to joint operations. Since JTF-ARES deviates from traditional organizational structures within U.S. Cyber Command, this paper articulates criteria for creating a joint, persistent cyber task force, which militaries may find useful when considering how to implement cyber-specific goals. The first criterion concerns the operations required for the mission – namely, are reconnaissance, offensive, and defensive cyberoperations required? The second criterion asks whether the cyberoperation has a uniquely cyber-oriented end state: for missions with non-kinetic goals, it may be helpful to consider a joint, persistent task force.

Keywords: Military Cyberoperations, Task Force, Cyber Organization, Offensive Cyberoperations, U.S. Cyber Command, Kinetic Warfare

1. Introduction

The increasing relevance of cyberspace as an operational domain of the US military has necessitated dedicated government cyber units. These units are often created in service of military organizations, and therefore are conceptualized using military terminology pertaining to "kinetic," or physical, responses. In recent years, however, a "persistence" approach has been used to describe activities that are continuous in nature and may include several strategies, as opposed to episodic defensive or offensive cyberoperations. This new articulation of government cyberoperations is seen clearly in the creation of Joint Task Force – ARES, a subsection of the U.S. Cyber Command established to address ISIS operations. This paper will evaluate the effectiveness of "jointness" and "persistence" in achieving cyber goals that do not directly support kinetic operations. "Jointness" and "Persistence" are evaluated via a case study of JTF-ARES, and its organization in contrast to the rest of the U.S. Cyber Command.

Section 1 of this paper describes a brief history of the U.S. Cyber Command and traditional doctrines around cyberspace operations. Section 2 discusses the relatively recent terminology of "persistence" and jointness" used to describe cyberoperations. Section 3 discusses the case study of JTF-ARES, which can be considered a concrete example of persistent, joint warfare in cyberspace, and illustrates the potential of "single-purpose" task forces to accomplish ambitious cyber-related goals. Subsection A considers the creation of JTF-ARES as the first collaboration between the NSA and the U.S. Cyber Command, and subsection B describes the novelty of the task force in the history of USCYBERCOM operations. Section 4 explores counterfactual scenarios: namely, why JTF-ARES was a dedicated unit as opposed to an existing U.S. Cyber Command service component. Section 5 describes some of the administrative challenges associated with creating JTF-ARES, and it suggests questions to

determine the suitability of a JTF in future operations. Section 6 articulates two potential criteria for establishing future JTFs, and section 6.2 applies these criteria to discuss hypothetical situations in which a persistent JTF may be useful. Lastly, section 6.3 discusses areas of potential future research.

2. A Brief History and Evolution of the U.S. Cyber Command

The U.S. Cyber Command (USCYBERCOM) was established in 2010 by Secretary of Defence Robert Gates as a sub-unified command of U.S. Strategic Command following internal penetration testing and major data breaches from foreign adversaries. Before its establishment, individual cybercommand units were separated into defensive and offensive units, and later unified into USCYBERCOM in 2009 (Command History, n.d.). Along with the 2009 establishment of USCYBERCOM, service subunits were created to serve the Army, Air Force, Tenth Fleet, and Marine Corps (Command History, n.d.). In 2014, the Cyber National Mission Force (CNMF) and Joint Force Headquarters–DoD Information Network (JFHQ-DoDIN) were added. The CNMF was designed to "synchroniz[e] full-spectrum cyberspace operations to disrupt, degrade and defeat malicious cyber actors," and is described as "broad, continuous, joint, and enduring in nature" (Cyber National Mission Force Public Affairs, 2022). The CNMF is the military's newest sub-unified command, and may conduct offensive or defensive attacks.

The JFHQ-DoDIN was created in 2015 to defend DoD networks (Cyber National Mission Force Public Affairs, 2022). General Paul Nakasone serves as the leader of both the USCYBERCOM and the NSA (Inamete, 2022).

The history of the US military in cyberspace is relatively brief when compared with traditional "kinetic" operations, where "kinetic" is defined as "actions designed to produce…physical damage to…or destruction of targets" (Integration and Synchronization of Joint Fires, 2018). Cyberspace was only deemed a domain akin to air, land, sea, and space, in 2004, and as a result, cyberoperations are often conceptualized using kinetic terminology, which will be further discussed in later sections (Proctor, 2006).

3. Key Definitions: "Persistence," and "Jointness"

The words "persistence" and "jointness" have informed the U.S. Cyber Command's strategy under General Nakasone and are helpful descriptors for JTF-ARES. The doctrine of "persistence" is often described as "defending forward," which has been articulated in 2018 DoD strategy documents (Warner, 2020). "Defending forward" typically involves halting threats before they become offensive attacks, and continuously monitoring malicious cyberactivity.

The term "persistence" in cyberspace has traditionally been defined in opposition to a "response-force concept," or "holding forces in reserve for war or responding to attacks after the fact" (Schneider et al., 2020). Response-force is best described as an ad-hoc and episodic approach to warfare, which derives from traditional offensive and defensive separation that is characteristic of kinetic, or physical, warfare. General Nakasone (Commander of the U.S. Cyber Command and Director of the National Security Agency) characterizes cyberspace as a domain that requires reconnaissance, defense, and offense – the US must accordingly "operate continuously to seize and maintain the initiative in the face of persistent threats" (Joint Force Quarterly Issue 92, 2019). Nakasone also claims that USCYBERCOM was initially a response force, designed to defend against attacks – it wasn't until 2018 that the doctrine of a "persistent" force was finally articulated in USCYBERCOM's vision document (Joint Force Quarterly Issue 92, 2019). This shift in approach from "response" to "persistence" helps explain the context for the creation of JTF-ARES, which was created with the ongoing, persistent goal of countering ISIS cyberspace operations.

The term "jointness" is also used by General Nakasone to describe cross-team capabilities or partnerships that enable increased agility in cyberspace. This contrasts with dedicated cyber "service" components, which are embedded within military units like the Army, Navy, Air Force, and Marines, and aid these groups in combat. Vice Admiral Timothy White argues that cyberspace links domains like the air, land, and sea, and has therefore necessitated a "joint" conception (Schneider, 2020). Nakasone further asserts that USCYBERCOM will become increasingly "joint" in future (Joint Force Quarterly Issue 92, 2019).

Notably, the US military has already used "joint" structures against terrorist threats. During the 2007 "Surge" into Iraq, the Special Forces assembled "Intelligence, Surveillance, and Reconnaissance" (ISR) teams with people from a range of agencies – including the FBI, CIA, NSA, and Treasury Department – to target terrorists (Sutherland, 2019). By putting everyone under one roof, these organizations reduced the frictions of cross-agency collaboration. Thus, ISR teams could leverage each agency's strengths on an as-needed basis to do whatever the situation demanded, from tracking fund flows to eavesdropping on phone calls to following a

vehicle. Because of this "jointness" (also called "agile culture"), ISR teams were good at identifying targets for the Special Forces to eliminate. Thus, the success of "joint" teams in kinetic counterterror operations presaged JTF-ARES' success in a cyber offensive.

4. JTF-ARES: A Case Study in Military and Cyber Co-ordination

We now turn to the example of Joint Task Forces-ARES (JTF-ARES), an NSA and U.S. Cyber Command collaboration intended to "deny, degrade, disrupt, and manipulate ISIS' info space" (Temple-Raston, 2019a). The operations of JTF-ARES were inspired by the realization that ISIS materials were distributed through only ten nodes on the internet – by gaining administrative access, the JTF hoped to deny access and disrupt ISIS operations via a mission entitled "Operation Glowing Symphony" (Temple-Raston, 2019a).

After extensive planning and reconnaissance, the offensive portion of "Operation Glowing Symphony" commenced. The task force successfully gained administrative access to ISIS networks and denied access to existing administrators, eliminating a predetermined list of "targets" (Figure 1). Following this initial attack, JTF-ARES completed more subtle follow-on attacks that focused on "eroding morale" (Temple-Raston, 2019a). Examples include deleting ISIS-created content, draining cell phone batteries, and slowing internet for ISIS network users (Temple-Raston, 2019a).

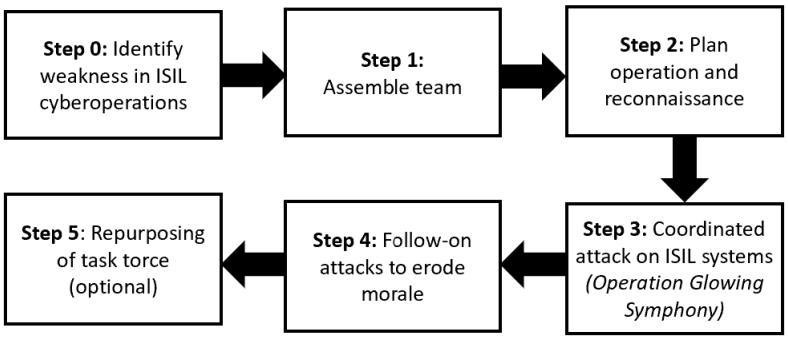

Figure 1: The lifecycle of JTF-ARES, from formation to repurposing

Internal documents deemed the operation a success, as it prompted a delay in official ISIS magazine publications. Other researchers noted a decrease in extremist Twitter activity following the authorization of Operation Glowing Symphony (Martelle, 2018). Alternatively, some have argued that ISIS' continued online presence represents an operational failure (Temple-Raston, 2019a). It is challenging to conclude whether a persistence attack is a distinct "success" or "failure" – persistence operations, by definition, have no end and require continual response.

4.1 JTF-ARES: The First of Its Kind

Before the creation of JTF-ARES, the U.S. Cyber Command launched offensives against ISIS, although no organizational structure for these offensives is available to the public. General Nakasone described cyberoperations against ISIS as "episodic," rather than continuous (Temple-Raston, 2019a). Individual attacks on ISIS servers from USCYBERCOM had no lasting impact on their operations – it is reasonable to conclude that JTF-ARES enabled success in part due to its organizational structure. JTF-ARES's novelty and relative success is also indicated by its longevity: ARES leadership noted that the brand name will be kept despite completion of Operation Glowing Symphony due to the benchmarks set by its approach (Atlantic Council, 2019).

Furthermore, the addition of JTF-ARES appears to be an anomaly within USCYBERCOM. For one thing, it represented the first coordinated effort between the NSA and USCYBERCOM (Temple-Raston, 2019a). It also represented a unique example of a JTF that was independent of a kinetic unit, which stands in contrast to the existing components of the U.S. Cyber Command. Aside from the four service components, the U.S. Cyber Command also includes a Cyber Mission Force (established in 2012), with 133 sub-teams. These teams appear to be primarily defensive (e.g., a Cyber Protection Team), focused on enabling combat (e.g., Combat Mission Force), or response-based (e.g., a National Mission Force to block attacks). Other components like the Cyber National Mission Force (CNMF) represent a larger move toward hybrid offensive and defensive operations, but small and singularly focused task forces are a relative anomaly (Command History, n.d.). The idea that

cyberoperations generally serve kinetic operations can also be seen in the integration of cyberoperations into service groups within the USCYBERCOM, which are created for primarily kinetic purposes. AFCYBER, ARCYBER, and MARFORCYBER are all examples of cyber service subunits that are created to serve their respective branches of military (Air Force, Army, and Marines, respectively).

Most importantly, the task force has been cited by military leadership as establishing new benchmarks in the history of cyberoperations (Atlantic Council, 2019). Brigadier General Leonard Anderson (Deputy Commander of JTF-ARES at USCYBERCOM) noted that singular cyberoperations not in support of a military subunit are a "very rare occurrence," and are more frequently part of a campaign plan that pairs cyberoperations with kinetic operations (Atlantic Council, 2019). General Anderson further notes that current cyber operations generally directly support a marine or soldier on the ground (i.e., kinetic forms of warfare) – while in 15 years, he anticipates cyberoperations that are not singularly in support of a military unit (Atlantic Council, 2019). This perspective of cyberoperations as a tool for accomplishing kinetic missions renders the creation of JTF-ARES unique for two reasons. First, JTF-ARES articulates a unique cyber "end state" in its founding documents, namely that "ISIL is denied use of the cyberspace domain to enable their critical capabilities" (U.S. Cyber Command, 2017). Secondly, this mission statement is not directly in support of a kinetic attack – while weakening ISIS cyberoperations would aid in a long-term kinetic goal, the self-described end state of Operation Glowing Symphony was a cyber, rather than a kinetic goal.

5. Exploring the Counterfactual: Why USCYBERCOM?

It is worth considering briefly why JTF-ARES was created within the purview of the U.S. Cyber Command, as opposed to being conducted within a service component of the USCYBERCOM, or within the Joint Task Force responsible for Operation Inherent Resolve, a coalition of government forces created specifically to counter ISIS (Operations and Exercises, n.d.).

The initial realization that ISIS materials were being distributed through relatively few accounts occurred within the U.S. Cyber Command. It may be the case that had this realization occurred elsewhere, the organizational process and operation would have resulted differently. Had Operation Glowing Symphony been implemented within a military service unit, there may have been conflicts of interest between combat and reconnaissance goals (Stolz, 2021). For example, the cyberoperation may have been apprehended by ISIS, and operations could have been moved to a new network – this may have jeopardized existing military operations that relied on cyber reconnaissance.

Furthermore, Operation Glowing Symphony has been described as the "most complex offensive cyberspace operation" that USCYBERCOM had conducted at the time, and planning documents alluded to the likelihood of conducting similarly complex cyberoperations in future (Martelle, 2020). This complexity necessitated a dedicated team – had the operation been conducted by a service component, or within an existing combat operation, the scale of objectives may have been less ambitious or compromised in favor of other combat-focused goals.

6. Administrative Challenges

JTF-ARES and its Operation Glowing Symphony represent broader moves towards "jointness" and "persistence" doctrines within military conceptions of cyberspace. JTF-ARES inspired similar small and singularly-focused task forces that are able to perform reconnaissance, offensive, and defensive operations. However, JTF-ARES was met with administrative hurdles and organizational challenges that jeopardized the efficacy of Operation Glowing Symphony. Examining these challenges offers insight into future task-force design.

First, Operation Glowing Symphony was met with "non-concurs", or objections from the CIA, State Department, and FBI. Agency leaders felt it was necessary to alert allied countries to potential disruption on servers containing ISIS information (Nakashima, 2017). This complication took weeks to resolve, and prevented the mission from being carried out as designed. Furthermore, extensive clearing processes were required by JTF-ARES to prevent conflicts with ongoing offensive operations in Mosul, Iraq. In FOIA-released documents, the USCYBERCOM notes that (redacted) measures could help "expedite the request and approval process" for clearing targets, especially considering the "likelihood that USCYBERCOM will be conducting more frequent and widely scoped cyber operations…in future" (Martelle, 2020).

Furthermore, the future of JTF-ARES poses questions about whether task forces are easily repurposed, and whether they should be permanent or temporary in nature. JTF-ARES has been refocused to cover great power

competition under the US Indo-Pacific Command's purview, collaborating with MARFORCYBER (Atlantic Council, 2019). The refocusing of JTF-ARES to great power competition as opposed to ISIS cyberoperations suggests that persistence does not mean permanence. A "persistent" task force need not focus on a single threat forever and may pivot in focus.

General Anderson notes that JTF-ARES staffing is dynamic: as JTF-ARES collaborates closer with MARFORCYBER, some of the military personnel within JTF-ARES (which constitute approximately 40% of operators) will return to their own subunits, and the marine-affiliated staffings will increase (Atlantic Council, 2019). Thus, JTF-ARES can be refocused and restaffed according to focus area and may offer increased agility in comparison to service subunits. It also, however, may require specialized training and an increased focus on collaboration to allow civilian and military operators from various agencies to work together.

Staffing and training protocols may need to be customized to enable collaboration between different agencies. FOIA-released documents claim that staffings within JTF-ARES were filled first with NSA employees, then USCYBERCOM service employees (i.e., members of service subunits like MARFORCYBER) (U.S. Cyber Command, 2017). While this protocol offers structure, it also implies that new employees may have different backgrounds and may struggle to collaborate, especially considering JTF-ARES marks the first major collaboration between U.S. Cyber Command and the NSA. The traditional General Staffing System employed by most NATO governments includes separate employees for staffing and training (U.S. Army Special Operations Command History Department, 2011). In the case of JTFs that draw from disparate organizations, staffing and personnel may need to work closely to design custom training courses to ensure personnel can collaborate effectively.

7. Potential Application of Joint Task Forces

JTF-ARES planning documents leave open the possibility of future, similar cyberoperations. We have discussed how the creation of JTF-ARES can be considered something of an anomaly, being the first NSA-USCYBERCOM JTF of its kind. It may, therefore, be useful to consider when a persistent JTF should be created. We propose two key questions to determine whether a JTF may be useful:

Does the cyberoperation require reconnaissance, defensive, and offensive components?

Reconnaissance operations in support of combat missions may be better suited to service subunits of USCYBERCOM. In contrast, JTF-ARES required months of reconnaissance and planning, coupled with offensive and psychological operations to erode morale. Furthermore, JTF-ARES required NSA and U.S. Cyber Command expertise, which meant a JTF was particularly useful.

Does the operation have a cyber (not primarily kinetic) "end state"?

As discussed previously, the concept of a cyberoperation not in service of a kinetic goal is rare. Cyberoperations with self-contained, non-kinetic goals may be ill-suited to service subunits, where their priorities may be subverted. Instead, an individual task force within U.S. Cyber Command that employs "jointness" to recruit specialty talent may be helpful in accomplishing singular, or predominantly cyber goals.

7.1 Further Scenarios and Applications

Having discussed the criteria for establishing a persistent JTF, it is worth considering real-world scenarios that may warrant this organizational structure. As mentioned above, General Nakasone observes that cyberthreats are evolving from episodic, response-based espionage to disruptive, persistent attacks, and this change warrants a new response. Nakasone identifies early cyberthreats as mostly information theft, while modern, "corrosive" threats weaponize information in subtle influence campaigns, a primary example being the 2016 US election (Joint Force Quarterly Issue 92, 2019). A persistent JTF would be especially well-suited to counter this new type of cyberthreat. Indeed, JTF-ARES influenced the formation of the Russia Small Group (RSG), a joint, persistent (and now permanent) task force established by USCYBERCOM and the NSA to counter Russian election influence during the 2018 US midterm elections (Temple-Raston, 2019b; Vavra, 2019).

Election security is particularly well-suited to the JTF structure and it fulfills both of the outlined persistent JTF criteria. To illustrate, one of RSG's public successes was the "hunt forward" initiative, which publicized malware found in foreign government systems. This threat-hunting directly helped foreign governments and had the secondary effect of allowing foreign allies to proactively defend against future malware (Warner, 2020). This mission reportedly allowed for the mass inoculation of "millions of systems" (Warner, 2020). Such activities may be well-suited to a persistent JTF, where a mission like "threat hunting" requires reconnaissance and offensive

capabilities (criterion 1) to investigate compromise on foreign networks. Threat hunting also has little relevance to other kinetic operations, but promotes the long-term health of cyber systems (criterion 2) (Nakasone & Sulmeyer, 2020). Beyond threat hunting, little is known about the operations of the RSG, but General Nakasone also described "offensive cyber and information operations" in connection to the 2018 midterm elections (Senate Hearings, 2015). Thus, the RSG effectively completed reconnaissance and offensive operations under a single, persistent task force structure, and, per Nakasone, "disrupt[ed] those planning to undermine the integrity of the 2018 midterm elections" (Senate Hearings, 2015). Furthermore, a task force dedicated to election security arguably has an end state that transcends kinetic and cyber domains. Senate reports suggest that Russia intended to sow general distrust in democratic voting processes, a goal that included cyber methods but would likely also have caused confusion at physical polling stations (United States Senate Select Committee on Intelligence, 2019). An effective task force would therefore have both cyber and physical goals, quashing DoS and phishing attacks at the local level while simultaneously maintaining the physical order of the election.

The Department of Homeland Security reported that "numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election" (United States Senate Select Committee on Intelligence, 2019). Since a single, powerful state has many vectors to attack an election, a dedicated task force may be well-suited to counter states with a motive and history of election interference. While no specific operational successes have been publicized, media outlets deemed the RSG a success in having "deterred some interference during the midterms," and Senator Blumenthal (D-CT) noted (without specifying) that the RSG had "some successes that the American people should know happen[ed]" (Warner, 2022). Such a success suggests that state-specific task forces, established to defend or act in advance of major events (like elections), may be well-suited to a persistent JTF.

7.2 Potential for Future Research

Although the idea of persistence in cyberspace has reached the highest levels of government, there is minimal practical literature on how to deploy persistent Joint Task Forces. The 2019 National Defense Authorization Act ("NDAA") classified "clandestine military…operations in cyberspace" as "traditional military activity." Thus, non-attack operations in cyberspace face fewer reporting requirements to Congress than do covert actions, the latter of which undergoes complex interagency approvals (Chesney, 2018b). The act also preauthorized the Secretary of Defense to undertake "proportional" cyber measures against an "active, systematic, and ongoing campaign of attacks" against the US that originates from Russia, China, North Korea, or Iran (U.S. Congress, 2018). Furthermore, in 2018, President Trump issued National Security Presidential Memorandum-13, which allows cyberoperations to be conducted with DoD approval, as opposed to the previously complex and time-consuming interagency process (Freedberg, 2018; Weingarten, 2020). In sum, the Secretary of Defense has been given increased autonomy and the ability to conduct offensive and defensive operations in accordance with a persistent, "defend forward" strategy (Chesney, 2018a; Chesney, 2019). While this strategic change is evident in legislation, tactical literature has overlooked the administrative opportunities and challenges of persistent Joint Task Forces, as this paper endeavors to do.

The existing literature about joint military operations in cyberspace does not adequately explain how to deploy tactical cyber operations on a day-to-day operational level. For example, the US Army War College's Strategic Cyberspace Operations Guide, a key document for students hoping to understand cyberoperations' structure, offers high-level information on conducting cyberoperations and potential "big picture" challenges, but fails to offer details on deploying cyberoperations day-to-day (US Army War College, 2022). The document references "defend[ing] forward" as a key and novel approach to cyberspace operations, but it does not discuss how persistent JTFs may differ in challenge, scope, or operation from existing organizational structures. Similarly, the 2018 U.S. Cyber Command's high-level "vision" document articulates persistent engagement as a key priority, citing lengthy approval processes as a hindrance that can force the US into a disadvantageous, "reactive" mode (U.S. Cyber Command Vision, 2018). Future research could discuss the potential of combining several discrete functions into a single JTF to reduce communication overhead costs, or how to effectively repurpose a persistent JTF upon mission completion.

8. Conclusion

This paper discussed the potential for persistent Joint Task Forces that address singularly cyber-oriented goals, using the case study of JTF-ARES. A history of the U.S. Cyber Command was presented, and early conceptions of

cyberoperations as "response"-based have been explained. Further, the terms "joint" and "persistent" have been defined as emerging cyberspace doctrines within the US Government. The unique creation of JTF-ARES has been explored, and we suggest that Operation Glowing Symphony was more likely to have failed under a different military-oriented or cyber service unit. Thus, the usefulness of Joint Task Forces has been shown, and criteria for their suitability has been established for future operations. We also discussed hypothetical scenarios where a persistent JTF may be useful, including election security, especially against a state with a history of cyber interference. While this paper has offered some criteria that may be useful in determining whether a JTF is necessary, further examinations of organizations like the Russia Small Group may offer interesting case studies. The doctrines of persistence and jointness are relatively new compared to response-oriented warfare concepts and merit further research, especially in the day-to-day practicalities of staffing and deployment.

References

Atlantic Council (2019) *Cyber Operations in Context: A Look at Joint Task Force Ares*, YouTube. YouTube. Available at: www.youtube.com/watch?v=aQsDTvQf4_E (Accessed: 9 February 2023).

Chesney, R. (2018a) *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*, Lawfare Blog. Available at: https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes (Accessed: April 17, 2023).

Chesney, R. (2018b) *The Law of Military Cyber Operations and the New NDAA*, Lawfare Blog. Available at: https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa (Accessed: 17 April 2023).

Chesney, R. (2019) *Covert Military Information Operations and the New NDAA: The Law of the Gray Zone Evolves*, Lawfare Blog. Available at: https://www.lawfareblog.com/covert-military-information-operations-and-new-ndaa-law-gray-zone-evolves (Accessed: April 17, 2023).

Command History (n.d.*) U.S. Cyber Command.* Available at: www.cybercom.mil/About/History/ (Accessed: 9 February 2023).

Cyber Mission Force (2022) *U.S. Army Cyber Command.* Available at: www.arcyber.army.mil/Resources/Fact-Sheets/Article/2079661/cyber-mission-force/ (Accessed: 9 February 2023).

Cyber National Mission Force Public Affairs (2022) The Evolution of Cyber: Newest Subordinate Unified Command is nation's Joint Cyber Force, U.S. Cyber Command. Cyber National Mission Force Public Affairs. Available at: https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe/ (Accessed: 16 April 2023).

Freedberg, S.J. (2018) *Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff*, *Breaking Defense*. Available at: https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/ (Accessed: April 17, 2023).

Inamete, U.B. (2022). *The Unified Combatant Command System*. Expeditions with MCUP digital journal. Marine Corps University Press. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/Expeditions-with-MCUP-digital-journal/The-Unified-Combatant-Command-System/ (Accessed: 16 April 2023).

Integration and Synchronization of Joint Fires (July 2018). Retrieved November 27, 2022, from www.jcs.mil/Portals/36/Documents/Doctrine/fp/int_and_sync_jointfires.pdf?ver=2018-%2009-18-102801-350.

Joint Force Quarterly Issue 92 (2019) National Defence University Press (NDU Press). Available at: ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-92.aspx (Accessed: 9 February 2023).

Martelle, M. (ed.) (2020) USCYBERCOM *After Action Assessments of Operation Glowing Symphony,* National Security Archive*.* Available at: nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony (Accessed: 9 February 2023).

Martelle, M. (ed.) (2018) *Joint Task Force Ares and Operation Glowing Symphony: Cyber Command's Internet War against ISIL,* National Security Archive. Available at: nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil (Accessed: 9 February 2023).

Nakashima, E. (2017) *U.S. Military Cyber Operation to Attack Isis Last Year Sparked Heated Debate Over Alerting Allies,* The Washington Post. WP Company. Available at: www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html (Accessed: 9 February 2023).

Nakasone, P.M. and Sulmeyer, M. (2020) *How to Compete in Cyberspace*, *Foreign Affairs*. Available at: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity?check_logged_in=1&utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20230416 (Accessed: April 16, 2023).

Operations and Exercises. (n.d.). *U.S. Cyber Command*. Retrieved November 27, 2022, from www.centcom.mil/OPERATIONS-AND-EXERCISES/OPERATION-INHERENT-%20RESOLVE/

Proctor, A. (2006) *AF launches Cyberspace Task Force, Air Force.* Air Force. Available at: www.af.mil/News/Article-Display/Article/131398/af-launches-cyberspace-task-force/ (Accessed: February 9, 2023).

Schneider, J.G. et al. (2020) *Ten years in: Implementing strategic approaches to cyberspace, U.S. Naval War College Digital Commons.* Available at: digital-commons.usnwc.edu/usnwc-newport-papers/45/ (Accessed: February 9, 2023).

2015 Senate Hearings*, Department of Defense Authorization for Appropriations for Fiscal Year 2016 and the Future Years Defense Program: Hearing on S. 1376 before the S. Comm. on Armed Servs., Subcomm. on Intelligence, Emerging Threats and Capabilities*, 114th Cong. 415 (2015) (statement of Admiral Michael S. Rogers, Commander, US Cyber Command)

United States Senate Select Committee on Intelligence. (2019). *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf (Accessed: 16 April 2023)

Stolz, M. (2021). *Competing Interests of Cyberintelligence and Cyberdefence Activities in Neutral Countries*. 9.

Sutherland, J.V. (2019) in Scrum: *The Art of Doing Twice the Work in Half the Time*. Random House, pp. 54–58.

Temple-Raston, D. (2019a) *How the U.S. Hacked Isis, NPR.* NPR. Available at: www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis (Accessed: 9 February 2023).

Temple-Raston, D. (2019b) *Task Force takes on Russian Election Interference*, *NPR*. NPR. Available at: https://www.npr.org/2019/08/14/751048230/new-nsa-task-force-takes-on-russian-election-interference (Accessed: 16 April 2023).

U.S. Army War College. (2022). *Strategic Cyberspace Operations Guide.* [online] Available at: https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf (Accessed: 16 April 2023).

U.S. Army Special Operations Command (USASOC) History Department (2011) *The General Staff System, U.S. Army Special Operations Command History Office.* Available at: www.arsof-history.org/articles/v7n2_general_staff_system_page_1.html (Accessed: 9 February 2023).

U.S. Congress. (2018*). John S. McCain National Defense Authorization Act for Fiscal Year 2019.* [online] Available at: https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf (Accessed: 16 April 2023).

U.S. Cyber Command. (2017*). Joint Task Force Areas. [pdf]* U.S. Strategic Command. Available at: https://www.stratcom.mil/Portals/8/Documents/FOIA/FOIA%2017-023,%2017-033,%2017-064%20-%20USCYBERCOM%20Joint%20Task%20Force%20Areas.pdf?ver=2017-04-19-111941-797 (Accessed: 17 April 2023).

U.S. Cyber Command. (2018). U.S. Cyber Command Vision April 2018. [online] Available at: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf (Accessed: 16 April 2023).

Vavra, S. (2019) NSA's Russian Cyberthreat Task Force is Now Permanent, CyberScoop. Available at: https://cyberscoop.com/nsa-russia-small-group-cyber-command/ (Accessed: 16 April 2023).

Warner, M. (2022). *U.S. Cyber Command's First Decade.* In M. Warner, The United States' Defend Forward Cyber Strategy (pp. 33–64). Oxford University Press. doi.org/10.1093/oso/9780197601792.003.0004

Weingarten, D. (2020) *Congress receives long-awaited memorandum from White House on Cyber Policy , MeriTalk*. Available at: https://www.meritalk.com/articles/congress-receives-long-awaited-memorandum-from-white-house-on-cyber-policy/#:~:text=National%20Security%20Presidential%20Memorandum%2013,offensive%20cyber%20operations%20are%20approved. (Accessed: 16 April 2023).