Cyber Joint Inter-Agency Task Forces

By Maj. Geoffrey Crawford

How do leaders identify the best cyber capability to achieve an objective? Once identified, how do they quickly and effectively bring the chosen capability to bear? In the current environment, the Army relies on limited Liaison Officer (LNO) relationships, which have long lead times, to access the capability. If the capability or terrain requires interagency support, interpersonal relationships and processes must be established on an ad-hoc basis; however, these relationships typically dissipate once the mission is completed. Operations in the cyber domain are complex, with no geographic limitations on friendly or adversary maneuver. A regional power with limited power projection capabilities, such as Iran or North Korea, can operate at scale in cyberspace; this complicates the requirements placed on regional combatant commands and has an outsized potential of hindering unity of effort when facing nation-states. The United States Central Command (USCENTCOM) Commander will inevitably view and engage Iranian cyber threats differently than the United States Indo-Pacific Command (USINDOPACOM) Commander, and vice versa for North Korean cyber threats. This problem extends outside Department of Defense (DOD) entities, with the National Security Agency (NSA) and CIA approaching cyber threat actors and nation-states differently than DOD forces. There are many stakeholders operating within the cyber domain, including the FBI, NSA, CIA, and DOD. All these stakeholders have their own approaches, goals, and priorities. These differences create an expansive menu of capabilities for national and strategic leaders but make deconfliction and synchronization difficult. The problem facing the DOD and all United States cyber stakeholders is to present a unified force that can operate both synchronously and asynchronously, while deconflicting operations to achieve unity of effort, increasing responsiveness to national and strategic level needs, and preserving freedom of operations. The solution will likely require one or multiple cyber centers of gravity, which would serve as a “one-stop shop” for leaders to find or create the correct capability to quickly and efficiently meet requirements.

Joint Task Force ceremony depicting various branches of services working together. (Photo by Petty Office 1st Class Samantha Jetzer

U.S. national and strategic level leaders face an uphill battle to coordinate and win in cyberspace. The domain and threat landscape constantly change at a speed that does not allow long decision cycles. It is complex, with threats coming from criminals, nation-states, protest groups, and anyone with malicious intent and access to the internet. It is global and requires a high degree of coordination to achieve valuable effects. The capabilities that those leaders can leverage are often disjointed, with little unity in effort or command, and each stakeholder has divergent priorities and objectives. All of this culminates in a domain that is fraught with challenges, which are becoming increasingly vital to navigate in order to operate effectively on the world stage. The centers of gravity would need strong habitual linkages to all stakeholders and the ability to make decisions and allocate resources in order to answer these challenges. By having a center of gravity with these linkages, situational understanding will increase and allow for a single panel of glass for leaders. This will also allow for better information and resource sharing, improving cyber forces’ posture and reducing unnecessary redundancies.

The one-stop shop approach will increase the interconnectedness of stakeholders and allow them to engage threat actors more effectively through a “whole of” government approach. The list of threat actors’ objectives and tactics, tech-

niques, and procedures are varied. New threats present themselves almost daily in cyberspace. Some criminal actors operate for profit and do not directly correlate to U.S. priorities. They can easily hold cyber assets at risk or sell access to nation-state actors. This creates complexity and difficulty in adequately prioritizing defensive assets and creates challenges for keeping pace with a threat landscape that is constantly changing.

Proposed Solution

A solution is the creation of Joint InterAgency Task Forces (JIATFs) that can either be threat or regionally aligned. The Joint Interagency Coordination Group Core Element would consist primarily of NSA and DOD personnel with LNOs, Memorandum of Understandings (MOUs)/Memorandum of Agreements (MOAs), and augmentation from other stakeholders on a permanent, semi-permanent, or as-needed basis. The JIATF would answer to the United States Cyber Command (USCYBERCOM) commander through NSA and USCYBERCOM staffs to answer Secretary of Defense (SECDEF), Combatant Commanders, and State Department requirements. The DOD bill payers to build this organization would be the Joint Force Headquarters-Cyber (JFHQ-C). Like JFHQ-Cs, the JIATF would have operational control of DOD cyber teams and operational control of NSA assets that align with the JIAFT's focus area. The JIATF would operate like an Air Operations Center by deconflicting operations in cyberspace, building mission/target packages, conducting cyber mission planning, and being the primary bridge between the Combatant Commander (CCMD) and cyber forces.

The joint approach has been used to address similar challenges in other areas of the DOD. JIATF-South was established to counter drug trafficking using all-domain capabilities through interagency collaboration and partnering with nations to target, detect, and monitor illicit drug trafficking in the air and maritime domains. They use this collaboration to leverage different authorities, relationships, and intelligence streams to magnify each agency's strengths and increase JIATF-South's effectiveness. Since its inception, JIATF-South has helped to interdict over 100 tons of cocaine annually, which represents approximately 60% of the U.S. Government's successful maritime drug interdictions. The National Cyber Investigative Joint Task Force (NCIJTF) was established in 2008 by National Security Presidential Directive 54, with the primary responsibility of developing and sharing information related to cyber threat investigations across the cyber stakeholder community, while coordinating and integrating associated operational activities to counter adversary based cyber threats. One of the current projects for NCIJTF is developing a capability to maintain awareness of federal computer intrusion investigations and help link cases across agencies. NCIJTF has fostered increased collaboration and uses its members' collective authorities and capabilities to bring available resources to bear against domestic cyber threats. In 2021, NCIJTF was instrumental in coordinating FBI, NSA, and Department of Justice (DOJ) support to operations against the REvil ransomware group; this ultimately led to the seizure of cryptocurrency payments and disruption of the group's infrastructure. These joint interagency formations have increased cooperation and integration while allowing for a whole-government approach to a specific problem set. They leverage relationships and synergy to achieve objectives that none of their components could achieve individually.

Mission and Goals

The mission of the cyber JIATFs would be to plan, synchronize, and coordinate across the cyber domain inside their area of operations and increase access and responsiveness for all capabilities and assets. They will also provide improved shared situational awareness for the entire cyber force, as well as senior leaders. The goal of the JIATFs is to provide responsive and adaptable support to answer regional, strategic, and national priorities; the joint forces will also combat emerging threats in the cyber domain through unity of effort across the whole of government.

In practice, cyber JIATFs would allow Combatant Commanders to have a single point for requesting support and understanding the cyber battlespace in their area of operations. JIATFs can provide subject matter expertise for regional cyber efforts and focal points for emerging threats in their areas of focus. JIATFs would be able to

coordinate amongst themselves to ensure commonality across approaches and engagement with nation-states operating in cyberspace. As an example, a JIATF would help ensure that USINDOPACOM's and USCENTCOM's responses to North Korean cyber actors are synchronized and the best capability or asset is being leveraged. Additionally, the JIATF can create synergy for cyber forces during operations. Instead of a cyber team having to answer Combatant Commander, JFHQ-C, and USCYBERCOM priorities simultaneously, the team can focus on supporting the JIATF's priorities and allow the JIATF, with its staff, to engage outside entities. This focuses the team on the mission instead of navigating different stakeholders' priorities and staff power dynamics.

The cyber JIATF approach to this problem set produces an interesting use case for the Department of Defense Information Network (DODIN). JFHQ-C DODIN is responsible for protecting the Defense Information System Agency's (DISA) infrastructure. JFHQ-C DODIN is not responsible for securing subcomponents of the DODIN, such as DODIN-Army. United States Army Cyber Command (ARCYBER) protects DODIN-Army, and the other services are responsible for their own subcomponents of the DODIN. This creates differing responsiveness to threats and no easy way to coordinate defensive efforts across the subcomponents of the DODIN. Establishing a JIATF-DODIN with responsibilities to operate across the entire DODIN with teams from across the DOD would improve and standardize responses to threats while increasing information sharing for emerging and ongoing response actions. This would enable improved whole-of-government approaches to threats against critical infrastructure. Since JIATF-DODIN would already be strongly integrated with FBI, Homeland Security, and Department of Justice, it would reduce the lead associated with creating a task force to address a crisis. JIATF-DODIN would provide a standardized defense of the U.S. cyber footprint. This would also allow for better use of all authorities to conduct investigations and pursue criminal prosecution when necessary.

Adversary and Ally Approaches

China has already created a whole government approach to cyber domain building, which amounts to a centralized cyber strategy. They focus heavily on commercial and government integration. China actively leverages companies like Huawei and Tencent to conduct cyber espionage and improve their use of technology. The government has bolstered integration through laws, like the National Intelligence Law of 2017, to ensure synergy across all sectors for cyber operations. They use a highly centralized framework with the People's Liberation Army Strategic Support Force (PLASSF) integrating cyber, electromagnetic, and space capabilities to achieve offensive and defensive effects. This deeply integrated approach allows for faster decision-making and easy access to many capabilities. In the current U.S. construct, though the U.S. can achieve similar integration of capabilities, this integration would be slowed by the need to stand up as an ad hoc organization.

Though less centralized, the Russian approach uses many non-state actors and cybercriminal groups to achieve state objectives. They have demonstrated a homogenous approach to using the cyber domain to achieve national objectives like disinformation and destabilizing infrastructure. They attack government and civilian systems to accomplish these objectives through hybrid operations. The U.S. can counter these tactics and improve detection and responsiveness by focusing on better interagency coordination.

The European Union has established the European Union Agency for Cybersecurity (ENISA), which coordinates cybersecurity efforts across member states, focusing on threat intelligence sharing. They have also established the Cyber Crisis Liaison Organization Network (CyCLONe) to facilitate coordination during cyber crises among national Computer Security Incident Response Teams (CSIRTs). These organizations bolster coordination and cooperation to disrupt threat actors and reduce the effectiveness of any threat actor's operation.

The United Kingdom has established the National Cyber Security Centre (NCSC) as part of the Government Communications Headquarters (GCHQ). The NCSC provides a centralized hub for managing cyber incidents, sharing threat

intelligence, and advising public and private sectors during cyber-attacks. The NCSC was instrumental in the UK's response to the WannaCry ransomware attack. The UK also has the National Offensive Cyber Programme (NOCP), which integrates military and intelligence agencies to conduct offensive cyber operations against adversaries.

Many allies and adversaries have identified the need for close cooperation and integration across stakeholders operating in the cyber domain and have established organizations to achieve this effect. These organizations have proven to be enablers that support faster responses, reducing threat actors' effectiveness by allowing cyber forces to be brought to bear more rapidly.

Conclusion

U.S. cyber stakeholders must provide elite capabilities to national and strategic leaders that will enable rapid offensive and defensive actions while providing an easy-to-digest menu of options for those leaders. To combat the increasing attack surface and growing threat in the cyber domain, stakeholders must be able to respond quickly and in coordination with other stakeholders. Historically, this has been ad hoc and only when a need arises, but that lengthens response time and requires a long lead time to facilitate. The decision-making space in cyber is getting shorter, so senior leaders need a fast and reliable way to understand the cyber domain and where friendly forces are operating. Cyberspace requires a whole-of-government approach because of its interconnectedness. Both ally and adversary nations have begun to increase integration among cyber stakeholders, increasing demand for the U.S. to keep pace. The JIATF approach can reduce lead time, reduce redundancy, improve responsiveness, and multiply the effects for stakeholders.

About the author

Maj. Geoffrey Crawford is an an instructor for Cyber Warfare Officer Basic Officer Leaders Course (CWO-BOLC) in the Cyber Training Battalion (CTB). Prior to serving in the CTB, Maj. Crawford attended resident Command and General Staff College (CGSC) at Fort Leavenworth, KS. Before CGSC, he was assigned to the Cyber Protection BDE, where he held positions as a Cyber Protection Team (CPT) Team Lead, battalion S-1, and Mission Element Lead. Maj. Crawford served as a Team Lead for 503 CPT, which supported USINDOPACOM and the Team Lead for 156 CPT, an Army service team focused on Industrial Control Systems technology. He was the Mission Element 1 lead for 91 CPT, which is the only Army team that supports the DoD Information Network (DoDIN).