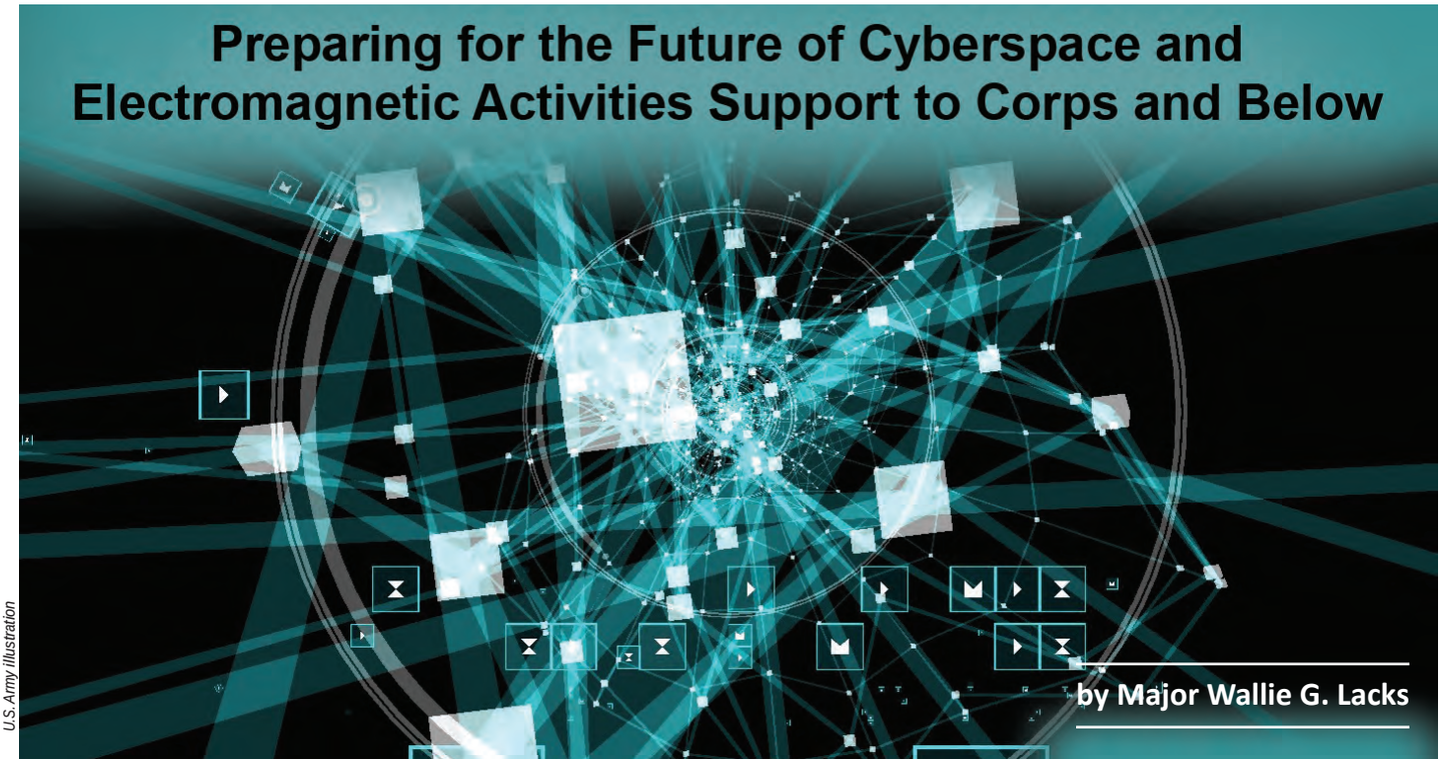
# Preparing for the Future of Cyberspace and Electromagnetic Activities Support to Corps and Below



U.S. Army illustration

The Defense Advanced Research Projects Agency's PlanX program is working to help military cyber operators visualize the cyber battlespace and perform missions there based on an established cyberspace framework and a common operational picture.

by Major Wallie G. Lacks

## Introduction

As a participant in the U.S. Army Intelligence Development Program–Cyber, I often heard much debate about the term "intelligence support to cyber." The phrase itself should be easily understandable and translatable to any intelligence professional. However, I have found that not to be the case. Too often, it breaks down into nondescript ideas of what "support" means. Those ideas often lead to confusing intelligence requirements, further impeding any agreed-upon meaning between intelligence and operational cyberspace planners about support.

As a member of the Combined Joint Task Force–Operation Inherent Resolve's cyberspace electromagnetic activities (CEMA) cell embedded within the joint fires section from December 2017 through July 2018, I came to view the term as a nuanced way of saying, "providing commanders a situational understanding of cyberspace." ADP 6-0, *Mission Command: Command and Control of Army Forces,* defines situational understanding as, "the product of *applying analysis and judgment to relevant information to determine the relationships* among the operational and mission variables" to facilitate decision making.[1] Therefore, the intelligence professional must understand what data is needed to build a situational picture and consider which intelligence elements at the appropriate echelon translate and synchronize the data to ease CEMA utilization into a commander's plan.

## Finding the Intelligence Data

The quote cited from ADP 6-0 is what an intelligence professional must do to turn data into a situational understanding of cyberspace for commanders and staff. Identifying operational and mission variables builds an understanding of a given operational environment.[2] This means building an understanding of how the enemy, friendly, and neutral parties operate in the cyberspace environment. These variables become the refinements necessary in linking the mission facts, constraints, and assumptions of not only probable enemy cyberspace courses of action but also possible friendly actions and counteractions. This requires knowing how to achieve understanding through the arrangement of collected data.

The intelligence professional should arrange data to identify, characterize, and monitor enemy and friendly activity within the cyberspace and electromagnetic spectrum environment. The data necessary to identify, characterize, and monitor enemy and friendly cyberspace activity resides in three keys layers of cyberspace—physical, logical, and cyber-persona.[3] Figure 1 (on the next page) shows these three layers and their relationship to the data collected for analysis to provide situational understanding to CEMA.

**Physical Layer.** The figure visually arranges the data in such a way as to focus it on the end state of situational understanding. The first data point of a cyberspace-collection

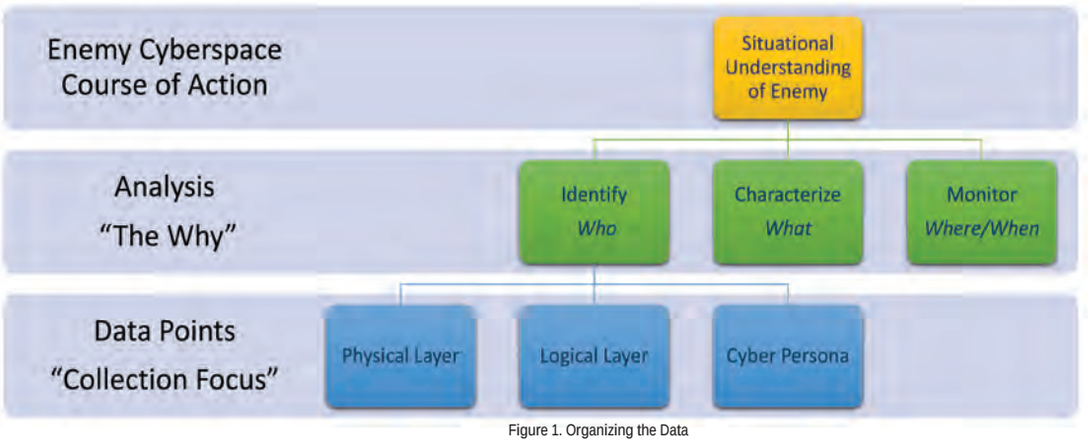



Figure by author

Figure 1. Organizing the Data

focus is the physical layer. The physical layer of cyberspace is just that—physical. It is the location (and components) where elements that create a logical network reside. The physical layer consists of hardware such as computers, smartphones, small office and home office wireless routers, personal Wi-Fi routers, telecommunication fiber hubs, and satellite point of presence. This physical infrastructure is the backbone upon which the logical layer exists.[4]

**Logical Layer.** The next layer is the logical layer. This layer consists of devices allowing data on the physical layer to move between different networks. The devices are physical, but their primary purpose is to support the transportation of data via logical addressing. This address at its most basic concept consists of a source internet protocol (IP) address and a destination IP address. It contains the data that makes up a transmitted message known as the payload. This framed data routes through cyberspace by devices that decipher the best method to get to the destination IP address. This routing is carried out by devices known as switches, routers, or multilayer switches.[5]

These logical layer devices are necessary in allowing data to go from one end user device (computer, tablet, smartphone, etc.) to another end user device across a single or series of networks. The switch electrically and logically connects devices together while the router and/or multilayer switch allows for connections between networks. Understanding the logical addresses and ports used for communications on the devices' operating systems within a network provides a way to visualize a mapped path between networks and end devices.[6]

**Cyber-Persona Layer.** The third layer is the cyber-persona layer. The cyber-persona layer is the digital representation of an individual or entity (organization) operating within cyberspace. This means that the ability to identify, attribute, and act upon individuals and entities is possible. Identities in cyberspace include email addresses, social networks, web forums, and computer IP addresses of end user devices such as tablets, computers, portable computers, smart watches, and mobile device numbers.[7]

The cyber-persona layer can be complex because of its elements that touch multiple virtual locations at once without having a solid link to a physical location or form.[8] The intelligence professional must understand that knowledge gained from any form of targeting or analysis to identify attribution requires significant diligence. This diligence is key to understanding the cyber-persona layer and its linkages to the physical and logical layer. The criticality of summarizing all three layers into an intelligence whole during analysis is the essence of developing the cyberspace situational awareness for commanders. Figure 2 shows this construct.

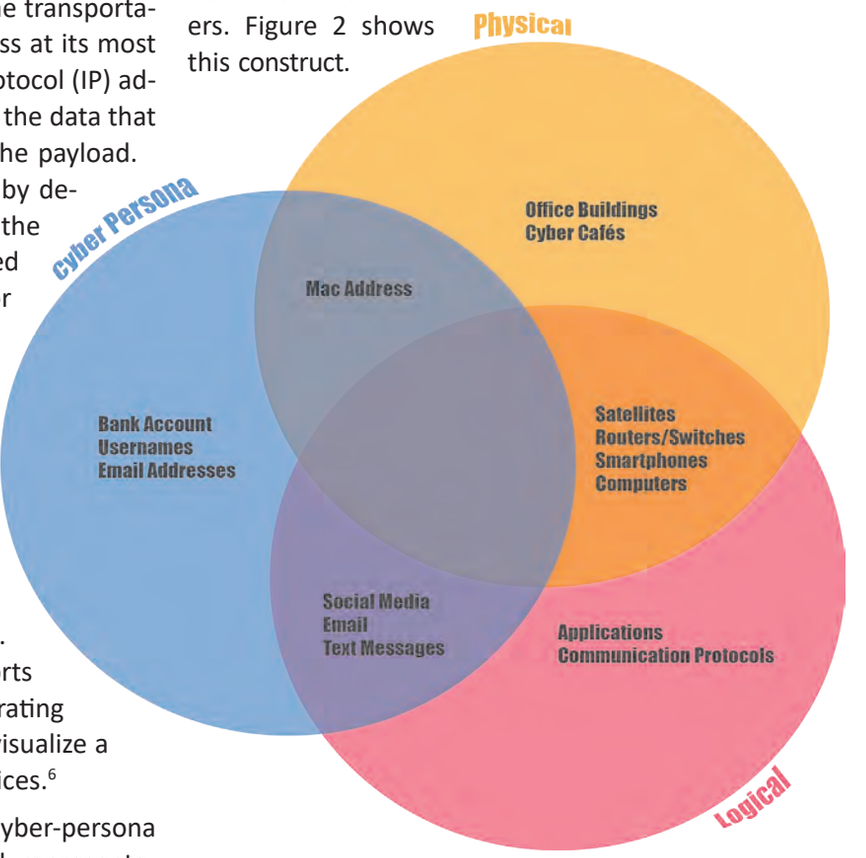



Figure by Jonathan S. Dingler

Figure 2. Understanding the Data

## Arranging the Data

The data-collectable aspects of the physical, logical, and cyber-persona layers of cyberspace are not mutually exclusive to just one form of collection. For instance, an IP address at the logical layer or an email address at the cyber-persona layer can come from either human intelligence (HUMINT) or signals intelligence (SIGINT). Physical locations housing components of a network's physical layer can be collected via imagery, HUMINT, or SIGINT as well. Therefore, an intelligence professional should not fall into the trap of thinking that the information necessary to build a picture should come from only one intelligence discipline.

However, given the nature of the intelligence collection enterprise architecture from the corps level down to the maneuver brigades and battalions, the ability to build a shared situational understanding of cyberspace shrinks at each command echelon. For instance, the intelligence enterprise structure from the corps down through brigade focuses on the land domain and the enemy's physical formations. This makes intuitive sense because lower echelon formations are or should be in constant contact with the enemy in a more kinetic fight. Therefore, the capacity of intelligence database network resources such as the SECRET Internet Protocol Router Network and Joint Worldwide Intelligence Communications System, as well as access to national-level data sets, shrinks as it goes from corps down to divisions and brigades.[9] The ability to build a robust situational understanding of cyberspace and the electromagnetic spectrum becomes ever more difficult the lower in the command echelon it is attempted. It is for these reasons that the corps intelligence staff must be the foundation of the translation point for the enemy's electronic order of battle and cyberspace courses of action for the area of operations.

The corps intelligence section can pull together the infrastructure necessary to cross-collaborate with national agencies as well as lower echelons. Additionally, it is at the corps where the tactical formation's situational awareness of cyberspace needs to begin because of today's cyberspace threat. The corps commander's guidance on offensive and defensive cyberspace operations, based upon awareness from the G-2/G-6, baselines not only the corps but also the echelons down to brigade. This essential guidance begins the process of ensuring cyberspace operations nest from corps to brigade and back up through the corps and into collaborating agencies. It is essential that the translation of the cyberspace fight start at the corps headquarters. The corps intelligence staff is the cornerstone that secures the process of ensuring lower-echelon intelligence staffs account for cyberspace effects while also aiding in shaping tailored processes that incorporate echelon above corps support.[10] This tailored process must be more than just a communications link to the Army Cyber enterprise.[11] Rather, the process must be a well-rehearsed and routinely employed endeavor that operates both in garrison and in the field. Additionally, the established relationship must account for communication with combatant command joint cyber cells. There must also be an understanding of what cyberspace elements (cyber combat mission teams supporting combatant commands) are actively posturing, collecting, and reporting in a potential future corps area of responsibility within a combatant command's region. The corps intelligence staff must also build relationships with the U.S. Army Intelligence and Security Command's theater military intelligence brigade supporting that region.

Theater military intelligence brigade designs can support not only the combatant command and Army theater command but also the corps headquarters. The theater military intelligence brigade intelligence capabilities could serve the purpose of assisting the corps with synchronizing strategic and operational-level intelligence collection and analysis necessary for building an understanding of the cyberspace domain within a corps assigned area of operations. Figure 3 shows this concept and the expected benefits of this construct.

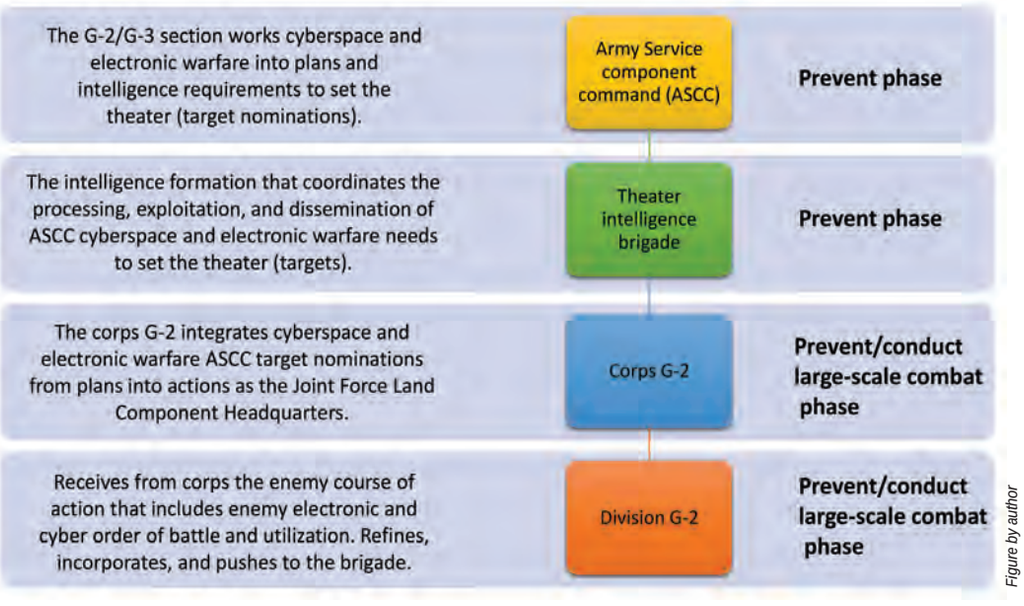



Figure by author

Figure 3. Aligning Intelligence Elements

## Benefits of an Aligned Ensemble

There are both positive and negative aspects to aligning or not aligning where the intelligence translation for cyberspace and electronic warfare begins. The proper aligning of intelligence translation will force intelligence sections to construct and collaborate more in developing virtual target folders for cyberspace effect nomination.[12] This is a critical step in developing targeting aim points against enemy military systems that use cyberspace. Just as critical is that the alignment normalizes intelligence elements at all echelons on how to request, systematize, support, and employ cyberspace-based information efficiently. A solid process set up in this manner would reassure commanders and result in clear cyberspace planning and targeting guidance for the staff.

By not having this solid process, organizations run the risk of pitting cyberspace against unrealistic requirements. Worse, it also results in little to no intelligence development toward a virtual target nomination that should accompany a cyberspace fires request. When intelligence alignment is off and not collecting to build a situational understanding of cyberspace, there is a tendency for cyberspace support requests to read, "Deny the enemy use of the internet on objective A within the next 96 hours." This type of request is indicative of the staff's and commander's limited understanding of the cyberspace domain and all the coordination necessary as it pertains to a tactical problem. It is symptomatic of staffs seeing cyberspace as a dynamic tool that delivers battlefield effects much like other fire support elements rather than a deliberate tool necessitating greater synchronization.

These overly broad requests with no accompanying intelligence information or virtual target targeting folders become cold starts for the cyber force. The basic through advanced target development and intelligence to build the target becomes the task of a small limited intelligence section that supports the cyber mission team. This increases the amount of time the cyber force needs to build an understanding of an adversarial network to deliver effects. It also causes cyber mission teams to have a lack of refined target guidance. This leads to teams being bogged down with additional considerations regarding the target, such as determining the targeted area's redundant internet connectivity. Do you target the internet service provider and its internal infrastructure, the local cellular provider, or the very small aperture terminal satellite points of presence?

Cyberspace operations are not a panacea for all things internet-related. Because of this, the cyber force must go back to the requestor and seek a more refined target aim point. In short, this results in intelligence staff work that should have been conducted during the targeting process, before the request was made, happening after the fact. The outcome is wasted time, effort, and man-hours.

U.S. Army photo

Cyber operations specialists from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), from Fort Gordon, GA, provided offensive cyber operations as part of the Cyber Electromagnetic Activities Support to Corps and Below Program during the 1st Stryker Brigade Combat Team, 4th Infantry Division, National Training Center Rotation 18-03, January 18 to 24, 2018.

## Conclusion

The Army is moving to integrate cyberspace support to tactical formations from the corps level to the brigade. This endeavor will not work unless the intelligence warfighting function understands its role and rethinks *where cyberspace translation begins.* Additionally, if intelligence translation begins at the corps or joint task force level, so too should operational implementation translation.

*Intelligence support to cyber* is the term often used. Yet the intelligence role in cyberspace is much larger than that. Rather, by thinking of how to build a situational understanding of cyberspace for staffs and commanders at the right organizational echelon, intelligence is not only supporting cyber but also easing its utilization and transition from a strategic, operational asset to a tactical tool.

**Endnotes**

1. Department of the Army, Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2019), 2-3 (emphasis added).

2. Department of the Army, Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. GPO, 11 April 2017).

3. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, 8 June 2018), I-3.

4. 30 Bird Media, *CompTIA A+ Certification 220-901/220-902 Comprehensive* (Rochester, NY: 30 Bird Media, 2016), 298, 312, 329.

5. 30 Bird Media, *Network+ Certification Exam N10-006 Student Edition* (Rochester, NY: 30 Bird Media, 2016), 165.

6. Ibid., 174–175.

7. Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations,* 1-13.

8. Ibid.

9. Department of the Army, Army Techniques Publication (ATP) 2-19.3, *Corps and Division Intelligence Techniques* (Washington, DC: U.S. GPO, 26 March 2015), C-3 (common access card [CAC] login required); and ATP 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington, DC: U.S. GPO, 25 June 2021), C-8 (CAC login required).

10. Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below* (Santa Monica, CA: RAND Corporation, 2017), 71–72.

11. Department of the Army, ATP 2-19.3, *Corps and Division Intelligence Techniques,* A-6.

12. Joint Staff, Chairman of the Joint Chiefs of Staff Instruction 3370.01B, *Target Development Standards* (Washington, DC: U.S. GPO, 6 May 2016) (CAC login required).

*MAJ Wallie Lacks is a graduate of the U.S. Army Intelligence Development Program–Cyber. He currently serves as the executive officer of the 308th Military Intelligence (MI) Battalion, 902nd MI Group. His previous cyber-affiliated assignments include Commander, Counterintelligence Cyber Activity, 310th MI Battalion, 902nd MI Group; cyber-planner for the Combined Joint Task Force-Operation Inherent Resolve cyberspace electromagnetic activities (CEMA) team; and deputy CEMA chief, cyber operations, 8th Army G-3 Fires. MAJ Lacks is a graduate of the Joint Network Attack Course and Joint Cyber Planners Course. He has completed A+, NET+, and SEC+ courses and earned certifications in A+ and SEC+.*