Reshaping Intelligence Operations in the Cyberspace Domain

Major General (Ret.) George Franz
Lieutenant Colonel Galen Kane
Lieutenant Colonel Jeff Fair

Cyberspace has become the most active, contested, and congested of the warfighting domains. Both the new National Cyber Strategy and recent Department of Defense (DoD) Cyber Strategy describe an environment wrought with adversaries attempting to gain a military, political, and economic advantage over the United States (US). [1] Given the pace of operations and the rate of change in the environment, new ways of operating develop at a rapid pace. Although DoD has published Joint Publication (JP) 3-12 (Cyberspace Operations) that provides a foundation for understanding cyberspace and operations therein, the Army and Joint Force have a great opportunity (and requirement) to reflect the complexity and fluidity in this new domain and to more fully describe the level of conceptual and practical convergence between the land (physical), human, and cyberspace domains. The Army and Joint Force have the capacity to understand and detail these changes in the land and cyber domains and have the innovative leadership we need to integrate this convergence into our discussions, debates, concepts, and doctrine. The changes involved with the technology and the extent to which cyberspace is impacting the land and human terrain are significant even today. DoD must be bold and innovative to stay ahead of the threat and to take advantage of the tremendous potential that exists.

The critical component of the Joint Force and the Army being able to understand and operate in a converged environment is the Intelligence Warfighting Function. The current ability of intelligence to comprehend and describe this new reality is limited at best. Unless this gap is closed, DoD will continue to be at a decided disadvantage as technological trends continue to shape our world. The need for increased capacity and capability includes analysis, Intelligence, Surveillance, and Reconnaissance and building the ability to clearly articulate what is changing in the converged domains of land and cyberspace.

Major General (Retired) George Franz served as a Military Intelligence Officer at every level from Ground Surveillance Radar Platoon to J2 at the Joint Task Force level, including Command of USA INSCOM. He also worked in Cyber Operations positions as Commander, Cyber National Mission Force and as Director of Operations, USCYBERCOM. He retired in September 2017 with 33 years of active service and continues to support the MI Corps as a Soldier for Life.

To be clear, intelligence operations conducted in the cyber domain do not equate to intelligence support to cyberspace operations. Intelligence support to cyberspace operations build understanding and enable commanders at all levels to plan, equip, organize, and execute successful campaigns in areas determined to be in the national interest.

DoD Convergence Considerations

Former Commander, U.S. Cyber Command and Director of the National Security Agency, General (GEN) Keith Alexander, U.S. Army, described the convergence between the elements of the electromagnetic spectrum and cyberspace, which encompasses networks, signals, digital, analog, information, and data, as a full convergence of the signals environment. Specific to technologic convergence, GEN Alexander further warned of vulnerabilities and challenges created by the signals environment convergence, but this was just the start. From an Army operational perspective, the convergence GEN Alexander envisioned goes much further than just the electromagnetic spectrum and cyberspace, it also includes a full convergence of the land (including the human/cultural dimension) and cyberspace domains. Conditions now reflect a complete fusing of the human terrain with cyberspace. The extent to which people live in and through cyberspace, and the reliance humans now have on cyberspace to conduct a vast majority of routine activities, communications, and transactions. This means the Army, and especially as Intelligence Enterprise professionals, must develop the capability to operate effectively within this evolving operational paradigm. Our understanding of the cyberspace domain and its impact on future conflict must evolve beyond a rudimentary user-level understanding.

From a Unified Land Power or Army Operating Concept (AOC) perspective, this concept of convergence does not diminish the essential aspects of physical

Lieutenant Colonel Galen Kane is a U.S. Army intelligence officer assigned to the Joint Staff J39 and recently completed the U.S. Army War College's Cyber Fellowship at the National Security Agency. He was previously the Commander of the 741st Military Intelligence Battalion and Deputy J2 for the Cyber National Mission Force, USCYBERCOM. He holds a BS from Indiana State University and an MA from Webster University.

land effects, nor does it change the fundamental elements of the land domain–the physical dimension – the Chief of Staff of the Army (CSA) General Mark Milley describes as the "crucible of ground combat" [2] is where the decisive aspects of land operations occur. The concepts outlined in the AOC establish the framework within which the Army will design its intelligence capabilities. In recent Congressional testimony, GEN Milley called for greater investment in cyber, Big Data, and networks and while the CSA's clear top priority is readiness, he indicated that "our number two priority is to invest in the technologies, organization, and doctrine that will allow us to maintain overmatch." [3]

A Converged Intelligence Approach

The U.S. Army and Joint Force are fully emerged in the cyber domain — every Soldier is a sensor, and these organizations have connected the individual to information networks in ways not previously envisioned. Equally fundamental to this land-human-cyber convergence is the nature of the terrain that we as an Army must operate in and are expected to understand and dominate. The depth of land-human-cyber convergence and the breadth of this condition across the globe means that wherever the Army and Joint Force will operate, we will deal with populations that are land-cyber converged. Every enemy, adversary, and competitor will operate in and exploit this converged land-human-cyber terrain to their advantage.

Doctrine already provides a structure with which to understand a converged environment. JP 3-12 describes the cyberspace domain as having three layers: 1) physical, 2) logical, and 3) cyber-persona. These three layers are used to define the environment, provide analysis on what resources the adversary utilizes, how it maneuvers, and operates throughout the three levels. What is clear from this is that the physical, as defined, encompasses land and land-based

Lieutenant Colonel Jeff Fair is a U. S. Army intelligence officer assigned to the USCYBERCOM/NSA Combined Action Group. He holds an MPA from the University of Washington's Evans School, an MBA from Hawaii-Pacific University, a MSSI from the National Intelligence University, and a BA from the George Washington University's Elliott School of International Affairs. He is a Ph.D. student at George Washington University's Trachtenberg School of Public Policy and Administration.

components. The aspect that requires additional development is the persona element. Intelligence professionals must take the initiative to capture the depth and breadth to which the human and cyber aspects are converged. It is possible for one individual to have multiple cyber personas. Due to the complexity of cyber personas, attributing responsibility or making an identification can be a very challenging task. In other words, the people among who we will operate are inseparable from the cyber-persona they live through.

For the Intelligence Enterprise specifically, this new operating model allows the Army to do a full and fundamental re-look of all current intelligence disciplines and concepts. The actions we take on land cannot be separated from those things we do in cyberspace–Army intelligence professionals must think of cyber-intelligence as a converged concept and related set of actions. All actions, analysis, and products must have a linked, fully integrated land-human-cyber core, which requires reconsidering all the intelligence disciplines, adjusting the intelligence cycle, and then pursuing opportunities to ensure a full appreciation of the land-human-cyber domain in our operational design.

Converged Army Intelligence

To inculcate the Army and the Joint Force into converged thinking, it should be integrated across the DOTMILPF. From an Army Intelligence perspective, the next place to reflect this new capstone concept could be foundational doctrine; Army Doctrine Reference Publication 2-0 (Intelligence). The following are ways that our doctrine could describe each intelligence discipline and its relationship to cyberspace:

- **All-Source Intelligence:** In a converged environment, all sensors must be integrated across multiple domains to build a reliable, accurate picture.

This begins with creating all source analysts that possess a detailed understanding of cyberspace. A July 2017 assessment by the United States Army Intelligence Center of Excellence determined that "to propose viable and worthwhile threat courses of action in cyberspace, all-source intelligence analysts require a true understanding of the Cyberspace Domain and the kinds of operations that threat actors perform in cyberspace to achieve different objectives." [4] The approach to all-source intelligence must expand to incorporate the significant information available that pertains to the cyberspace domain, particularly network data that is currently seen as defensive or administrative. All sources must include operational reporting from network operators and administrators, just as operational forces report combat information on the ground.

Just as every Soldier is a sensor, then every network sensor must be integrated as a potential intelligence sensor. The Cyber ISR system must incorporate network data collected from the wide array of security and information assurance sensors such as the Host Based Security System and others. Network operators must also be more effective in reporting a threat or potential threat activity, using the established report formats and mechanisms that will enable ingestion of combat network data into the intelligence processing, exploitation, and dissemination (PED) enterprise.

- **Signals Intelligence (SIGINT):** The signals and information environments are fully converged, although conventional legacy communications that, in many cases, are used to defeat or protect from our current signals collection capability must be addressed and updated. Even as cyber forces develop their combat (Title 10) collection capabilities, SIGINT will remain the most vital component of the ISR system. SIGINT is recognized as a primary driver for operations within the cyberspace operating environment, but the fusion of all sources of intelligence is critical to disrupting or defeating adversaries.
- **Human Intelligence (HUMINT):** Almost every human on the planet now has multiple cyber-personas to match their physical/actual identity requiring that all HUMINT operations account for the whole person/persona synthesis as a target. The tactics, techniques, and procedures (TTPs) for all aspects of HUMINT operations must integrate activities in both the land and cyber domains. As much of valuable intelligence information is now passed via electronic means, the cyberspace aspects of HUMINT will become the main effort, with physical activities becoming a deliberate enabler for virtual/cyberspace access development.
- **Open-Source Intelligence (OSINT):** Open source data is becoming the timeliest and potentially, the most lucrative form of intelligence as rate the level of data produced by individuals increases daily. Given the difficulties in accessing encrypted data and recognizing the effects of unauthorized public disclosure of classified information, we will have to rely on more widely accessible data in this new era. Our ability to collect process, exploit, and disseminate social media information, open source data, and commercial

and personal imagery, will be a critical aspect of Indications and Warning, Intelligence Preparation of the Battlefield, developing situational awareness, and cueing more sensitive and precise collection systems.

- **Counterintelligence (CI):** It is also clear that the enemy is fully exploiting cyber-space and the weaknesses in our network defenses to their advantage. Everyday threat intelligence services and other adversaries attempt to penetrate our networks and collect valuable information. In many cases, the enemy uses personal contact and HUMINT targeted spear-phishing as the means to establish cyber access and, while the days of dead-drops and microfilm are not entirely gone, the vast majority of collection against the U.S. Government and Army is accomplished through cyberspace. The Army must take a hard look as it executes CI operations, how it trains and employ the force, and how it establishes much tighter links between the network operators, defenders, and CI agents. While there is still a vital need for covering agents, face-to-face contact, threat awareness briefs, and walk-in reporting, intelligence organizations must expand their presence and operational capabilities to defeat the enemy pouring through the cyber gap.
- **Geospatial Intelligence (GEOINT):** This discipline will continue to play a vital role in cyberspace intelligence, with the cyberspace physical aspects being most commonly associated with GEOINT. Geography and location are still core elements of Unified Land Operations and the AOC and, as long as the current model of international governance recognizes land borders, the Intelligence Warfighting Function will provide the geographic location and precision in targeting required for military operations. To ensure effective geospatial support to cyber operations, we must develop the means to geolocate network activity, to track actions in both network time and space, and establish the means for PED that can support decision makers and operations.
- **Targeting:** From a practical perspective, targeting comes down to our ability to effectively achieve effects and impact in cyberspace in support of combined armed operations, across multiple domains. We must be able to target for precision Intelligence, Surveillance, and Reconnaissance, CI, Information Operations, and across the full range of military operations. The Department of Defense has spent years developing the TTPs for targeting in support of combatant command operations, and this remains an incredibly difficult task.

The Convergence Imperative

As early as 2013, BG Jeff Smith, U.S. Army, captured the concept of land-cyber convergence, but his white paper was ahead of its time. [5] Six years later, the Army has moved forward with the creation of the Cyberspace Operations Branch, the establishment of the Army Cyberspace Center of Excellence, Army Cyber Institute, and the growth of Army Cyber Command (ARCYBER) as a fully capable Army Service Component Command, validating much of BG Smith's work. In addition to the publication of JP 3-12, the release of Field Manual 3-12 (Cyberspace and Electronic Warfare Operations) in April 2017, and the AOC, as well as the increased level of awareness of cyberspace across the Army and Joint Force has established conditions that allow a much more complete and holistic approach to a land-human-cyber concept. We should be aggressive and bold in our approach, or we risk failing to provide useful intelligence to support and drive operations in the complex environment as it now exists. We must rapidly proliferate this concept across Army and Joint Force doctrine and concepts. To drive successful operations in the cyber domain, Intelligence must continue to be Always Out Front.

DISCLAIMER

The views and opinions expressed in this paper and/or its images are those of the author(s) alone and do not necessarily reflect the official policy or position of the U.S. Department of Defense (DOD), U.S. CYBERCOM, or any agency of the U.S. Government. Any appearance of DoD visual information for reference to its entities herein does not imply or constitute DOD endorsement of this authored work, means of delivery, publication, transmission or broadcast.

NOTES

1. The White House, "National Cyber Strategy," Washington, DC, September 20, 2018. United States Department of Defense, "2018 Department of Defense Cyber Strategy Summary," Washington, DC, September 2018.
2. Chief of Staff of the Army General Mark A. Milley, "39th Chief of Staff of the Army Initial Message to the Army, " memorandum for the U.S. Army, Washington, D.C., September 1, 2015.
3. Sydney J. Freedberg Jr., "Gen. Milley to SASC: World Getting Worse, Army Getting Smaller," July 21, 2015, https://breakingdefense.com/2015/07/gen-milley-to-senate-world-getting-worse-army-getting-smaller/, accessed May 10, 2018.
4. United States Army Intelligence Center of Excellence, "Intelligence Support to Defensive Cyberspace Operations and DoD Information Networks (ISDD) Assessment," Fort Huachuca, AZ, July 17, 2017. 37. (Classified).

5 U.S. Department of the Army, *The U.S. Army Land Cyber White Paper* 2018-2030, Fort George G. Meade, MD: U.S. Army Cyber Command/2nd U.S. Army, September 9, 2013.