BULLETIN

16-13

APR 16

Cybersecurity Operations:

Observations; Lessons; and Tactics, Techniques, and Procedures Cyber Bulletin No. 2

U.S. UNCLASSIFIED
FOR OFFICIAL USE ONLY

Handling Instructions for Cyber Center of Excellence (CoE) Electronic Media and Paper Products

The United States (U.S.) Army Cyber Center of Excellence (CoE) authorizes official use of this bulletin for operational and institutional purposes that contribute to the overall success of U.S. government efforts. The information contained in this product is provided for informational purposes only and is not necessarily approved U.S. Army policy or doctrine.

This product is designated for official use by U.S. government personnel and their approved contractors. It cannot be released to allies, coalition partners, or the public without the consent of Cyber CoE. This product has been furnished with the expressed understanding it will be used for official defense-related purposes only; and it will be afforded the same degree of protection that the U.S. affords information marked "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" in accordance with U.S. Army Regulation (AR) 380-5, section 5-2. Official military personnel, civil service/government personnel, and approved contractors of the U.S. may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official U.S. government products or research.

However, integration of Cyber CoE "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" information into official products or research renders them FOUO, and they must be maintained and controlled within official channels or approved contractor facilities and cannot be released to allies, coalition partners, or the public without the consent of Cyber CoE. Cyber CoE "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents may be placed on protected UNCLASSIFIED intranets within military organizations or units, provided access is restricted through user identification and password or other authentication means to ensure only properly accredited military, government officials, and approved contractors have access to Cyber CoE "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" materials.

Regulations strictly forbid posting Cyber CoE "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" documents to Army Knowledge Online or other Department of Defense (DOD) websites that do not restrict access to authorized personnel. AR 25-1, 25 Jun 2013, Army Information Technology and DOD Web Site Administration Policy and Procedures (11 Jan 2002) require appropriate mechanisms to protect sensitive information. DOD 5400.7-R, Freedom of Information Act (FOIA) Program, 1 Sep 1998, provides guidance on the release, safeguard, and unauthorized disclosure of FOUO information.

Appropriate disciplinary action may be taken against those responsible for the unauthorized release of FOUO information. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against those responsible for the release; in addition unauthorized releases by contractor personnel to unauthorized persons may warrant action relative to the contractor under the Federal Acquisition Regulation (FAR).

When no longer needed, all Cyber CoE "U.S. UNCLASSIFIED, For Official Use Only [FOUO]" paper products and electronic media will be shredded or destroyed using approved paper shredders or CD-ROM destroyers.

Cyberspace Operations: Observations; Lessons; and Tactics, Techniques, and Procedures Cyber Bulletin No. 2

DIGITAL VERSION AVAILABLE

A digital version of this CALL publication is available to view, download, or reproduce from the CALL restricted website, <https://call2.army.mil>. Reproduction of this publication is welcomed and highly encouraged.

Common Access Card (CAC) or Army Knowledge Online (AKO) login is required to access the digital version.

Foreword

(FOUO) This is one of many cyberspace bulletins originating from the United States Army Cyber Center of Excellence. This edition of the cyberspace bulletin is an institutional vehicle that can be used to share insights, lessons, and observations with others in the field in hopes of providing a common view of cyberspace operations, such as electronic warfare and Signal Corps topics.

(FOUO) As joint regional security stacks are rolled out and we become more knowledgeable of their framework, I cannot help but consider the similarities between the Army's portion of the Department of Defense information network (DODIN) and the Hubble Space Telescope. Both cost millions of dollars and were platforms that enabled critical downstream operations. The Hubble Space Telescope was launched with an optical mirror flaw that made it unable to focus, causing great distress to the National Aeronautics and Space Administration teams that engineered, built, launched, and operated it. Upon investigation, it was determined that leaders did not effectively coordinate between organizations and pressure on the highly technical teams lead to over-rationalization of key problems that should have been reported to senior leaders. The moral of this story for us, as we build the Army's portion of the DODIN is clear, every member of team cyber must have agency in the mission. Leaders must collaborate and coordinate across teams and individual problems should not be rationalized away to avoid unwanted scrutiny of internal processes.

(FOUO) Handling problems at the lowest level is a good philosophy, but when coupled with communication failures across teams, as was the case for the Hubble project, the result can be complete mission failure. The DODIN is our warfighting platform and it needs to be aggressively protected and extended to enable mission accomplishment at all levels. Therefore, at the United States Army Cyber Center of Excellence, we are working hard to change the culture of cyberspace operations to ensure everyone is included in our processes. This is the reason for the production of Cyberspace Bulletin No. 2, to ensure collaboration occurs to the maximum extent possible, apply the lessons learned from the Hubble Space Telescope, and roll out our portion of the DODIN effectively and safely in support of commanders at all echelons.

Mark A Mollenkopf

Mark A. Mollenkopf
CW5, CY
CCWO, Cyber Center of Excellence

Cyberspace Operations: Observations; Lessons; and Tactics, Techniques, and Procedures
Cyber Bulletin No. 2

Table of Contents

Center for Army Lessons Learned

Director	**COL Paul P. Reese**
CALL Analyst	**Bruce Adams**
Contributing Authors	**LTG L.D. Holder (Retired)** **Victor J. Delacruz, Cyber Center of Excellence** **Rick San Miguel, Cyber Center of Excellence** **MAJ Heather Fisk, National Training Center** **CW3 Robert Sullivan, National Training Center**

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications (other than CALL publications) referenced in this product, such as ARs, ADRPs, ADPs, ATPs, FMs, TMs, etc., must be obtained through your pinpoint distribution system.

Introduction

(FOUO) This edition of the Cyber Bulletin continues the discussion from the first edition that emphasized tactics, techniques, and procedures (TTP) for conducting cybersecurity at the brigade level. This bulletin focuses on an initial set of observations, lessons, and emerging TTP on Army cyberspace operations at echelons of corps and below. Throughout the operations process, commanders and staffs are assuming increased responsibilities to plan, coordinate, and synchronize cyberspace operations in support of unified land operations. This bulletin will aid commanders in effectively incorporating cyberspace operations into their units' daily operations and culture.

(FOUO) The information in this bulletin is presented in two ways. First, in Chapter 1, *Cyberspace Observations and Lessons,* lessons are consolidated to clarify the linkages of initial observations to the development of emerging TTP. Second, information is presented as articles in Chapter 2, *Cybersecurity Observations at the National Training Center*; Chapter 3, *Doctrine for Cyberspace Operations*; and Chapter 4, *Commander's Integration of Cyberspace Operations,* that expand on and emphasize individual and collective tasks for integrating cyberspace operations throughout planning, preparation, execution, and assessment of combat operations. Awareness and implementation of TTP identified in this bulletin can assist Army commanders and staffs as they observe common challenges while incorporating cyberspace operations throughout the operations process. Many of these TTP will be addressed further in Field Manual 3-12, *Army Cyberspace and Electronic Warfare Operations,* when published.

(FOUO) **Note**: The terminology LandWarNet is synonymous with the phrase "the Army's portion of the Department of Defense information network [DODIN]." This bulletin uses the terms interchangeably. LandWarNet is currently used throughout Army doctrine. However, in some situations, it is more appropriate to refer to the Army's portion of the DODIN. In these instances, readers should be aware of this terminology. Future doctrine relating to cyberspace operations will clarify these terms.

Chapter 1

Cyberspace Observations and Lessons

Victor Delacruz and Rick San Miguel
United States Army Cyber Center of Excellence

(FOUO) In summer 2012, the Army began to focus on training and integrating cyberspace operations at echelons of corps and below. The combat training centers incorporated cyberspace operations into scenarios designed to drive rotational training units and training audiences to plan, coordinate, synchronize, and integrate cyberspace operations into unified land operations. Their efforts were hindered by a lack of required resources (e.g., specialized personnel and related equipment) and limited doctrine (e.g., minimal information on tactics, techniques, and procedures [TTP] for cyberspace operations). Considerable progress has been made in these areas but many challenges remain.

(FOUO) Army doctrine first codified cyberspace operations in Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command*, 17 MAY 2012. The primary staff task to "conduct cyber electromagnetic activities (CEMA)," emphasized the relationship between cyberspace and the electromagnetic spectrum. Cyberspace operations as a new mission set for the Army required, at a minimum, coordination and deconfliction with electronic warfare (EW) and spectrum management operations.

(FOUO) Center for Army Lessons Learned publication 14-06, *Cyber Bulletin No. 1*, published in May 2014, represented the Army's first effort to capture observations and put forth emerging TTP specific to incorporating cyberspace operations throughout the Army operations process. *Cyber Bulletin No. 2* builds on the previous bulletin and discusses three major categories of observations. These categories of observations are not all inclusive; there are other categories in various stages of development. However, these three categories are most representative of the top challenges units face today when integrating cyberspace operations. The following three categories were derived from observations made during home-station training events, combat training center rotations, and other events where units had to incorporate cyberspace operations throughout the operations process:

- Coordinating and synchronizing staff to enable cyberspace operations
- Developing planning products for cyberspace operations
- Applying the intelligence process and developing intelligence products

Coordinating and Synchronizing Staff to Enable Cyberspace Operations

(FOUO) Units require continuous training to develop and sustain high levels of proficiency in performing staff coordination and synchronization to achieve common understanding. ADRP 6-0 explains, "a critical challenge for commanders, staffs, and unified action partners is creating shared understanding of their operational environment, the operation's purpose, problems, and approaches to solving them." Staff coordination and synchronization to enable cyberspace operations involves a broader problem and opportunity set, and, therefore, adds to existing challenges when developing shared understanding.

(FOUO) Observations and insights indicate that units have difficulty planning, coordinating, synchronizing, and integrating cyberspace operations. Primary reasons for these difficulties include:

- A lack of a fully manned and functioning coordinating staff section (e.g., CEMA element/section) responsible for incorporating cyberspace operations and EW
- A limited ability to develop and disseminate a common operational picture that includes cyberspace (e.g., cyberspace situational understanding)
- Limited opportunities to integrate cyberspace operations during key battle rhythm events (e.g., working groups)

(FOUO) Table 1-1 lists observations that reflect unit challenges during staff coordination and synchronization for enabling cyberspace operations.

Table 1-1. Sample observations

(FOUO) The commander decided to hold only lethal and nonlethal working groups. A CEMA working group was not added to the unit's battle-rhythm events resulting in partial coordination efforts by the EW officer, targeting officer, and others involved.

(FOUO) Synchronization of cyberspace effects was often coordinated outside the unit course of action analysis (i.e., war game) and target synchronization meetings. These unit meetings were consumed by working through the scheme of maneuver. Cyber effects were later "bolted on" to key events within the scheme of maneuver.

(FOUO) CEMA was not replicated at the joint task force/division level. Although the rotational unit built and utilized a CEMA section, there was no similar fusion effort to vet its collaboration at the division level. Fires stayed in the fires lane, the EW officer stayed in the EW officer lane, cyber stayed in the cyber lane, signal stayed in the signal lane, and military information support operations (MISO)/information operations (IO) stayed in the MISO/IO lane.

(FOUO) There is currently a lack of standard language and terminology for cyberspace operations. This situation complicates staff interaction across warfighting functions and with cyber planners who are external to the organization (e.g., offensive cyberspace operations planners).

Lessons and Tactics, Techniques, and Procedures

(FOUO) The challenges associated with staff coordination and synchronization of cyberspace operations can be partially addressed through improved understanding and implementation of current doctrine (e.g., Joint Publication [JP] 3-12, *Cyberspace Operations*, 05 FEB 2013; JP 6-0, *Joint Communications System*, 10 JUN 2015; Field Manual [FM] 6-0, *Commander and Staff Organization and Operations*, 05 MAY 2014; FM 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014; FM 6-02, *Signal Support to Operations*, 22 JAN 2014; and Army Techniques Publication [ATP] 3-60, *Targeting*, 07 MAY 2015). Chapter 3 of this bulletin, *Doctrine for Cyberspace Operations*, has additional information on current and emerging doctrine.

Commanders can emphasize staff coordination and synchronization to enable cyberspace operations in a variety of ways. For example, they can establish training objectives focusing on CEMA tasks codified in ADRP 1-03, *Army Universal Task List*, 02 OCT 2015. Army tactical task 5.9, "Conduct Cyber and Electromagnetic Activities," provides guidance on mission essential task list development.

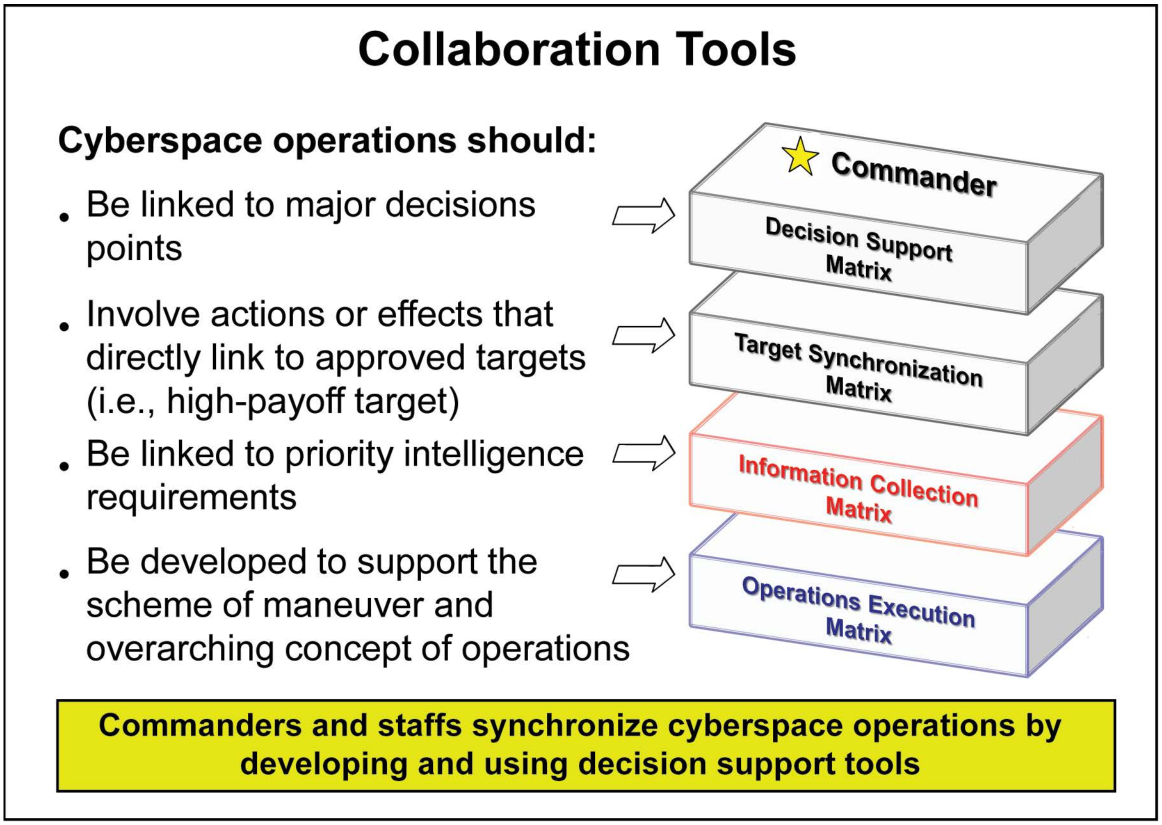
(FOUO) Table 1-2 lists TTP that further address challenges associated with staff coordination and synchronization to enable cyberspace operations.

Table 1-2. Recommended TTP

(FOUO) Units should establish and conduct battle-rhythm events (e.g., working groups, targeting meetings, and synchronization meetings) that include cyberspace operations coordination and synchronization. All CEMA staff principals (i.e., assistant chief of staff, intelligence [G-2]/intelligence staff officer [S-2], assistant chief of staff, operations [G-3]/ operations staff officer [S-3], assistant chief of staff, signal [G-6]/signal staff officer [S-6], EW officer/CEMA element, IO officer/element, chief of fires/fires cell, and space officer/ space support element) should be required to participate in these events. When appropriate, these events should be conducted in sensitive compartmented information facilities to enable full CEMA coordination, synchronization, and collaboration.

(FOUO) Units should schedule and conduct CEMA synchronization meetings to improve vertical command and staff integration and related collaboration among the evolving cyberspace operations community. This will allow CEMA staff principals to collaborate more effectively with higher headquarters and subordinate unit counterparts while maintaining cyberspace situational understanding. For consistency with targeting cycle events (e.g., assessment working groups), these CEMA synchronization meetings should include specific personnel and follow an established agenda.

(FOUO) Commanders and staffs should develop and use decision support tools to aid in synchronizing cyberspace actions and effects, outlined in Figure 1-1 on page 6. Because these tools are part of the operation order (OPORD), a fragmentary order (FRAGORD) is issued whenever there are significant updates. Additionally, these tools should be maintained at all three levels of classification.



Collaboration Tools

Cyberspace operations should:

- Be linked to major decisions points
- Involve actions or effects that directly link to approved targets (i.e., high-payoff target)
- Be linked to priority intelligence requirements
- Be developed to support the scheme of maneuver and overarching concept of operations

Commander

Decision Support Matrix

Target Synchronization Matrix

Information Collection Matrix

Operations Execution Matrix

Commanders and staffs synchronize cyberspace operations by developing and using decision support tools

Figure 1-1. Decision support tools

Developing Planning Products for Cyberspace Operations

(FOUO) Units plan for cyberspace operations using two main Army planning methodologies: the military decisionmaking process (MDMP) and the targeting process. Key outputs from the MDMP for cyberspace operations are included in the following portions of the OPORD: Annex B, Intelligence; Appendix 12, Cyber Electromagnetic Activities, of Annex C, Operations; and Annex H, Signal. These outputs provide key information for conducting cyberspace operations. They should nest with higher headquarters' guidance in order to provide clear direction for subordinate unit actions. See FM 6-0 for additional information on where and how CEMA appears in the OPORD.

(FOUO) Observations and insights indicate that commanders and staffs are planning and coordinating cyberspace operations and EW with increasing success. They are receiving inputs, analyzing and processing these inputs, and producing outputs during the planning process (e.g., CEMA running estimate, CEMA appendix, cyberspace topologies/overlays, and cyber effects request formats). However, many of these outputs have varying degrees of completeness and utility for conducting cyberspace operations and EW. Primary reasons for this include:

- An insufficient amount of cyberspace doctrine providing detailed TTP

- Limited information from higher headquarters (e.g., OPORDs and FRAGORDs) directing or otherwise informing employment of cyberspace operations

- Limited ability to develop a common operational picture inclusive of cyberspace operations that enable staff planning and coordination

(FOUO) Table 1-3 lists observations gathered during cyberspace operations planning events.

Table 1-3. Sample observations

(FOUO) The higher headquarters OPORD required more specifics regarding CEMA. The OPORD lacked contextual details supporting cyber activity, threats, and possible targeting, resulting in numerous requests for information from subordinate units.

(FOUO) The unit developed a CEMA appendix and later briefed a CEMA concept of support. Neither products were detailed enough to conduct operations. There were few targets identified for cyberspace effects. The planning outputs were not well nested with the unit's scheme of maneuver and scheme of fires.

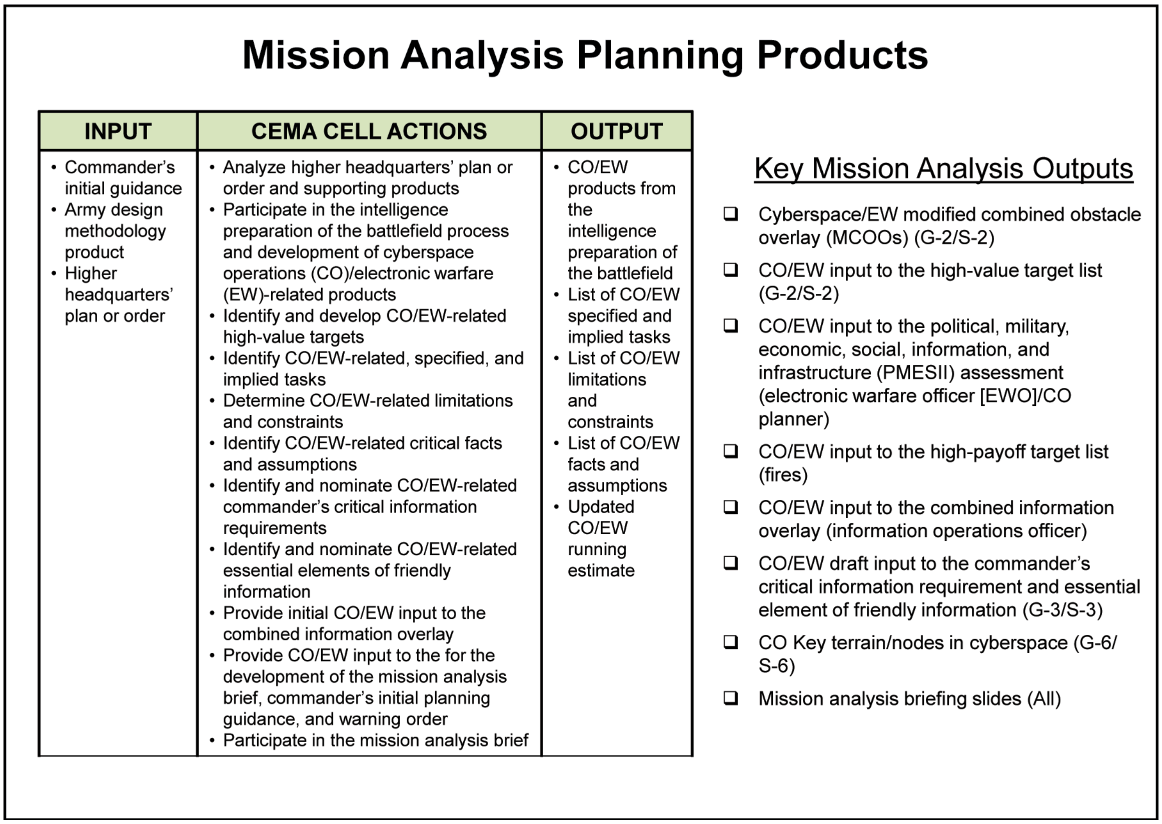
(FOUO) The S-6 was not part of the planning process. Also, the S-6 did not take part in the intelligence preparation of the battlefield (IPB) or targeting process. The S-6 took actions to defend his network, but he did not provide information for intelligence refinement or follow-on targeting data.

(FOUO) There was a lack of cyber situational understanding and an accompanying cyber common operational picture. This undermined the unit's ability to have a common view of its overall cyber signature to support operational decisions.

Lessons and Tactics, Techniques, and Procedures

(FOUO) Although planning methodologies are described in considerable detail in joint and Army doctrine, planning techniques for cyberspace operations are in early development. FM 3-12, *Army Cyberspace and Electronic Warfare Operations,* when published, will discuss tactics and procedures for planning cyberspace operations and EW using the MDMP and targeting processes. Additionally, future ATPs will address proven practices and methods to further guide planning, coordination, synchronization, and integration of cyberspace and EW operations.

(FOUO) Numerous planning aids exist that can assist commanders and staffs in their efforts to develop and implement cyberspace operations and EW planning outputs. Many of these planning products are available on the Army Training Network website at https://atn.army.mil. Figure 1-2 provides a mission-analysis, best-practice product for integrating cyberspace operations and EW early in the planning process.



Mission Analysis Planning Products

INPUT	CEMA CELL ACTIONS	OUTPUT
• Commander's initial guidance • Army design methodology product • Higher headquarters' plan or order	• Analyze higher headquarters' plan or order and supporting products • Participate in the intelligence preparation of the battlefield process and development of cyberspace operations (CO)/electronic warfare (EW)-related products • Identify and develop CO/EW-related high-value targets • Identify CO/EW-related, specified, and implied tasks • Determine CO/EW-related limitations and constraints • Identify CO/EW-related critical facts and assumptions • Identify and nominate CO/EW-related commander's critical information requirements • Identify and nominate CO/EW-related essential elements of friendly information • Provide initial CO/EW input to the combined information overlay • Provide CO/EW input to the for the development of the mission analysis brief, commander's initial planning guidance, and warning order • Participate in the mission analysis brief	• CO/EW products from the intelligence preparation of the battlefield • List of CO/EW specified and implied tasks • List of CO/EW limitations and constraints • List of CO/EW facts and assumptions • Updated CO/EW running estimate

Key Mission Analysis Outputs

- ❑ Cyberspace/EW modified combined obstacle overlay (MCOOs) (G-2/S-2)
- ❑ CO/EW input to the high-value target list (G-2/S-2)
- ❑ CO/EW input to the political, military, economic, social, information, and infrastructure (PMESII) assessment (electronic warfare officer [EWO]/CO planner)
- ❑ CO/EW input to the high-payoff target list (fires)
- ❑ CO/EW input to the combined information overlay (information operations officer)
- ❑ CO/EW draft input to the commander's critical information requirement and essential element of friendly information (G-3/S-3)
- ❑ CO Key terrain/nodes in cyberspace (G-6/S-6)
- ❑ Mission analysis briefing slides (All)

Figure 1-2. Sample best-practice product for planning

(FOUO) The key mission analysis outputs shown in Figure 1-2 are developed by one or more of the CEMA staff principals (i.e., G-2/S-2, G-3/S-3, G-6/S-6, EW officer/CEMA element, IO officer/element, chief of fires/fires cell, and space officer/space support element). These outputs are foundational planning products that inform course of action development and eventual course of action approval.

(FOUO) Table 1-4 provides TTP that further address challenges associated with developing planning products for cyberspace operations.

Table 1-4. Recommended TTP

(FOUO) Units should conduct political, military, economic, social, information, infrastructure, physical environment, and time analysis focusing on cyberspace within the designated area of interest. See JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, 21 MAY 2014; ADRP 5-0, *The Operations Process*, 17 MAY 2012; and FM 6-0 for detailed information on the operational variables.

(FOUO) Units should determine key terrain in cyberspace. See Figure 1-3 showing key terrain in cyberspace. A list of key terrain in blue network space (friendly force) should detail those nodes and devices critical to the operation of the mission command system and most likely to be targeted by adversaries. A list of key terrain in red network space (enemy) should detail those nodes and devices that friendly forces seek to take action or create effects. Last, a list of key terrain in grey network space should detail nodes and devices that may be used by friendly force, adversaries, or neutral actors. These lists should be maintained in running estimates and included in orders where appropriate.

(FOUO) Develop target folders for each target nomination involving cyberspace operations. Apply doctrinal guidance from JP 3-60, *Joint Targeting*, 31 JAN 2013, that emphasizes the design and use of the electronic target folder. Also apply techniques from ATP 3-60 in target vetting and validation. Target folders may suffice for concept of operations, which may be used as supporting enclosures in the cyber effects request format. Maintain and update target folders in digital and hardcopy form to facilitate collaboration in various settings.

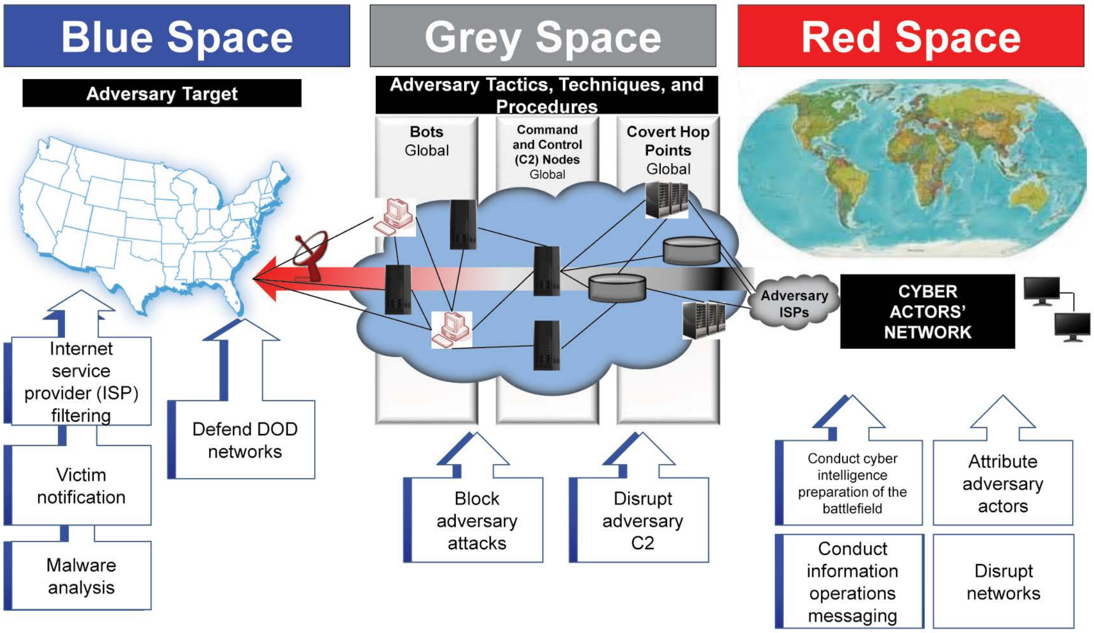

Blue Space
Adversary Target
Internet service provider (ISP) filtering
Victim notification
Malware analysis
Defend DOD networks
Grey Space
Adversary Tactics, Techniques, and Procedures
Bots Global
Command and Control (C2) Nodes Global
Covert Hop Points Global
Block adversary attacks
Disrupt adversary C2
Red Space
Adversary ISPs
CYBER ACTORS' NETWORK
Conduct cyber intelligence preparation of the battlefield
Attribute adversary actors
Conduct information operations messaging
Disrupt networks

Figure 1-3. Key terrain in cyberspace

Applying the Intelligence Process and Developing Intelligence Products

(FOUO) Units understand that operations in cyberspace rely on a constant flow of timely and accurate intelligence that can result in the ability to "see the enemy." With this understanding and awareness of cyberspace, units can more effectively integrate cyberspace operations to achieve the commander's objectives in support of unified land operations. The Army intelligence process (i.e., plan and direct, collect, produce, and disseminate) guides and informs intelligence support to cyberspace operations.

(FOUO) Observations and insights indicate that units are applying the intelligence process and developing TTP to more effectively integrate cyberspace operations. However, these efforts are hindered because units have limited access to certain types of information and do not have the knowledge and ability to immediately process information to support cyberspace operations. Primary reasons for this situation include:

- Lack of specialized Army personnel (e.g., cyber branch [17 series] and military intelligence branch [35 series]) assigned or attached to the unit who can plan, coordinate, synchronize, and integrate cyberspace operations.
- Limited resources (e.g., technical networks and related hardware and software) that enable individual and collective training for cyberspace operations and EW.
- Limited understanding of cyberspace capabilities, missions (e.g., cyberspace intelligence, surveillance, and reconnaissance [ISR] and computer network exploitation), and related policy and authority.

(FOUO) Table 1-5 lists observations gathered during recent training events.

Table 1-5. Sample observations

(FOUO) The unit developed planning products and tools to describe enemy and adversary use of cyberspace. However, this effort was stovepiped and not part of a comprehensive IPB effort.
(FOUO) The staff did not have the knowledge or skills to describe cyberspace and how it linked to the situation template, named area of interest, and high-value target list. As a result, the staff was not able to describe the cyber terrain or develop the collection plan for target nodes in cyberspace.
(FOUO) The staff was unaware of the importance of cyber ISR capabilities. Although cyber ISR capabilities were not organic to the brigade combat team, the staff needed to know how to coordinate and integrate them throughout the intelligence process.
(FOUO) The intelligence staff did not understand how to fuse digital network intelligence with other intelligence multidisciplines, resulting in minimal efforts to insert cyber-derived intelligence with other intelligence disciplines.

Lessons and Tactics, Techniques, and Procedures

(FOUO) Units apply the intelligence process to the cyberspace domain using existing doctrine such as JP 2-01.3; FM 2-0, *Intelligence Operations*, 15 APR 2014; and ATP 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*, 10 NOV 2014. Although many of the techniques for planning and conducting cyberspace operations are contained in classified documents, many existing TTP can and should be used.

(FOUO) Similar to the other domains, cyberspace can be analyzed and described using standard planning frameworks and tools. For example, Army corps staffs performing in a joint task force headquarters role use the political, military, economic, social, information, and infrastructure systems framework to determine nodes and links of adversaries operating in cyberspace. See JP 2-01.3 for additional information on the systems perspective. Army division and brigade staffs commonly apply the mission variables of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations, as well as areas, structures, capabilities, organizations, people, and events tools to identify aspects of cyberspace having relevance to the concept of operations.

(FOUO) The G-2/S-2 leads the staff through the IPB process, which includes cyberspace as one of many characteristics of the operational environment. Figure 1-4 is based on Figure 2-1 from ATP 2-01.3; it aligns IPB outputs to products that are used to describe and later operate in cyberspace. The cyberspace products listed in Figure 1-4 are not all inclusive.

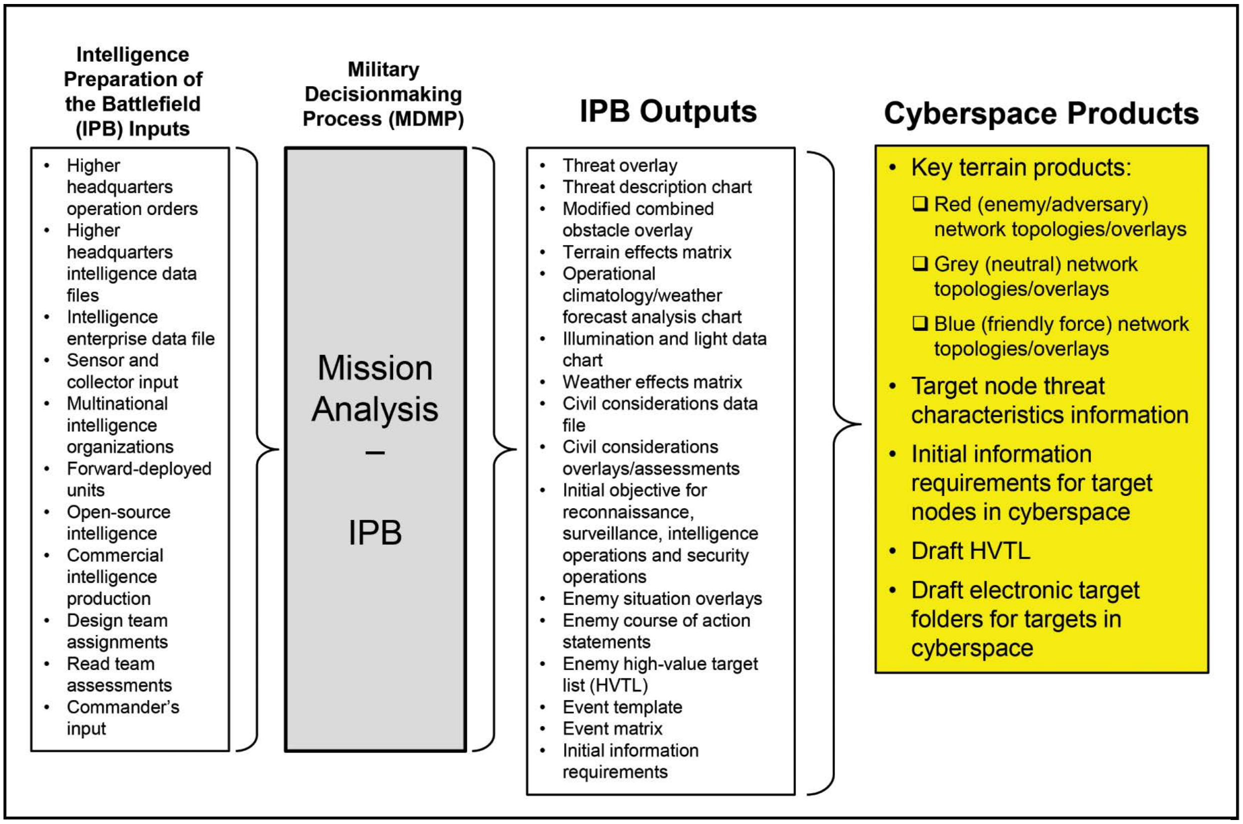

Intelligence Preparation of the Battlefield (IPB) Inputs
• Higher headquarters operation orders
• Higher headquarters intelligence data files
• Intelligence enterprise data file
• Sensor and collector input
• Multinational intelligence organizations
• Forward-deployed units
• Open-source intelligence
• Commercial intelligence production
• Design team assignments
• Read team assessments
• Commander's input
Military Decisionmaking Process (MDMP)
Mission Analysis – IPB
IPB Outputs
• Threat overlay
• Threat description chart
• Modified combined obstacle overlay
• Terrain effects matrix
• Operational climatology/weather forecast analysis chart
• Illumination and light data chart
• Weather effects matrix
• Civil considerations data file
• Civil considerations overlays/assessments
• Initial objective for reconnaissance, surveillance, intelligence operations and security operations
• Enemy situation overlays
• Enemy course of action statements
• Enemy high-value target list (HVTL)
• Event template
• Event matrix
• Initial information requirements
Cyberspace Products
• Key terrain products:
❑ Red (enemy/adversary) network topologies/overlays
❑ Grey (neutral) network topologies/overlays
❑ Blue (friendly force) network topologies/overlays
• Target node threat characteristics information
• Initial information requirements for target nodes in cyberspace
• Draft HVTL
• Draft electronic target folders for targets in cyberspace

Figure 1-4. IPB outputs and cyberspace products

(FOUO) The challenges associated with applying the intelligence process to cyberspace and developing intelligence products to support cyberspace operations can be partially addressed through improved implementation of current doctrine (e.g., JP 2-01.3, FM 2-0, and ATP 2-01.3). The TTP in Table 1-6 address some of these existing challenges.

Table 1-6. Recommended TTP

(FOUO) As a part of the IPB, units should identify intelligence gaps in cyberspace. These gaps should be translated into information requirements and priority intelligence requirements. It is not necessary to conduct a separate IPB process or develop separate products to account for cyberspace. The G-2/S-2 can expect the intelligence estimate and other planning outputs to expand considerably to account for friendly, enemy, adversary, and neutral actors' (e.g., host-nation populations) use of cyberspace.

(FOUO) The G-2/S-2 should ensure joint cyberspace ISR are integrated into the collection step of the Army intelligence process. Cyber-enabled ISR should be detailed in intelligence and operations synchronization matrices and supporting decision tools. The G-2/S-2 should maintain SharePoint sites on the SECRET Internet Protocol Router Network and the Joint Worldwide Intelligence Communications System to enable CEMA coordination and synchronization.

(FOUO) The intelligence staff should fuse digital network intelligence through coordination and augmentation when required. This effort will enable units to create desired effects while supporting the overall intelligence fusion effort.

Other Emerging Categories

(FOUO) In addition to the three major categories discussed, the following four emerging categories are under current observation:

- Integrating effects created in cyberspace with the scheme of maneuver
- Unit integration of external enablers to support cyberspace operations
- Developing cyber battle drills and standard operating procedures
- Developing products to depict key terrain in cyberspace

As doctrine evolves and personnel are trained and educated in cyberspace operations, TTP will continue to be developed, codified, and disseminated in order to assist commanders and staffs to leverage cyberspace in support of unified land operations.

Chapter 2

Cybersecurity Observations at the National Training Center

MAJ Heather Fisk and CW3 Robert Sullivan
Bronco Team, Operations Group, National Training Center

(FOUO) Cybersecurity observations define the challenges from numerous rotational units (RTUs) at the National Training Center (NTC). The NTC Operations Group collected observations and tactics, techniques, and procedures (TTP) and recommended approaches to improve the unit's cybersecurity posture.

Cybersecurity at the National Training Center

(FOUO) According to Joint Publication (JP) 6-0, *Joint Communications System*, 10 JUN 2015, cybersecurity is one of several proactive actions that contribute to Department of Defense information network (DODIN) operations. Cybersecurity involves achieving and maintaining an effective cybersecurity posture that requires the employment of secure configuration; comprehensive security training for DODIN users; and monitoring, detecting, and restoring capabilities to shield and preserve information and information systems.

(FOUO) Currently, RTUs struggle to effectively secure and defend their technical networks (i.e., LandWarNet). They often are unable to enforce standard operating procedures and other network defense measures that align with DODIN operations and defensive cyberspace operations mission sets as described in JP 3-12, *Cyberspace Operations*, 05 FEB 2013; Field Manual (FM) 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014; and FM 6-02, *Signal Support to Operations*, 22 JAN 2014. Signal observer coach/trainers consistently observe RTUs arriving with undeveloped security postures. However, these postures do improve throughout the rotation, allowing RTUs to gain a more comprehensive understanding of cybersecurity and best practices to mitigate cyber threats.

Observations

(FOUO) **Phishing attacks**. Phishing emails were used by the cyber opposing force (OPFOR) to penetrate and exploit the RTU's network. Phishing emails were sent from the cyber OPFOR to users in the RTU. These emails contained a uniform resource locator (known as URL) intended to deceive the user. The cyber OPFOR attempted to influence users to access malicious websites. If successful, the cyber OPFOR acquired sensitive information from users, while infecting their systems with malicious software. Once the cyber OPFOR had a user's credentials, it was able to gain access to other systems such as SharePoint, file share, and domain controllers.

(FOUO) **Network hardening**. Units were inconsistent in their implementation of Security Technical Implementation Guides (STIGs), information assurance vulnerability alerts (IAVAs), updates, and patches. RTUs often arrive at the NTC without implementing appropriate network safeguards. For example, quarterly updates for Army Battle Command Systems (ABCS) often are not applied until the information assurance validation exercise, after the rotation has already begun. Due to time constraints, systems were not effectively patched or updated prior to the rotation, resulting in network vulnerabilities. Also, training shortfalls were identified in configuring router access control lists and firewall rules. As a result, the cyber OPFOR was able to gain access to the RTU network, therefore disrupting the RTU mission command system.

(FOUO) **Password management**. The use of weak system administrators and user passwords on client systems and ABCS is a vulnerability that can be exploited by the cyber OPFOR to gain access to the RTU network. Poor password management enables the cyber OPFOR to capture additional domain administrator and user credentials. The cyber OPFOR can gain access to user information if the default passwords are not changed on printers. Having only default passwords or no passwords on the Tactical Operations Intercommunications System (TOCNET) allows the cyber OPFOR to extract configuration files from the Soft Crew Access Unit. These files contain password pin codes that give the cyber OPFOR the ability to monitor communications across the Enhanced Micro Central Switching Unit (EMCSU).

(FOUO) **Triad model of information assurance**. There is currently an imbalance across RTU efforts to ensure data confidentiality, integrity, and availability. Confidentiality is assurance of data privacy. Integrity is assurance of non-altered data. Availability is assurance in the timely and reliable access to data services for authorized users. Units tend to weigh one pillar of the triad model instead of trying to develop an effective balance between confidentiality, integrity, and availability.

(FOUO) Recommended Tactics, Techniques, and Procedures to Reverse Negative Cybersecurity Observations

- Implement STIGs, IAVAs, software updates, and software patches across the entire network.

- Change all systems (client and ABCS) default passwords to unique, complex passwords.

- Educate users about current cyber threats and cyber incident reporting procedures.

- Only use elevated privileges to conduct administrative work, then log out of the system. Do not remain logged in as an administrator.

- Configure TOCNET EMCSU with a complex password.

- Turnoff unnecessary services (Web, Secure Shell, Telnet, File Transfer Protocol, etc.) in the TOCNET EMCSU menu.

- Enforce the policy of no emails with links or attachments without a digital signature.

- Implement Exchange Server rules to stop emails with certain words or a combination of letters (e.g., HTTP, HTML, WWW, .COM, or //) from leaving the server. Have the emails forwarded to an administrator account for evaluation instead. This rule allows the administrator to determine if a phishing email attempt was made. This rule applies to both the body of the email and attachments.

- Implement the use of the Lightweight Directory Access Protocol (LDAP) query on its Active Directory, which allows the server technician to see if new users have been created since a set time within the LDAP query.

- Timely mitigate identified threats. Determine the cause of the cyber incident and enforce the unit’s cyber incident battle drill. Take appropriate action to block future emails from the identified source.

- Use the Exchange Management Shell to block specific Internet Protocol addresses.

- Use Exchange Troubleshooting Assistant to identify users who have received a specific email.

Chapter 3

Doctrine for Cyberspace Operations

Victor Delacruz
United States Army Cyber Center of Excellence

(FOUO) In August 2011, Joint Publication (JP) 3-0, *Joint Operations*, 11 AUG 2011, introduced cyberspace operations into doctrine. In May 2012, Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations*, 16 MAY 2012, was published introducing cyberspace operations as an activity of cyber electromagnetic activities (CEMA). These two doctrine publications established conditions upon which other doctrinal sources were developed to address the new operational domain of cyberspace. This chapter outlines 15 key current and emerging doctrine publications that specifically address cyberspace operations (see Figure 3-1); key terms and concepts; and recommended tactics, techniques, and procedures (TTP).

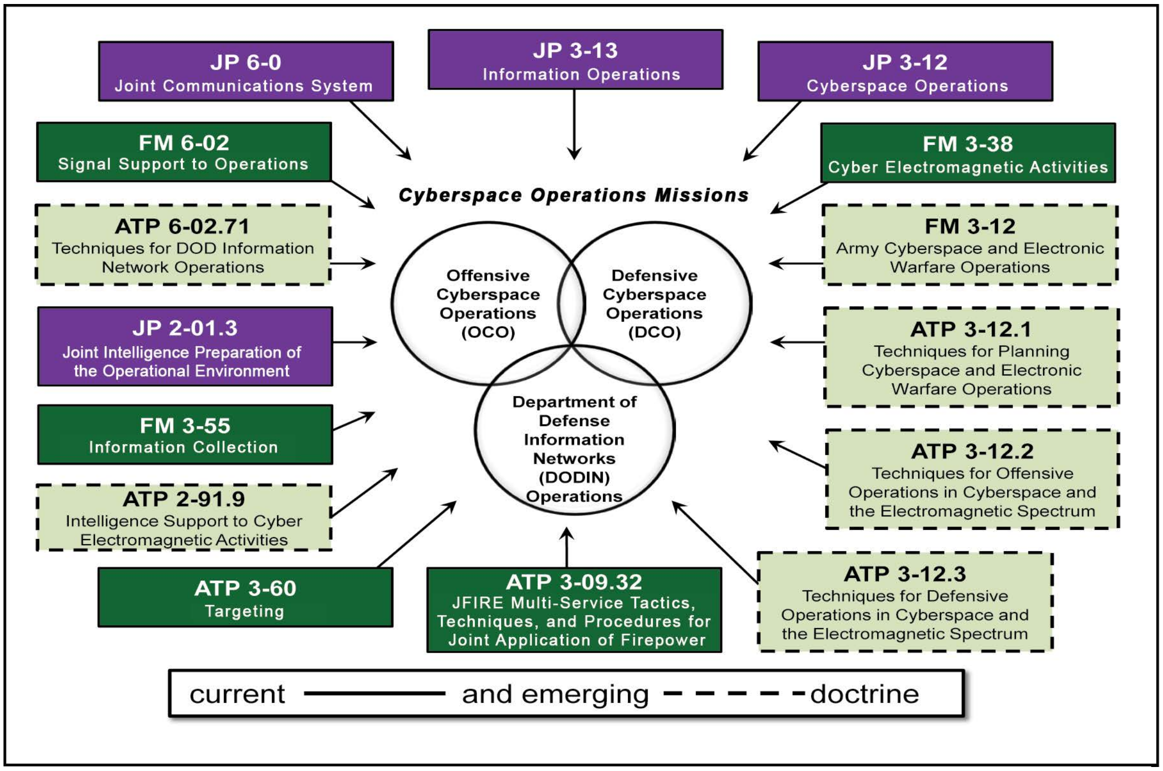

JP 6-0
Joint Communications System
JP 3-13
Information Operations
JP 3-12
Cyberspace Operations
FM 6-02
Signal Support to Operations
FM 3-38
Cyber Electromagnetic Activities
Cyberspace Operations Missions
ATP 6-02.71
Techniques for DOD Information Network Operations
FM 3-12
Army Cyberspace and Electronic Warfare Operations
Offensive Cyberspace Operations (OCO)
Defensive Cyberspace Operations (DCO)
JP 2-01.3
Joint Intelligence Preparation of the Operational Environment
ATP 3-12.1
Techniques for Planning Cyberspace and Electronic Warfare Operations
Department of Defense Information Networks (DODIN) Operations
FM 3-55
Information Collection
ATP 3-12.2
Techniques for Offensive Operations in Cyberspace and the Electromagnetic Spectrum
ATP 2-91.9
Intelligence Support to Cyber Electromagnetic Activities
ATP 3-60
Targeting
ATP 3-09.32
JFIRE Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower
ATP 3-12.3
Techniques for Defensive Operations in Cyberspace and the Electromagnetic Spectrum
current and emerging doctrine

Figure 3-1. Current and emerging doctrine for cyberspace operations

(FOUO) As commanders and staffs strive to integrate and leverage cyberspace operations, they refer to both joint and Army doctrine publications. Figure 3-1 shows only a portion of several key doctrine publications that specifically address cyberspace operations. This collection of publications is not all inclusive. Rather, it represents doctrinal sources that facilitate a greater understanding of cyberspace operations in the context of joint and Army operations.

Synopsis of Current and Emerging Doctrine

(FOUO) **JP 3-12, *Cyberspace Operations*, 05 FEB 2013**. Cyberspace operations have traditionally involved the employment of cyberspace capabilities at echelons above the corps level. JP 3-12 discusses how cyberspace capabilities are coordinated and employed down to the joint task force and corps levels. Topics such as cyberspace actions, targeting, and authorities are discussed allowing Army commanders and staffs to appreciate the unique nature of cyberspace operations from a joint perspective. The roles of the cyberspace support element and Joint Cyberspace Center are also discussed. Table 3-1 lists recommended TTP from JP 3-12.

Table 3-1. JP 3-12 recommended TTP

(FOUO) Ensure JP 3-12 is read and understood by staff members, especially from the mission command (assistant chief of staff, signal [G-6]/signal staff officer [S-6], electronic warfare [EW] officer/CEMA element), intelligence (assistant chief of staff, intelligence [G-2]/intelligence staff officer [S-2]), movement and maneuver (assistant chief of staff, operations [G-3]/operations staff officer [S-3], information operations [IO] officer/IO element) and fires warfighting functions. The space officer/space support element personnel should also review this publication. Staff members need to be aware of similarities and differences between this JP and Army doctrine publications that currently address CEMA and cyberspace operations.
(FOUO) Army CEMA staff principals at corps level and above (G-2, G-3, G-6, EW officer/CEMA element, IO officer/element, chief of fires/fires cell, space officer/space support element) should be knowledgeable of the extensive joint taxonomy for cyberspace operations, which is detailed throughout the publication. This knowledge will enable clear communication between Army and joint cyberspace organizations.

(FOUO) **Field Manual (FM) 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014**. This FM is the Army's first effort to describe tactics and procedures regarding the conduct of CEMA as established in ADRP 6-0, *Mission Command*, 17 MAY 2012. Cyberspace operations are described as functions and missions to include offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense information network (DODIN) operations. Additionally, EW and spectrum management operations are discussed in this FM. The CEMA working group is also discussed at length. Planning tables of the military decisionmaking process (MDMP) are provided to guide the staff in coordinating and synchronizing cyberspace operations, EW, and spectrum management operations. Table 3-2 lists recommended TTP for FM 3-38. (**Note**: FM 3-38 will be superseded by FM 3-12, *Army Cyberspace and Electronic Warfare Operations*, when published, and will reflect updated tactics and procedures for cyberspace operations and EW.)

Table 3-2. FM 3-38 recommended TTP

(FOUO) Commanders and staffs should consider the implications of cyberspace operations employed primarily inside the DODIN (e.g., DCO internal defense measures) and outside the DODIN (e.g., OCO and DCO response actions). For example, some tasks and types of DCO involve the employment of unique capabilities that secure and defend the DODIN that, in turn, support and enable the mission command system. OCO tasks involve the employment of unique capabilities designed to create effects on enemy and adversary target nodes. Understanding the implications of these actions and effects contributes to the commander's ability to provide clear guidance for cyberspace operations throughout the operations process. In some instances, cyberspace operations and associated capabilities may be combined with EW, signal, IO, space operations, and intelligence to employ primarily nonlethal actions to create desired effects in and through cyberspace.

(FOUO) Ensure the CEMA MDMP tables (see FM 3-38, Chapter 6, *Operations Process*) are incorporated into unit planning standard operating procedures and used during collective training events (e.g., home-station and command-post exercises). These tables, along with FM 6-0, *Command and Staff Organization and Operations*, 05 MAY 2014; and Army Techniques Publication (ATP) 3-36, *Electronic Warfare*, 16 DEC 2014, provide a quick reference to enable key collaboration — horizontal and vertical — and accountability for key planning products in support of cyberspace operations, EW, and spectrum management operations.

(FOUO) Ensure enemy and adversary target nodes and associated devices designated for effects by cyberspace operations capabilities are also considered for effects by EW capabilities and vice versa. This effort will further ensure that effects are complementary and reinforce the scheme of maneuver and overall concept of operations.

(FOUO) **FM 3-12, *Army Cyberspace and Electronic Warfare Operations***. (**Note:** Not yet published.) This FM will provide the Army with tactics and procedures for planning, preparing, conducting, and assessing cyberspace operations and EW with a focus on units at echelons of corps and below. Additionally, this FM will emphasize CEMA coordination and synchronization during the CEMA working group, provide detailed MDMP planning tables, and provide guidance on developing operation order products specific to cyberspace operations and EW. This FM will nest with JP 3-12 and JP 6-0, *Joint Communications System*, 10 JUN 2015. FM 3-12 will supersede FM 3-38 when published.

(FOUO) **ATP 3-12.1-3 series**. (**Note**: Not yet published, program directive in development as of November 2015.) This series of ATPs will nest with the future FM 3-12. Each ATP will provide the Army with techniques on planning, coordinating, synchronizing, integrating, and conducting cyberspace operations, EW, and OCO and DCO in particular. Due to the nature of these techniques, these ATPs will be classified.

(FOUO) **ATP 3-09.32, *JFIRE Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower*, 21 JAN 2016**. Army units request effects in designated cyberspace by preparing and submitting the cyber effects request format (CERF) and/or electronic attack request format (EARF). This ATP provides techniques on how to prepare the CERF and EARF. Table 3-3 lists recommended TTP for ATP 3-09.32.

Table 3-3. ATP 3-09.32 recommended TTP

(FOUO) Staffs should combine the guidance in ATP 3-09.32 with the formats in FM 6-99, *U.S. Army Report and Message Formats*, 19 AUG 2013. Staffs should establish internal procedures for preparing and submitting the following formats:

- CERF, report number C090, FM 6-99, pages A-74 and A-75
- Cyberspace operations mission request status/tasking, report number C095, FM 6-99, page A-76

(FOUO) Ensure supporting products (e.g., target folders and tailored planning products) are developed to accompany CERF and/or EARF submissions. Consider how enemy and adversary target nodes in cyberspace, nominated for effects by cyberspace and EW capabilities, will often involve one or more nodes consisting of one or more devices accessed by one or more users. First-order effects in cyberspace should be designed to create deliberate second-order effects in support of the scheme of maneuver and overall concept of operations.

(FOUO) **ATP 3-60, *Targeting*, 07 MAY 2015**. Cyberspace operations as an activity of CEMA is addressed throughout this publication. Topics such as desired effects; decide, detect, deliver, and assess targeting methodology; and corps-to-battalion targeting are discussed. Techniques are provided to both inform and enable Army commanders and staffs to more effectively integrate cyberspace operations.

(FOUO) **ATP 3-36, *Electronic Warfare Techniques*, 16 DEC 2014**. EW is described as one of three capabilities of CEMA. Each of the divisions of EW are described to include electronic attack, electronic protection, and EW support. Techniques are described for developing specific planning products resulting from the MDMP. Additionally, joint and Army EW capabilities are described in considerable detail. Future updates to this ATP will ensure it nests with FM 3-12; FM 6-02, *Signal Support to Operations,* 22 JAN 2014; and ATP 6-02.71, *Techniques for Department of Defense Information Network Operations* (not yet published).

(FOUO) **ATP 2-91.9, *Intelligence Support to Cyber Electromagnetic Activities***. (**Note**: Not yet published.) Operating in cyberspace requires a high degree of situational understanding. The intelligence warfighting function is uniquely designed to develop, disseminate, and maintain cyberspace situational understanding. This ATP will provide techniques for intelligence support to CEMA; it will also include a chapter specifically for cyberspace operations. Due to the nature of these techniques, this ATP will be classified.

(FOUO) **FM 3-55, *Information Collection*, 03 MAY 2013**. Operating in cyberspace requires considerable information and intelligence collection efforts. These efforts enable the staff to answer the commander's critical information requirements, which contribute to effective decision making and mission accomplishment. Topics such as commander's guidance; information collection planning; and joint intelligence, surveillance, and reconnaissance are discussed.

(FOUO) **JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, 21 MAY 2014**. Planning for cyberspace operations requires an intensive intelligence effort to enable cyberspace situational understanding. This JP describes the four-step joint intelligence preparation of the operational environment process while emphasizing a systems perspective. Topics such as systems network analysis and systems nodes and links are discussed to ensure Army commanders and staffs are more aware of joint intelligence methods and related products (e.g., modified combined obstacle overlays) that explain the Army intelligence process.

(FOUO) **ATP 6-02.71, *Techniques for Department of Defense Information Network Operations***. (**Note**: Not yet published.) The defense of the Army's portion of the DODIN (i.e., LandWarNet) remains a top priority for commanders. This ATP will provide techniques to address this priority. Topics such as the joint information environment, cybersecurity, and DODIN operations roles and responsibilities will be discussed in detail. This ATP will nest with recent doctrinal changes in JP 6-0.

(FOUO) **FM 6-02, *Signal Support to Operations*, 22 JAN 2014**. The Signal Corps has traditionally performed numerous tasks to enable communications in support of Army operations. With the integration of cyberspace operations into Army doctrine, this FM aligns with FM 3-38 and further explains tactics related to DODIN operations. Topics such as network operations, signal support to CEMA, and cyber threats are discussed. Future updates to this FM will ensure it nests with JP 6-0 and FM 3-12. Table 3-4 lists recommended TTP for FM 6-02.

Table 3-4. FM 6-02 recommended TTP

(FOUO) Commanders and staffs should be aware of the signal enabling commands and personnel described throughout FM 6-02, Chapter 2, *Roles and Responsibilities of Signal Organizations*. These organizations and personnel provide unique capabilities in support of cyberspace operations, particularly those inside the Army's portion of the DODIN (i.e., LandWarNet). (FOUO) Staffs should review the cyber threats in FM 6-02, Chapter 3, *LandWarNet*, and ensure full compliance with the communications security procedures in Appendix B, *Communications Security Procedures*.

(FOUO) **JP 6-0, *Joint Communications System*, 10 JUN 2015**. It is essential to understand DODIN operations that were initially introduced in JP 3-12. JP 6-0 explains DODIN operations, describes key command and support relationships, and discusses cybersecurity (replaces the term "information assurance"). Other discussion topics include the joint information environment, the role of the Joint Cyberspace Center, and the Joint Force Headquarters-Department of Defense Information Network. This JP aligns with JP 3-12. The future version of FM 6-02 will nest with JP 6-0.

(FOUO) **JP 3-13, *Information Operations*, 27 NOV 2012**. It is essential to understand the relationship between cyberspace and the information environment. This JP explains the dimensions of the information environment — physical, informational, and cognitive — and how cyberspace capabilities may be employed in support of information operations. The future FM 3-13, *Information Operations*, will nest with this JP. Table 3-5 lists recommended TTP for JP 3-13.

Table 3-5. JP 3-13 recommended TTP

(FOUO) Ensure all information-related capabilities, including cyberspace operations and EW, are considered throughout the operations process to create desired effects in support of unified land operations, especially the concept of operations and scheme of maneuver. Staff members should leverage joint and Army IO products, such as the combined information overlay, to achieve greater situational understanding of cyberspace leading to enhanced planning, preparation, and execution. (FOUO) Ensure enemy and adversary target nodes designated for effects by cyberspace operations capabilities are also considered for effects by other information-related capabilities and vice versa. This effort will ensure effects are complementary and reinforce the scheme of maneuver and overall concept of operations.

Conclusion

(FOUO) The current and emerging doctrine outlined in this chapter are key to understanding and integrating cyberspace operations throughout the operations process. Also, the TTP provided in the tables reflect best practices to date and will be updated as observations and lessons are gathered and processed. Commanders and staffs should continue to seek out and incorporate doctrine on cyberspace operations, which will likely be in a constant state of change.

Key Doctrinal Terms for Cyberspace Operations

(U) The terms listed are addressed in JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 08 NOV 2010; and ADRP 1-02, *Terms and Military Symbols*, 07 DEC 2015. It is essential for commanders and staffs to know these terms. The list is not all inclusive.

cyber electromagnetic activities — Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same, and protecting the mission command system. (ADRP 3-0)

cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

cyberspace operations — The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

defensive cyberspace operation response action — Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. (JP 3-12)

defensive cyberspace operations — Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 3-12)

Department of Defense information network — The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policymakers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (JP 6-0)

Department of Defense information network operations — Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information network. (JP 3-12)

intelligence, surveillance, and reconnaissance — An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. (JP 2-01)

LandWarNet — The Army's portion of the Department of Defense information network. A technical network that encompasses all Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide. (FM 6-02)

named area of interest — The geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected, usually to capture indications of adversary courses of action. (JP 2-01.3)

node — In communications and computer systems, the physical location that provides terminating, switching, and gateway access services to support information exchange. (JP 6-0) An element of a system that represents a person, place, or physical thing. (JP 3-0)

offensive cyberspace operations — Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 3-12)

Chapter 4

Commander’s Integration of Cyberspace Operations

LTG L.D. Holder (Retired) and Victor Delacruz
United States Army Cyber Center of Excellence

(FOUO) Today’s combat conditions place a premium on understanding and acting in cyberspace. Corps-, division-, and brigade-level commanders can gain important tactical advantages through mastery of operations in the cyberspace domain if they understand its nature and potential. Conversely, these commanders can subject themselves to considerable risks if they do not. As with every other area of combat power, commanders play a critical role guiding their subordinate leaders in integrating effects into their overall operations. This role extends into operations in and through cyberspace.

(FOUO) Commanders supported by their staffs must consider cyberspace throughout the operations process as they understand, visualize, describe, direct, lead, and assess operations. Cyberspace operations are described as missions in cyberspace and they include offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense information network (DODIN) operations. Figure 4-1 depicts cyberspace operations and the divisions of electronic warfare (EW).

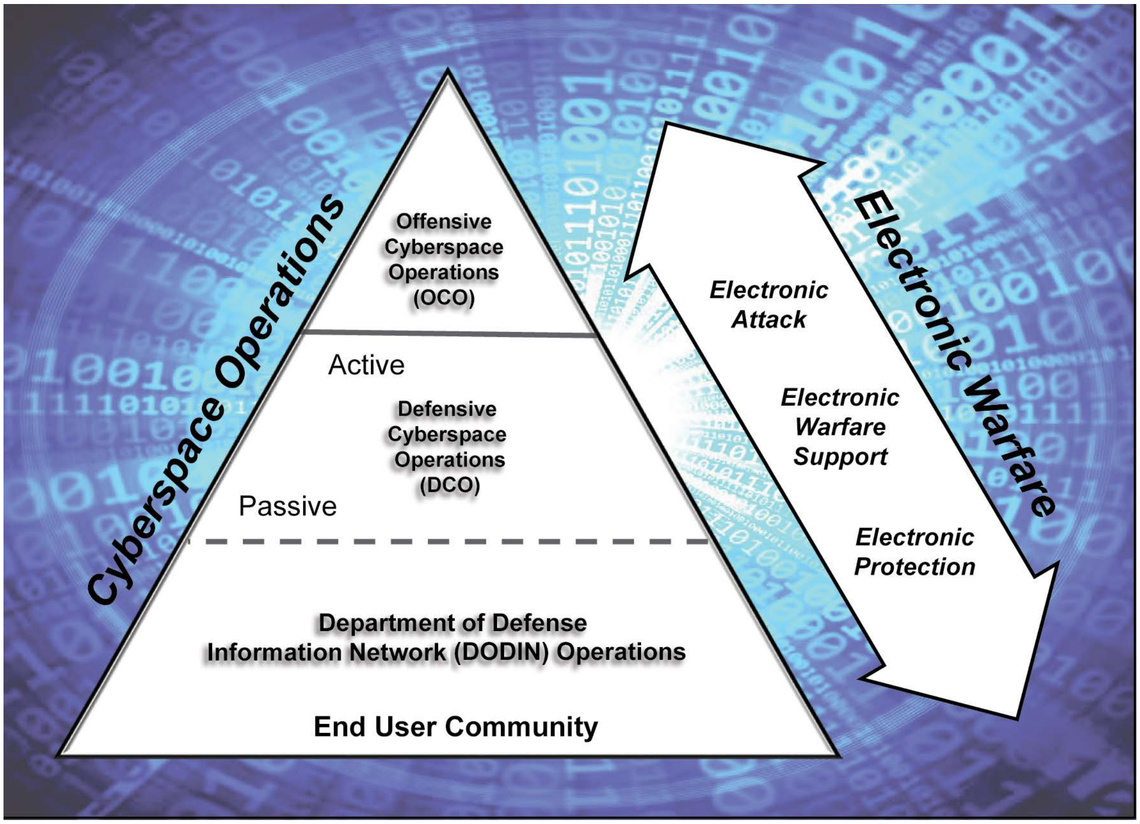

Cyberspace Operations
Offensive Cyberspace Operations (OCO)
Active
Defensive Cyberspace Operations (DCO)
Passive
Department of Defense Information Network (DODIN) Operations
End User Community
Electronic Warfare
Electronic Attack
Electronic Warfare Support
Electronic Protection

Figure 4-1. Cyberspace operations and EW

(FOUO) Depending on the situation, cyberspace operations and associated capabilities may be combined with EW, signal, information operations (IO), space operations, and intelligence to employ primarily nonlethal actions and create desired effects in and through cyberspace. The lessons to date in combat and at training events reflect the difficulty of integrating cyberspace operations in support of the scheme of maneuver and the overarching concept of operations. Commanders and staffs struggle to integrate cyberspace missions and supporting tasks with the elements of combined arms operations for several reasons. To varying degrees, commanders lack personnel; equipment; and tactics, techniques, and procedures (TTP) (e.g., the ability to access intelligence to support cyberspace operations). This lack of resources and supporting doctrine, combined with little experience, particularly with OCO at echelons of corps and below, make it more difficult to integrate cyberspace operations into training and combat operations.

(FOUO) Commanders' roles in integrating cyberspace operations are defined by actions they are uniquely responsible for as they drive the operations process. These actions (i.e., understand, visualize, describe, direct, lead, and assess) are well codified in Army doctrine. However, commanders must now account for cyberspace domain and operations.

Commander's Role

(FOUO) Based on observations, insights, and emerging lessons, commanders can integrate cyberspace operations more effectively by addressing the following four focus areas:

- Provide a clear commander's intent and accompanying guidance for cyberspace operations to inform staff and subordinate actions throughout the operations process.

- Ensure active collaboration across the staff, subordinate units, higher headquarters, and unified action partners to enable shared understanding of cyberspace and the opportunities and risks cyberspace operations present for military operations.

- Approve high-priority target lists, target nominations, collection priorities, and risk mitigation measures that reflect the commander's visualization, description, and direction specific to cyberspace operations.

- Create massed effects by synchronizing cyberspace operations with lethal and nonlethal actions (e.g., fires and IO) in support of the concept of operations. Anticipate and account for related second- and third-order effects.

Provide a Clear Commander's Intent

(FOUO) Commanders guide their subordinates throughout the operations process by issuing a commanders intent and articulating a concept of operations. These two key contributions, along with continual guidance to the staff, are essential for effective mission command across all domains (i.e., land, air, maritime, space, and cyberspace) and the electromagnetic spectrum.

(FOUO) The current lack of trained cyberspace operations planners and the absence of equipment specifically designed to provide situational awareness and situational understanding of cyberspace limit the commander's ability to understand and visualize cyberspace. This limitation further impacts the commander's ability to effectively describe and direct cyberspace operations. Despite these challenges, commanders apply their experience and judgment, along with their knowledge of doctrine, to ensure cyberspace operations are integrated into their intent and concept of operations.

(FOUO) The commander's intent and concept of operations should be broad enough to guide the employment of all elements of combat power, including cyberspace capabilities in conjunction with EW, information operations, and space capabilities. Although the technical aspects (science) of cyberspace operations are often emphasized during planning, the operational aspects (art), to include the commander's intent and concept of operations, cannot be overlooked. As commanders provide guidance, they benefit from directing such guidance toward actions or effects that should occur primarily inside (internal) and outside (external) of the Army's portion of the DODIN (see Figure 4-2). Table 4-1 on page 28 lists recommended TTP for commander's guidance and the Army's portion of the DODIN.

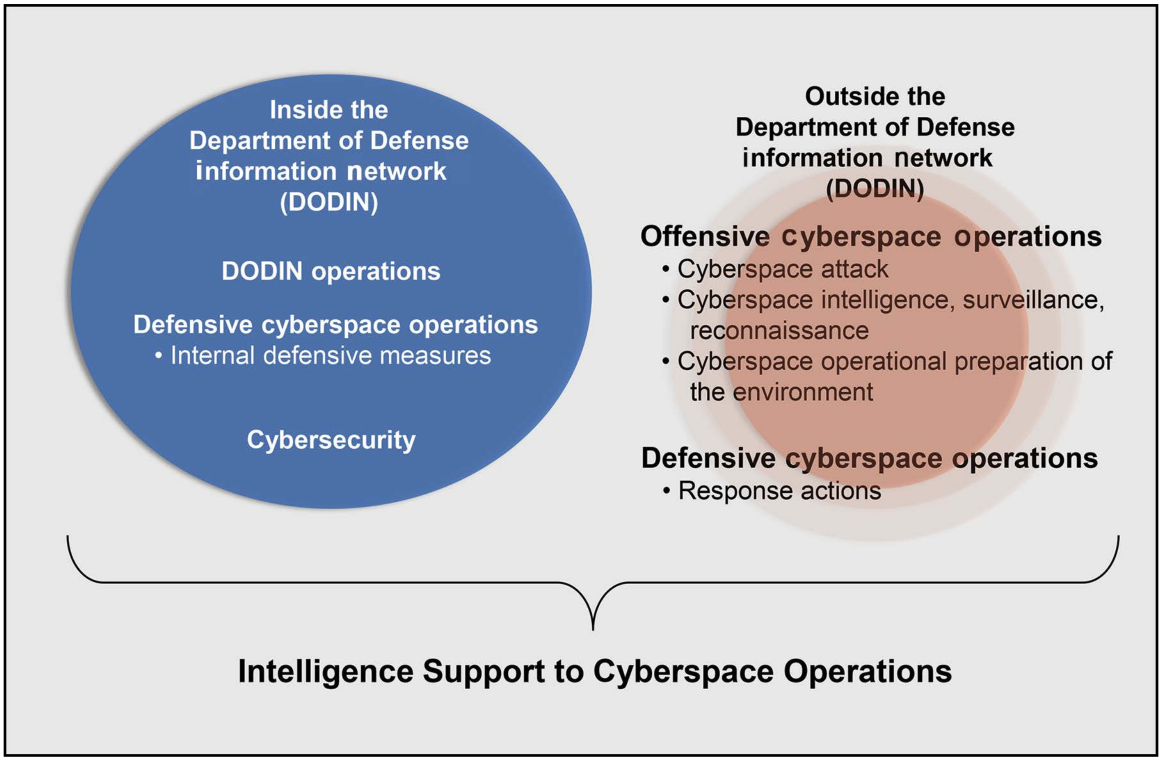

Inside the Department of Defense information network (DODIN)
DODIN operations
Defensive cyberspace operations
• Internal defensive measures
Cybersecurity
Outside the Department of Defense information network (DODIN)
Offensive cyberspace operations
• Cyberspace attack
• Cyberspace intelligence, surveillance, reconnaissance
• Cyberspace operational preparation of the environment
Defensive cyberspace operations
• Response actions
Intelligence Support to Cyberspace Operations

Figure 4-2. Cyberspace operations inside and outside the DODIN

Table 4-1. Recommended TTP for commander's guidance and the Army's portion of the DODIN

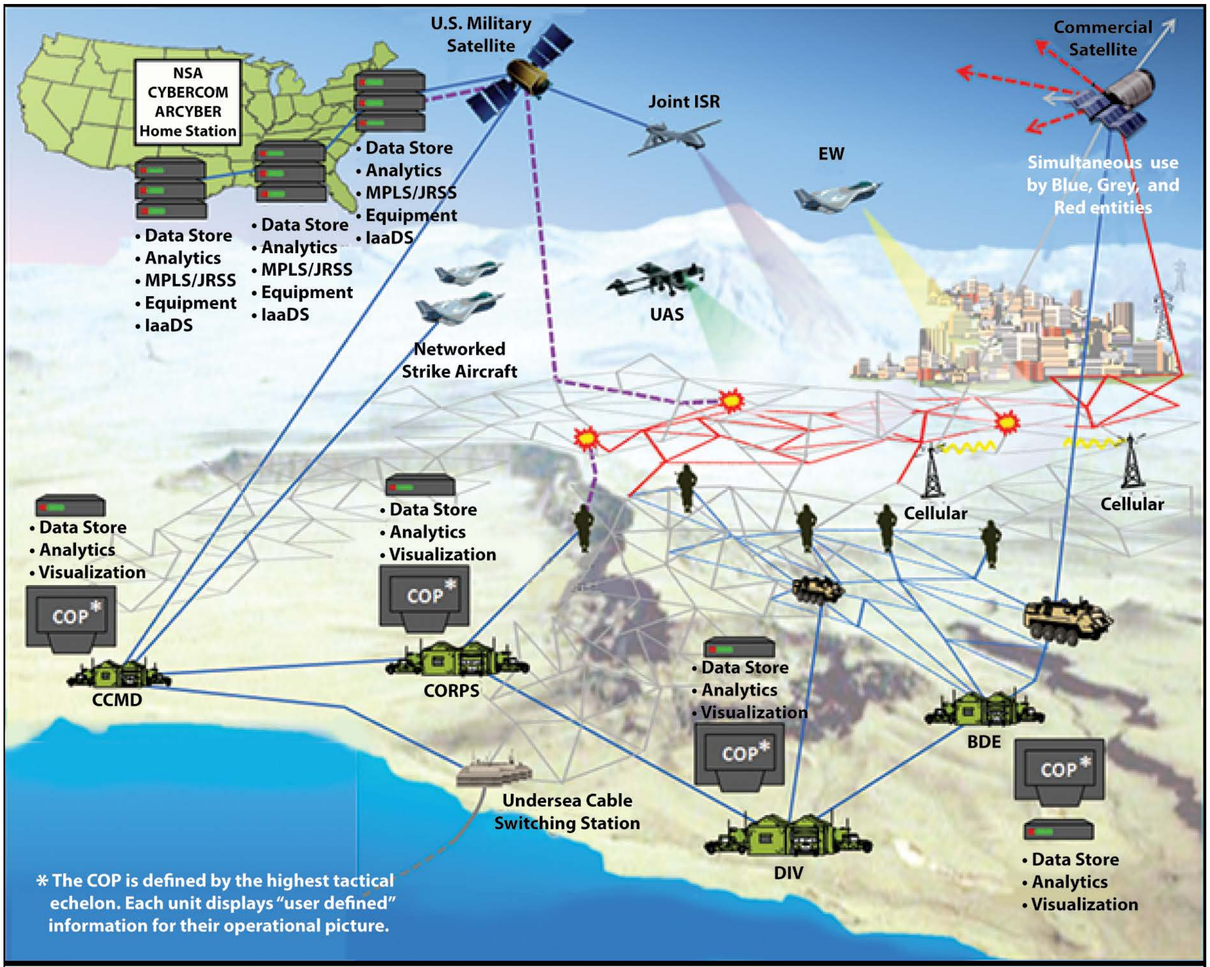
(FOUO) The commander should provide guidance to the staff throughout the operations process to inform cyberspace operations occurring or projected to occur inside and outside of the Army's portion of the DODIN, as shown in Figure 4-2.

(FOUO) For operations inside the DODIN, commanders should engage the assistant chief of staff, signal (G-6)/signal staff officer (S-6) to identify key terrain in cyberspace. The G-6/S-6 will ensure the defense of network nodes within this key terrain enables mission command system effectiveness. For operations outside the DODIN, commanders should engage cyber electromagnetic activities (CEMA) staff principals (i.e., assistant chief of staff, intelligence [G-2]/intelligence staff officer [S-2], assistant chief of staff, operations [G-3]/operations staff officer [S-3], G-6/S-6, EW officer/CEMA element, IO officer/element, chief of fires/fires cell, and space officer/space support element) to ensure first-order effects created in cyberspace result in second-order effects in support of the commander's intent and overarching concept of operations.

Enable Shared Understanding of Cyberspace

(FOUO) Command situational understanding and staff integration are critical for the effective synchronization of cyberspace operations both inside and outside the DODIN. Guided by the commander's intent and concept of operations, the staff collaborates internally, and among echelons, adjacent units, and other actors (e.g., unified action partners) to achieve shared understanding of cyberspace operations.

(FOUO) Shared understanding requires commanders and staffs to engage in continual collaboration as they employ forces in a congested and contested operational environment. Commanders and staffs collaborate to ensure their portion of the DODIN is secure and defended, while gaining and maintaining situational understanding of enemy and adversary cyberspace activities. Developing shared understanding is key, because it contributes to situational understanding and is imperative to achieving cyberspace situational understanding. Figure 4-3 on page 29 depicts various aspects within the operational environment that contribute to cyberspace situational understanding as described in Joint Publication (JP) 3-12, *Cyberspace Operations*, 05 FEB 2013. Table 4-2 on page 30 lists recommended TTP for enabling shared understanding of cyberspace.



LEGEND

——	DODIN	COP	common operational picture
——	Enemy network	CYBERCOM	United States Cyber Command
——	Neutral network	DIV	division
- - - -	Offensive cyberspace operations	EW	electronic warfare
- - - -	Enemy cyber attack	IaaDS	Installation as a docking station
ARCYBER	United States Army Cyber Command	JRSS	joint regional security stacks
BDE	brigade	ISR	intelligence, surveillance, and reconnaissance
CCMD	combatant command	NSA	National Security Agency
		UAS	unmanned aircraft system

Figure 4-3. Aspects of cyberspace situational awareness

Table 4-2. Recommended TTP for enabling shared understanding of cyberspace

(FOUO) The commander should ensure that battle-rhythm events incorporate updates on cyberspace operations and EW to promote situational understanding and achieve unity of effort through collaboration. These battle-rhythm events include not only planning events (e.g., Army design methodology sessions and the military decisionmaking process [MDMP]), but also briefings (e.g., updates and assessments), meetings (e.g., operations synchronization), and working groups (e.g., targeting, CEMA, and IO).

(FOUO) The commander should provide guidance to the staff, specifically the G-2/S-2, IO officer/element, and EW officer/CEMA element, as they co-develop enemy, adversary, and neutral network infrastructure diagrams (e.g., network topologies and overlays) as a part of the joint intelligence preparation of the operational environment/intelligence preparation of the battlefield. These diagrams, topologies, and overlays will contribute to the development of the common operational picture.

(FOUO) Commanders must understand that integration of cyberspace operations requires both horizontal and vertical staff coordination and synchronization. Given the joint nature of cyberspace operations, coordination with higher headquarters within warfighting functions is essential. The commander ensures and, when needed, facilitates collaboration and dialog between the staff and higher headquarters to ensure cyberspace operations are effectively nested and integrated. For example, the EW officer/CEMA element at corps level should maintain direct dialog with the Joint Cyberspace Center and Joint Force Headquarters-Cyber, as required, to track cyber effects request format (CERF) submissions and facilitate direct collaboration.

(FOUO) The complicated nature of planning, preparing, conducting, and assessing cyberspace operations requires concentrated attention from staffs until Army units acquire more experience in performing these activities. Even experienced staffs will have to continually share and integrate information to gain and maintain situational understanding of cyberspace and the electromagnetic spectrum. Commanders within a formation will have to consciously keep each other informed and facilitate staff integration of effects in cyberspace as operations progress. Commanders must ensure their battle-rhythm events and supporting mission command systems enable effective integration of cyberspace operations and EW in support of the mission. For example, through the use of information systems, commanders can "see themselves" (friendly force networks) and "see the enemy" (enemy and adversary networks) while continually gathering information to make decisions and take action in and through cyberspace and the electromagnetic spectrum.

(FOUO) Commanders and staffs establish and maintain a primary focus on defending the Army's portion of the DODIN. They continually receive and assess information on cyber threat activity and ensure measures are in place to anticipate, mitigate, and respond to any form of network intrusion. Commanders and staffs analyze networks and nodes, identifying opportunities to create first-order effects in cyberspace that can cause second- and third-order effects in other domains. Similarly, commanders and staffs follow fire, maneuver, and intelligence developments to identify opportunities to create effects in cyberspace that allow for exploitation of success within other domains.

Visualize, Describe, and Direct Cyberspace Operations

(FOUO) Commanders integrate cyberspace operations throughout the operations process, not only to account for cyberspace as a discrete aspect of the operational environment, but also to find and mitigate risks. Commanders define cyberspace operations initially in the planning process and the resulting commander's intent, concept of operations, and operation plans or orders to establish the foundation for conducting operations. Commanders are responsible for approving high-priority target lists, target nominations, collection priorities, and risk mitigation measures. Commanders actively modify cyberspace operations based on assessments and, where possible, ensure synergy with EW, space, and information-related capabilities. To support the commanders, staffs implement TTP, such as those described in Table 4-3.

Table 4-3. Recommended TTP for key staff actions

(FOUO) The commander should ensure that CEMA staff principals (i.e., G-2/S-2, G-3/S-3, G-6/S-6, EW officer/CEMA element, IO officer/element, chief of fires/fires cell, and space officer/space support element) integrate and synchronize effects and related actions detailed in the scheme of cyberspace operations. To accomplish this task, the staff develops and implements key planning products to include the consolidated high-payoff target list, target synchronization matrix, and information collection matrix.

(FOUO) The staff, led by the G-6/S-6, continually assesses and designates key terrain in cyberspace across all phases of the operation. The commander's guidance will inform this assessment and guide the G-6/S-6 in preventing or mitigating intrusions into the Army's portion of the DODIN.

(FOUO) The staff, led by the G-2/S-2, implements information collection in support of cyberspace operations and EW in accordance with the commander's guidance. Information is collected through discussions about cyberspace actions (e.g., cyberspace intelligence, surveillance, and reconnaissance [ISR]) and EW divisions (e.g., electronic attack).

(FOUO) The commander should ensure the CEMA staff principals effectively coordinate with higher headquarters on receiving and integrating special capabilities (e.g., elements from the Cyber Mission Force). Additional equipment and facilities should be identified, requested, received, and effectively integrated.

Employ Lethal and Nonlethal Actions to Create Massed Effects

(FOUO) Cyberspace operations are rarely employed in isolation. Commanders and staffs must understand that cyberspace is an integral part of the operational environment; the effects commanders and staffs produce by cyberspace capabilities can and should magnify the overall effectiveness of their units' operations. These effects, produced by cyberspace and other capabilities (e.g., EW, space, and information-related) must be carefully integrated and synchronized. Ideally, commanders' cyberspace operations supplement the massed effects produced at decisive points throughout the operation.

(FOUO) Commanders and staffs ensure that cyberspace operations are coordinated, synchronized, and integrated throughout the operations process. During both course of action development and course of action analysis, all domains are considered by all warfighting functions, simultaneously allowing complete and comprehensive outputs. Planning products are tailored to incorporate cyberspace operations. These operations may be combined with EW and other products depending on mission requirements. Lethal and nonlethal actions are considered and matched to desired effects. Also, during the targeting process, staffs ensure cyberspace capabilities are discussed along with other capabilities in the detect, deliver, and assess functions. Primary and secondary designations of identified capabilities are determined through synchronization efforts and further detailed by phase or in accordance with other timeline methods. Table 4-4 lists TTP for commanders and staffs when producing massed effects.

Table 4-4. Recommended TTP for employing actions to create massed effects

(FOUO) The G-3/S-3 and IO officer/element coordinate to receive support from the IO field support team (IO-FST) to ensure effects in cyberspace are synchronized and deconflicted with other information-related capabilities. The IO-FST is uniquely designed to integrate and synchronize information-related capabilities in support of operations at echelons of corps and above. Additionally, IO-FSTs are capable of integrating military deception, EW, military information support operations, operations security, and other activities that have an impact on the information environment.

(FOUO) While conducting cyberspace operations, commanders coordinate among echelons and adjacent units to ensure cyberspace operations and EW are deconflicted as necessary. The G-3/S-3, assisted by the IO officer/element, coordinate continually with the G-6/S-6, G-2/S-2, and EW officer/CEMA element to ensure cyberspace operations are integrated and synchronized to support the scheme of maneuver, which may involve coordination with adjacent units.

(FOUO) Army forces at echelons of corps and below should develop and submit CERFs processed by the joint task force and elevated to the combatant command. These requests for effects in cyberspace should be validated, prioritized, and submitted to higher headquarters for additional processing and approval. See Army Techniques Publication 3-09.32, *JFIRE, Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower*, 21 JAN 2016; and Field Manual 6-99, *U.S. Army Report and Message Formats*, 19 AUG 2013, for additional information on completing the CERF.

Conclusion

(FOUO) In order to achieve the greatest tactical advantage in combat, commanders must integrate cyberspace operations into their combined arms operations both during planning and execution. This integration is holistic and inclusive of EW, space operations, IO, spectrum management, and signal support to operations. Cyberspace capabilities and other capabilities that create effects in cyberspace are tools for the commander that should not be stovepiped.

(FOUO) Today's shortage of specially trained cyberspace operations planners, lack of equipment to support situational understanding of cyberspace, and gaps in Army doctrine and TTP, to include an inability to access intelligence in support of cyberspace operations, all limit the commander's ability to effectively plan, coordinate, synchronize, integrate, and conduct cyberspace operations. Consideration of cyberspace effects throughout the operations process can offset some of these problems. Commanders can use the four focus areas discussed in this chapter to aid them in this effort. It is important to acknowledge that these four focus areas are not all inclusive.

(FOUO) Current and emerging TTP reflect how effectively commanders work with their staffs and subordinate commanders to ensure cyberspace operations and EW are integrated and synchronized throughout the operations process. These commanders must understand the critical nature of this relatively new operational domain and the unique opportunities and risks it presents. Special training in cyberspace operations can help bridge the gap between current inexperience and true tactical ability. Ultimately, commanders should leverage cyberspace operations and EW in conjunction with other capabilities as key components of combat power that can enable them to seize, retain, and exploit the initiative in support of unified land operations.

Chapter 5

Corps, Division, and Brigade Roles During Cyberspace Operations

Victor Delacruz
United States Army Cyber Center of Excellence

Overview

(FOUO) Army forces operating at corps level and below plan, prepare, conduct, and assess cyberspace operations as a part of cyber electromagnetic activities (CEMA). CEMA is a staff task associated with the mission command warfighting function. The roles; responsibilities; capabilities; and tactics, techniques, and procedures (TTP) specific to cyberspace operations are currently described in Field Manual (FM) 6-0, *Commander and Staff Organization and Operations*, 05 MAY 2014; FM 3-38, *Cyber Electromagnetic Activities*, 12 FEB 2014; and FM 6-02, *Signal Support to Operations*, 22 JAN 2014. Commanders and staffs must be aware of these roles and supporting actions to effectively integrate cyberspace operations throughout the operations process.

(FOUO) The staff members and elements regarded as CEMA principals include the assistant chief of staff, intelligence (G-2)/intelligence staff officer (S-2), assistant chief of staff, operations (G-3)/operations staff officer (S-3), assistant chief of staff, signal (G-6)/signal staff officer (S-6), electronic warfare (EW) officer/CEMA element, information operations (IO) officer/element, chief of fires/fires cell, and space officer/space support element. These CEMA principals are depicted in Figure 5-1 for echelons of corps and below. Although not depicted, the staff judge advocate and brigade operational law team also have key roles in CEMA coordination and synchronization.

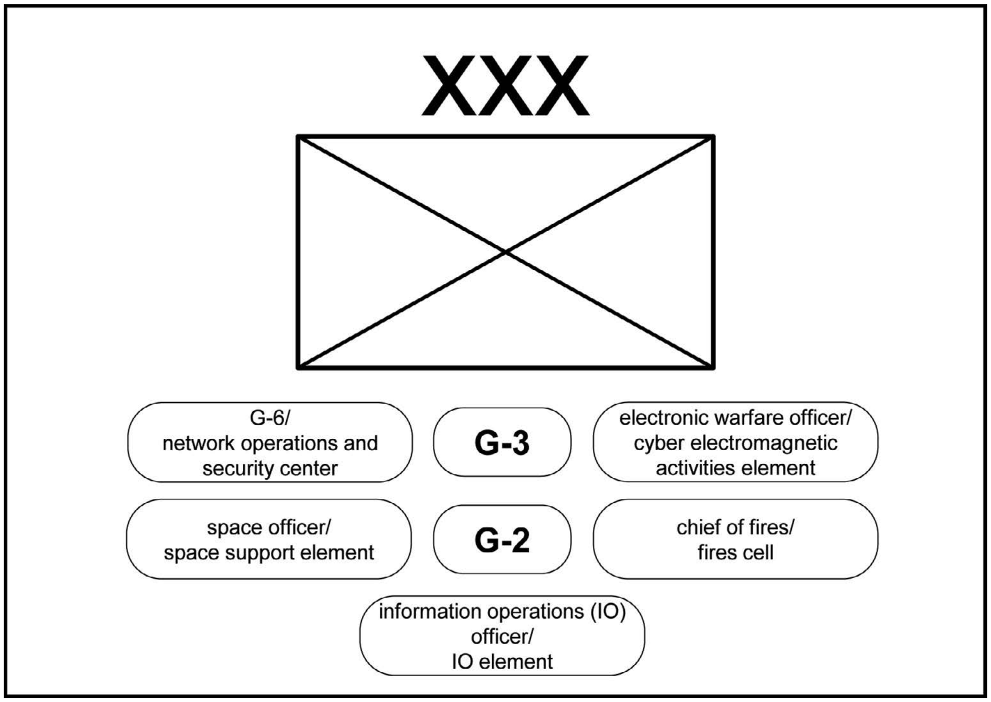

XXX
G-6/ network operations and security center
G-3
electronic warfare officer/ cyber electromagnetic activities element
space officer/ space support element
G-2
chief of fires/ fires cell
information operations (IO) officer/ IO element

Figure 5-1. CEMA principal staff officers and elements

Corps-Level Cyberspace Operations

(U) The corps headquarters may be employed in various roles to include an ARFOR, joint force land component command, joint task force headquarters, or tactical echelon. Regardless of the role, the commander and staff are responsible for coordinating and synchronizing cyberspace operations. FM 3-94, *Theater Army, Corps, and Division Operations*, 21 APR 2014, provides guidance on CEMA and the role of the corps staff.

(FOUO) The corps commander and staff are responsible for certain activities in support of cyberspace operations. These activities can result in actions and/or effects that occur primarily outside the Department of Defense information network (DODIN). Cyberspace operations may be combined with other operations (e.g., EW, IO, and space) and at the corps level. As a result, most of the CEMA staff principals are required to integrate and synchronize these activities as described in Table 5-1.

Table 5-1. Recommended TTP for corps outside the DODIN

(FOUO) The corps commander and staff should be prepared to engage in the following activities that result in actions and/or effects occurring primarily outside the DODIN:

- Plan, coordinate, synchronize, and integrate cyberspace operations missions including offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO) response actions (in conjunction with EW, as appropriate), resulting in the creation of effects primarily outside the DODIN and in support of the corps concept of operations.

- Develop, maintain, and disseminate a common operational picture of designated cyberspace to enable situational understanding of cyberspace and friendly and threat networks.

- Receive, process, and submit cyber effects request formats (CERFs) from subordinate units. Develop and submit CERFs to higher headquarters.

- As required, prepare and submit input for an evaluation request message (EReqM) to higher headquarters.

- Develop, recommend, and brief the corps scheme of cyberspace operations.

- As directed by higher headquarters (i.e., execute order [EXORD] or fragmentary order [FRAGORD]), coordinate and integrate enablers and other expeditionary capabilities in support of corps operations.

(FOUO) The corps commander and staff are also responsible for certain activities in support of cyberspace operations that result in actions and/or effects occurring inside the DODIN as described in Table 5-2. The key staff members involved in these activities include the corps G-2, G-3, G-6 (supported by the corps network operations and security center [NOSC] and corps signal company), and EW officer/CEMA element.

Table 5-2. Recommended TTP for corps inside the DODIN

(FOUO) The following list of activities result in actions and/or effects that occur inside the DODIN. This list is not all inclusive. The corps commander and staff:

- Plan, coordinate, synchronize, integrate, and conduct cyberspace operations missions including DCO and DODIN operations in support of the division concept of operations.

- Oversee and direct the planning, operations, and coordination of all matters concerning corps DODIN operations, network transport, information services, and spectrum management operations for the corps headquarters and assigned units.

- Establish the corps information network and provide operational and technical support to subordinate signal elements.

- Engineer, build, install, configure, secure, operate, maintain, and defend the corps information network and recommend priorities to support the corps commander's priorities.

- Establish and implement procedures for processing relevant information to enable development and dissemination of the corps common operational picture.

- Prepare and submit CERFs to higher headquarters.

- Coordinate, plan, manage, and direct corps cybersecurity activities.

- As directed by higher headquarters, coordinate and integrate enablers and other expeditionary capabilities in support of corps DCO and DODIN operations.

Division-Level Cyberspace Operations

(FOUO) The division is the Army's primary tactical warfighting headquarters, with a primary role as a tactical headquarters, commanding brigades in decisive action. The division commander integrates and synchronizes CEMA to seize, retain, and exploit an advantage over enemies and adversaries in both cyberspace and the electromagnetic spectrum.

(FOUO) The division commander and staff conduct the operations process, ensuring cyberspace operations are integrated throughout decisive action tasks and in accordance with appropriate authorities and legal guidance. The division employs organic and nonorganic capabilities outside and inside the DODIN to accomplish various cyberspace operations missions and supporting tasks. FM 3-94 and Army Techniques Publication 3-91, *Division Operations*, 17 OCT 2014, provide additional information on CEMA and the role of the division commander and staff.

(FOUO) The division commander and staff are responsible for certain activities in support of cyberspace operations that can result in actions and/or effects occurring primarily outside the DODIN. At the division level, most of the CEMA staff principals are required to coordinate and synchronize these activities as described in Table 5-3.

Table 5-3. Recommended TTP for divisions outside the DODIN

(FOUO) The following list of activities result in actions and/or effects that occur outside the DODIN. This list is not all inclusive. The division commander and staff:

- Plan, coordinate, synchronize, and integrate cyberspace operations missions including OCO and DCO response actions, resulting in the creation of effects primarily outside the DODIN and in support of the division scheme of maneuver.

- Develop, maintain, and disseminate a common operational picture of designated cyberspace to enable division situational understanding of cyberspace and situational understanding of friendly and threat networks.

- Receive, process, and submit CERFs from subordinate units. Develop and submit CERFs to higher headquarters.

- As required, prepare and submit input for an EReqM to higher headquarters.

- Develop, recommend, and brief the division scheme of cyberspace operations.

- As directed by higher headquarters (i.e., EXORD or FRAGORD), coordinate and integrate enablers and other expeditionary capabilities in support of division operations.

(FOUO) The division commander and staff are also responsible for certain activities in support of cyberspace operations occurring primarily inside the DODIN as described in Table 5-4 on page 39. The key staff members involved in these activities include the corps G-2, G-3, G-6 (supported by the division NOSC and division signal company), and EW officer/CEMA element.

Table 5-4. Recommended TTP for divisions inside the DODIN

(FOUO) The following list of activities result in actions and/or effects that occur inside the DODIN. This list is not all inclusive. The division commander and staff:

- Plan, coordinate, synchronize, integrate, and conduct cyberspace operations missions including DCO and DODIN operations in support of the division concept of operations.
- Oversee and direct the planning, operations, and coordination of all matters concerning division DODIN operations, network transport, information services, and spectrum management operations.
- Establish the division information network and provide operational and technical support to subordinate signal elements.
- Engineer, build, install, configure, secure, operate, maintain, and defend the division information network and recommend priorities to support the division's priorities.
- Establish and implement procedures for processing relevant information to enable development and dissemination of the division common operational picture.
- Prepare and submit CERFs to higher headquarters.
- Coordinate, plan, manage, and direct cybersecurity activities.
- As directed by higher headquarters, coordinate and integrate enablers and other expeditionary capabilities in support of division DCO and DODIN operations.

Brigade-Level Cyberspace Operations

(FOUO) The brigade combat team is the Army's primary close-combat force, which operates across the range of military operations in support of unified land operations. The brigade commander integrates and synchronizes cyberspace operations to seize, retain, and exploit an advantage over enemies and adversaries in cyberspace. The brigade employs organic and nonorganic cyberspace capabilities inside and outside the DODIN in support of unified land operations.

(FOUO) The brigade commander and staff are responsible for certain activities in support of cyberspace operations that can result in actions and/or effects occurring primarily outside the DODIN as described in Table 5-5. At the brigade level, most of the CEMA staff principals are required to coordinate and synchronize these activities.

Table 5-5. Recommended TTP for brigades outside the DODIN

(FOUO) The following list of activities result in actions and/or effects that occur outside the DODIN. This list is not all inclusive. The brigade commander and staff:

- Plan, coordinate, synchronize, and integrate cyberspace operations missions including OCO and DCO response actions, in conjunction with EW as appropriate, resulting in the creation of effects primarily outside the DODIN and in support of the brigade scheme of maneuver.
- Develop, maintain, and disseminate a common operational picture of designated cyberspace to enable situational understanding of cyberspace and friendly and threat networks.
- Develop and submit CERFs to higher headquarters.
- As required, prepare and submit input for an EReqM to higher headquarters.
- Develop, recommend, and brief the brigade scheme of cyberspace operations.
- As directed by higher headquarters (i.e., EXORD, operation order [OPORD], or FRAGORD), coordinate and integrate enablers and other cyberspace expeditionary capabilities in support of brigade operations.

(FOUO) The brigade commander and staff are also responsible for certain activities in support of cyberspace operations occurring primarily inside the DODIN as described in Table 5-6 on page 41. The key staff members involved in these activities include the brigade S-2, S-3, S-6 (supported by the brigade NOSC and signal company), and EW officer/CEMA element.

Table 5-6. Recommended TTP for brigades inside the DODIN

(FOUO) The following list of activities result in actions and/or effects that occur inside the DODIN. This list is not all inclusive. The brigade commander and staff:

- Plan, coordinate, synchronize, integrate, and conduct cyberspace operations missions including DCO and DODIN operations in support of the brigade concept of operations.
- Conduct DODIN operations and spectrum management operations for the brigade, brigade command posts, and subordinate units organic or assigned to, or operating within the brigade area of operations.
- Establish and implement procedures for processing relevant information to enable development and dissemination of the brigade common operational picture.
- Prepare and submit CERFs to higher headquarters.
- Coordinate, plan, manage, and direct brigade cybersecurity activities.
- Perform fault, configuration, accounting, performance, and security management of network system components and services to ensure systems and software applications meet the commander's operational requirements.
- As directed by higher headquarters, coordinate and integrate enablers and other expeditionary capabilities in support of brigade DCO and DODIN operations.

Conclusion

(FOUO) Commanders and staffs at corps, division, and brigade levels integrate cyberspace operations in similar manners that result in deliberate actions and effects occurring both inside and outside the Army's portion of the DODIN. These roles and responsibilities continue to evolve as the Army develops a greater understanding of cyberspace and cyberspace operations in the context of unified land operations. What is apparent from recent operations and lessons is the necessity of CEMA coordination and synchronization, which enables the staff to achieve varying levels of synergy of effort. This chapter only discusses roles and responsibilities at the echelons of corps and below. FM 3-12, *Army Cyberspace Operations*, when published, will provide greater detail and associated context to further guide commanders and staffs as they seek to more effectively integrate cyberspace operations and EW throughout the operations process.

PROVIDE US YOUR INPUT

To help you access information quickly and efficiently, the Center for Army Lessons Learned (CALL) posts all publications, along with numerous other useful products, on the CALL restricted website (CAC login required). The CALL website is restricted to U.S. government and allied personnel.

PROVIDE FEEDBACK OR REQUEST INFORMATION

https://call2.army.mil

If you have any comments, suggestions, or requests for information (RFIs), use the following links on the CALL restricted website (CAC login required): “RFI or Request Pubs” or “Contact CALL.”

PROVIDE LESSONS AND BEST PRACTICES OR SUBMIT AN AFTER ACTION REVIEW (AAR)

If your unit has identified lessons or best practices or would like to submit an AAR, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

CALL Restricted Website <https://call2.army.mil> (CAC login required):

- Select “Submit Observations, Best Practices, or AARs” tab at the top of the page.
- Under “Document Identification,” enter AAR subject in “Subject of Lesson or TTP” block.
- Identify whether or not the AAR is classified in the “Is it Classified?” block.
- Select the “Browse” button by “File to Upload” block and upload the AAR file.
- Enter questions or comments in the “Comments/Questions” block.
- Press “Submit Form” button.

Mailing Address: **Center for Army Lessons Learned**
ATTN: Chief, Collection Division
10 Meade Ave., Bldg. 50
Fort Leavenworth, KS 66027-1350

TO REQUEST COPIES OF THIS PUBLICATION

If you would like copies of this publication, please submit your request at <https://call2.army.mil>. Mouse over the “RFI or Request Pubs” tab and select “Request for Publication.” Please fill in all the information, including your unit name and street address. Please include building number and street for military posts.

NOTE: Some CALL publications are no longer available in print. Digital publications are available by using the “Products” tab on the CALL restricted website.

PRODUCTS AVAILABLE ONLINE

CENTER FOR ARMY LESSONS LEARNED

Access and download information from CALL's restricted website. CALL also offers Web-based access to the CALL archives. The CALL restricted website address is:

https://call2.army.mil

CALL produces the following publications on a variety of subjects:

- **Handbooks**
- **Bulletins, Newsletters, and Trends Reports**
- **Special Studies**
- ***News From the Front***
- **Training Lessons and Best Practices**
- **Initial Impressions Reports**

You may request these publications by using the "RFI or Request Pubs" tab on the CALL restricted website. (**NOTE:** Some CALL publications are no longer available in print. Digital publications are available by using the "Products" tab on the CALL restricted website.)

COMBINED ARMS CENTER (CAC)
Additional Publications and Resources

The CAC home page address is:

http://usacac.army.mil

Center for Army Leadership (CAL)

CAL plans and programs leadership instruction, doctrine, and research. CAL integrates and synchronizes the Professional Military Education Systems and Civilian Education System. Find CAL products at <http://usacac.army.mil/cac2/cal>.

Combat Studies Institute (CSI)

CSI is a military history think tank that produces timely and relevant military history and contemporary operational history. Find CSI products at <http://usacac.army.mil/cac2/csi/csipubs.asp>.

Combined Arms Doctrine Directorate (CADD)

CADD develops, writes, and updates Army doctrine at the corps and division level. Find the doctrinal publications at either the Army Publishing Directorate (APD) <http://www.apd.army.mil> or the Central Army Registry (formerly known as the Reimer Digital Library) <http://www.adtdl.army.mil>.

Foreign Military Studies Office (FMSO)

FMSO is a research and analysis center on Fort Leavenworth under the TRADOC G2. FMSO manages and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. Find FMSO products at <http://fmso.leavenworth.army.mil>.

Military Review (MR)

MR is a revered journal that provides a forum for original thought and debate on the art and science of land warfare and other issues of current interest to the U.S. Army and the Department of Defense. Find MR at <http://usacac.army.mil/cac2/militaryreview>.

TRADOC Intelligence Support Activity (TRISA)

TRISA is a field agency of the TRADOC G2 and a tenant organization on Fort Leavenworth. TRISA is responsible for the development of intelligence products to support the policy-making, training, combat development, models, and simulations arenas. Find TRISA at <https://atn.army.mil/media/dat/TRISA/trisa.aspx> (CAC login required).

Capability Development Integration Directorate (CDID)

CDID conducts analysis, experimentation, and integration to identify future requirements and manage current capabilities that enable the Army, as part of the Joint Force, to exercise Mission Command and to operationalize the Human Dimension. Find CDID at <http://usacac.army.mil/organizations/mccoe/cdid>.

Joint Center for International Security Force Assistance (JCISFA)

JCISFA's mission is to capture and analyze security force assistance (SFA) lessons from contemporary operations to advise combatant commands and military departments on appropriate doctrine; practices; and proven tactics, techniques, and procedures (TTP) to prepare for and conduct SFA missions efficiently. JCISFA was created to institutionalize SFA across DOD and serve as the DOD SFA Center of Excellence. Find JCISFA at <https://jcisfa.jcs.mil/Public/Index.aspx>.

Support CAC in the exchange of information by telling us about your successes so they may be shared and become Army successes.

CENTER FOR ARMY LESSONS LEARNED
10 Meade Ave. Building 50
Fort Leavenworth, KS 66027-1350

www.leavenworth.army.mil

US Army
Combined
Arms Center

"Intellectual Center of the Army"

U.S. UNCLASSIFIED
FOR OFFICIAL USE ONLY