Chapter 4
Integration through the Operations Process

This chapter discusses how the cyberspace electromagnetic activities section integrates cyberspace operations and electromagnetic warfare through the operations process. It outlines the four activities of the operations process and how the working group contributes to each activity. This chapter details how the cyberspace electromagnetic activities section and members of the working group synchronize cyberspace operations and electromagnetic warfare with intelligence preparation of the battlefield, information collection, targeting, risk management, and knowledge management processes.

SECTION I – THE OPERATIONS PROCESS

4-1. At corps and below, the planning, synchronization, and integration of cyberspace operations and EW are conducted by the CEMA section, in collaboration with key staff members that make up the CEMA working group. The CEMA section is an element of the G-3 or S-3 and works closely with members of the CEMA working group to ensure unity of effort to meet the commander's objectives. Integration and synchronization of cyberspace operations and EW—

- Unifies Army and joint forces' effort to engineer, manage, secure, and defend the DODIN.
- Ensures information collected in cyberspace and the EMS is routed to the appropriate staff to provide the commander and staff for situational awareness of the OE, targeting, and as potential intelligence.
- Ensures the efficient use of cyberspace operations and EW assets for information collection and targeting.
- Ensures appropriate coordination between Army, joint, unified action partners and host nations before employing cyberspace operations and EW.

4-2. The *operations process* includes the major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0). The operations process is the Army's framework for the organization and implementation of command and control. The CEMA working group enables the commander with the ability to understand cyberspace and the EMOE. With this understanding, the commander can better visualize and describe an operation's end state and operational approach; this in turn enables the commander to make and articulate decisions, direct, lead, and assess operations. The commander and staff at a corps or division must align the commander's concept of operations with adjacent corps and divisions, joint forces, and unified action partners when conducting large-scale combat operations to ensure unity of effort.

4-3. Commanders, staff, and subordinate headquarters use the operations process to organize efforts, integrate the warfighting functions across multiple domains, and synchronize forces to accomplish missions. Army forces plan, prepare, execute, and assess cyberspace operations and EW in collaboration with joint forces and unified action partners as required. Army commanders and staffs will likely coordinate or interact with joint forces to facilitate cyberspace operations and EW. For this reason, commanders and staff should have an awareness of joint planning systems and processes that enable cyberspace operations and EW. Some of these systems and processes include—

- The Joint Planning Process (See JP 5-0).
- Adaptive Planning (See JP 5-0).
- Review and approval process for cyberspace operations (Refer to Appendixes A and C).

- Joint Electromagnetic Spectrum Operations Planning Process (See JP 3-85).

PLANNING

4-4. *Planning* is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Commanders apply the art of command and the science of control to ensure cyberspace operations and EW support the concept of operations. Whether cyberspace operations and EW are planned and directed from higher headquarters or requested from tactical units, timely staff actions and commanders' involvement coupled with continued situational awareness of cyberspace and the EMS are critical for mission success.

4-5. The Army design methodology and military decision-making process are two planning methods used by Army headquarters. Members of the CEMA working group must understand these two methods fully. See Appendix A for a detailed discussion on how CEMA integrates cyberspace operations and EW within Army design methodology and the military decision-making process.

4-6. The Army design methodology consists of more adductive and systemic reasoning for complex, ill-formed problems. The military decision-making process consists of a more deductive and analytical approach to planning and commanders at corps and below are likely to employ military decision-making process more frequently than Army design methodology. Commanders, however, may use a different approach to planning or combine approaches. Regardless of the planning approach, commanders and staff must integrate cyberspace operations and EW throughout the planning activity. During planning, commanders and staff should seek to—

- **Understand situations and develop solutions to problems.** The commander and staff build an understanding of the cyberspace domain, information aspects of the OE, and the EMOE within the assigned AO. Commanders and staff develop a situational understanding of the impact cyberspace operations and EW effects can cause throughout multiple domains and develop solutions to resolve issues that might negatively affect neutral entities and friendly forces.
- **Task-organize the force and prioritize efforts.** The commander and staff task-organizes cyberspace and EW capabilities and implement priority of support efforts. A *priority of support* is a priority set by the commander to ensure a subordinate unit has support in accordance with its relative importance to accomplish the mission (ADP 5-0).
- **Direct, coordinate, and synchronize action.** The commander and staff use this planning function to direct, coordinate, and synchronize cyberspace operations, EW, and spectrum management operations with missions conducted through intelligence operations, IO operations, and the targeting process.
- **Anticipate events and adapt to changing circumstances.** The commander and staff anticipate potential attacks by threats in cyberspace and the EMS and adapts to the uncertain nature of operations by implementing active and passive countermeasures associated with cyberspace security and EP. The commander and staff use such tools as decision points, branches, and sequels to adapt to changing circumstances (See ADP 5-0).

4-7. The IPB process begins and is synchronized with the operations process during planning and continues throughout the operations process. During the IPB process, the G-2 or S-2 supports cyberspace operations and EW by providing the commander and staff with analyzed intelligence on the operational and mission variables in an area of interest to determine conditions relevant to those operations. This information assists the commander and staff in understanding the OE, identifying opportunities for cyberspace operations and EW, and determining appropriate COAs.

4-8. During planning, the fires support element uses the commander's intent and concept of operations to develop a fire support plan. The fire support plan is a plan that addresses each means of fire support available. It describes how Army indirect fires, joint fires, and target acquisition are integrated with a maneuver to facilitate operational success (refer to FM 3-09). The fires support coordinator or support officer collaborates with the CEWO to integrate cyberspace attacks and EA into the fire support plan.

4-9. The final product of planning is an operation plan (OPLAN) or operation order (OPORD). The OPLAN is developed by the commander and staff well in advance of execution and becomes an OPORD once directed for implementation based on a specific time or event. The CEWO is responsible for completing Annex C, Appendix 12, and upon request, assists the G-6 or S-6 with Annex H, Appendixes 1 and 6 of the OPLAN or

OPORD. The CEWO is also responsible for making updates, changes, and modifications to Annex C, Appendix 12 and assisting in updating Annex H, Appendixes 1 and 6 as appropriate, for fragmentary order(s) (FRAGORDs) (See Appendix A for Army design methodology, military decision-making process , and CEMA products for orders).

PREPARATION

4-10. *Preparation* consists of those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5.0). Preparation activities include initiating information collection, DODIN operations preparation, rehearsals, training, and inspections. Preparation requires the commander, staff, unit, and Soldiers' active engagement to ensure the force is ready to execute operations.

4-11. Preparation activities typically begin during planning and continue into execution. At corps and below, subordinate units' that are task-organized to employ cyberspace operations and EW capabilities (identified in the OPLAN or OPORD) conduct preparation activities to improve the force's opportunity for success during operations. Commanders drive preparation activities through leading and assessing. Using the following preparation functions, commanders and staff can—

- **Improve situational understanding.** Commanders, staff, and subordinate units continue to refine knowledge of cyberspace and the EMOE within the assigned AO, including the improved insight on how the use of cyberspace and the EMS could affect operations across multiple domains.
- **Develop a shared understanding of the plan.** Commanders, staff, and tasked subordinate units develop a shared understanding of the plan (described in the OPLAN or OPORD) by conducting home-station training and combat training center(s). These training events provide the perfect opportunity for subordinate commanders, leaders, and Soldiers to execute the developed plan in a controlled environment and to identify issues in the developing plan that require modification.
- **Train and become proficient in critical tasks.** Through rehearsals and training, subordinate units gain and refine skills in those individual and collective tasks essential to the success of cyberspace operations and EW. Commanders also allocate training time for anticipated and unanticipated events and circumstances.
- **Integrate the force.** Commanders allocate preparation time to put the new task-organized force into effect. Integrating the force includes detaching units, moving cyberspace and EW assets, and receiving and integrating new units and Soldiers into the force. Task-organized forces require preparation time to learn the gaining unit's policies and standards and to understand their role in the overall plan. The gaining unit requires time to assess the task-organized forces' cyberspace and EW capabilities and limitations and integrate new capabilities.
- **Ensure the positioning of forces and resources.** Positioning and task organization occur concurrently. Commanders ensure cyberspace and EA assets consist of the right personnel and equipment using pre-operations checks while ensuring those assets are in the right place at the right time.

EXECUTION

4-12. *Execution* is the act of putting a plan into action by applying combat power to accomplish the mission (ADP 5-0). The commander, staff, and subordinate commander's focus on translating decisions made during planning and preparing into actions. Commanders conduct OCO and EA to project combat power throughout cyberspace and the EMS, conduct DCO and EP to protect friendly forces and systems, and conduct reconnaissance through cyberspace and the EMS to gather combat information for continuing situational awareness.

4-13. Commanders should understand that detailed planning provides a reasonable forecast of execution but must also be aware that situations may change rapidly in cyberspace and the EMOE. During execution, commanders take concerted action to seize, retain, and exploit operational initiative while accepting risk.

4-14. *Operational initiative* is the setting or tempo and terms of action throughout an operation (ADP 3-0). By presenting the enemy with multiple cross-domain dilemmas, including cyberspace and the EMS, commanders force the enemy to react continuously, driving the enemy into positions of disadvantage.

Commanders can use cyberspace attacks and EA to force enemy commanders to abandon their preferred courses of action and make costly mistakes. Commanders retain the initiative by synchronizing cyberspace attacks and EA as fires combined with other elements of combat power to apply unrelenting pressure on the enemy using continuously changing combinations of combat power at a tempo an enemy cannot effectively counter.

4-15. Commanders and staff continue to use information collection and electromagnetic reconnaissance assets to identify enemy attempts to regain the initiative. Information collected can be used to readjust targeting priorities and fire support plans, including cyberspace attacks and EA, to keep adversaries on the defensive.

4-16. Once friendly forces seize the initiative, they immediately exploit it through continued operations to accelerate the enemy's defeat. *Defeat* is to render a force incapable of achieving its objective (ADP 3-0). Commanders can use cyberspace attacks and EA to disrupt enemy attempts to reconstitute forces and exacerbate enemy disorganization by targeting adversary command and control and sensing nodes.

ASSESSMENT

4-17. *Assessment* is the determination of the progress toward accomplishing a task, creating an effect, or achieving an objective (JP 3-0). The commander and staff continuously assess cyberspace operations and EW to determine if they have resulted in the desired effect. Assessment activities support decision making by ascertaining the progress of the operation to develop and refine plans.

4-18. Assessment both precedes and guides the other activities of the operations process, and there is no single way to conduct it. Commanders develop an effective assessment plan built around the unique challenges of the operations. A Commander develops an assessment plan by—

- Developing the assessment approach (planning).
- Developing the assessment plan (planning).
- Collecting information and intelligence (execution).
- Analyzing information and intelligence (execution).
- Communicating feedback and recommendations (execution).
- Adapting plans or operations (planning and execution).

Note. For more information on the operations process, see ADP 5-0.

SECTION II –INTEGRATING PROCESSES

4-19. Commanders and staff integrate warfighting functions and synchronize the force to adapt to changing circumstances throughout the operations process. The CEMA section aligns cyberspace operations and EW with the operations process and its associated integrating processes to identify threats in cyberspace and the EMS, to target and attack enemy cyberspace and EMS enabled systems, and to support the warfighting functions. Figure 4-1 on page 4-5 illustrates the integration and synchronization of CEMA throughout the operations process using the various integrating processes.

4-20. The operations process is the principal essential activity conducted by a commander and staff. The commander and staff integrate and synchronize CEMA with five key integrating processes throughout the operations process (see figure 4-1). These integrating processes are—

- IPB.
- Information collection.
- Targeting.
- Risk management.
- Knowledge management.

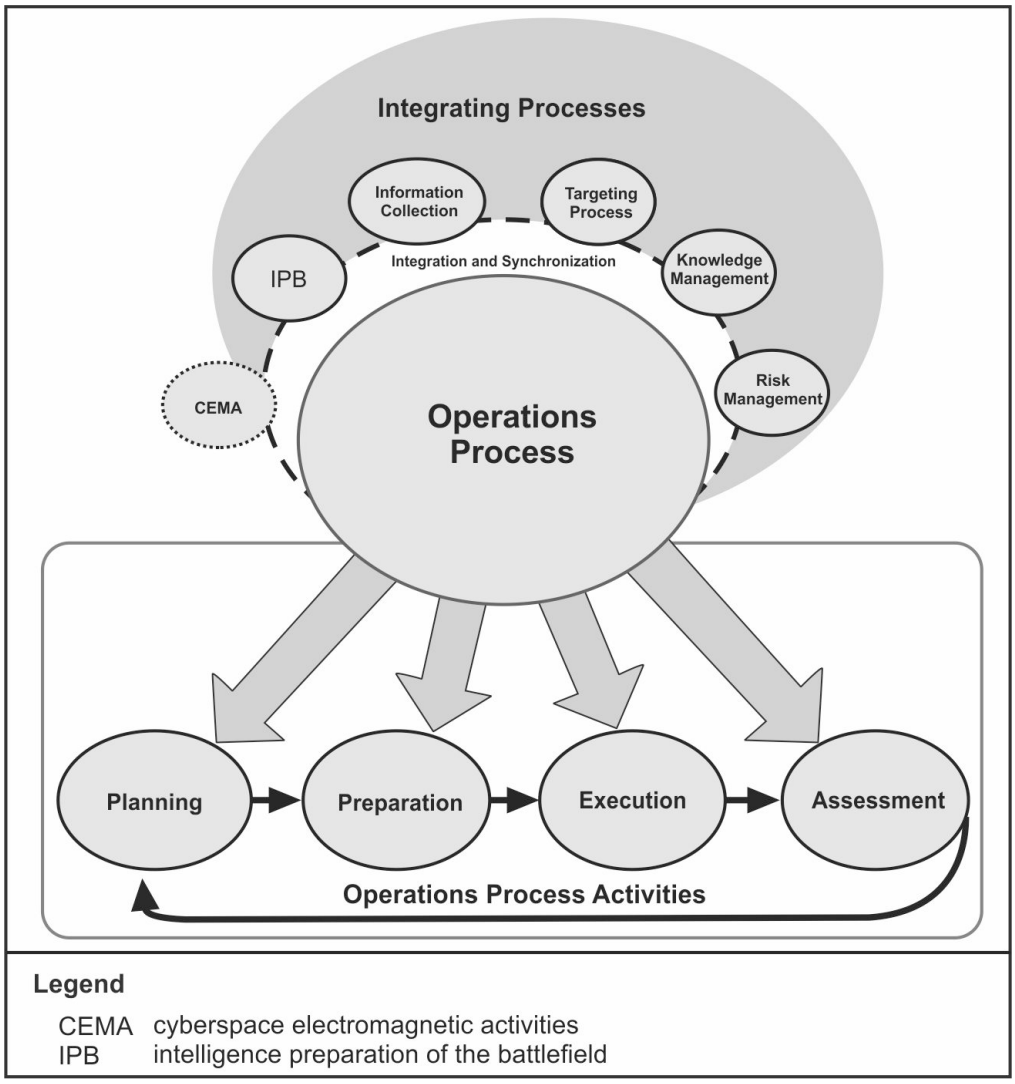

Figure 4-1. The operations process and integrating processes

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

4-21. To integrate and synchronize the tasks and missions of information collection, the G-2 or S-2 leads the staff through the IPB process. *Intelligence preparation of the battlefield* is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (ATP 2-01.3). IPB assists in developing an in-depth understanding of relevant aspects of the OE, including threats.

4-22. Integrating the IPB process into the operations process is essential in supporting the commander's ability to understand the OE and visualize operations throughout the operations process. Integrating the IPB process and the operations process is an enabler that allows commanders to design and conduct operations continuously. Integrating the IPB process and the operations process provides the information and intelligence required to plan, prepare, execute, and assess operations. Four steps in the IPB process are—

- Define the operational environment.
- Describe environment effects on operations.
- Evaluate the threat.
- Determine threat COAs.

4-23. The IPB process begins during planning activities and continues throughout the operations process. The IPB process results in IPB products used for developing friendly COAs and decision points for the commander throughout planning activities. IPB products are critical to planning cyberspace operations and EW.

DEFINE THE OPERATIONAL ENVIRONMENT

4-24. The G-2 or S-2 uses the IPB process to define cyberspace and the EMOE within an OE. Defining the cyberspace and the EMOE enables the commander and staff to visualize both friendly and enemy cyberspace and EW assets through the three layers of cyberspace and the EMS. The CEMA section supports the IPB process by assisting the G-2 or S-2 with developing and managing the electromagnetic order of battle.

4-25. The G-2 or S-2 is responsible for synchronizing available SIGINT assets. Combat information attained through cyberspace operations and EW assists the G-2 or S-2 in defining the OE. Additionally, the G-2 or S-2 may combine the intelligence disciplines with criminal intelligence to gather cyberspace and EW-related information to define the OE fully.

4-26. The G-2 or S-2 uses intelligence gathered through information collection to develop graphic AO overlays that include cyberspace and the EMS-related terrain aspects throughout the assigned AO. Graphic AO overlays of cyberspace may depict the physical layer of cyberspace more easily than the logical or cyber-persona layers. Attaining information on threat cyberspace capabilities at the logical and cyber-persona layers occurs through SIGINT, criminal intelligence, or cyberspace exploitation.

4-27. The G3 should ensure information gathered by operational systems, platforms, and sensors, such as those used to monitor friendly networks during the execution of DODIN operations, is formally disseminated and made accessible to the intelligence community. This is a critical component necessary to define the operational environment in support of cyberspace operations, as well as to enable the G2 or S2 to evaluate the threat.

DESCRIBE ENVIRONMENTAL EFFECTS ON CYBERSPACE AND THE ELECTROMAGNETIC SPECTRUM

4-28. As a result of answering IRs received from the CEMA section, the G-2 or S-2 defines the types of threats and threat cyberspace and EW capabilities while also defining environmental effects. It is essential to consider how environmental effects will impact friendly and enemy operations, including those that may affect cyberspace and the EMS. Such considerations include terrain, weather, light, illumination data, and civil. Terrain analysis allows the commander to understand the terrain's impact on cyberspace operations and EW. The CEMA working group conducts cyberspace and the EMS-related terrain analysis by employing traditional methods and examining the five military aspects of terrain when determining threat courses of action:

- Observation and fields of fire.
- Avenues of approach.
- Key terrain.
- Obstacles.
- Cover and concealment.

4-29. Civil considerations are applied by cross walking with the operational variables. The G-2 or S-2 includes such civil considerations as cellular phone coverage, internet service providers, and electricity distribution for industrial, commercial, and residential areas.

4-30. Threats in cyberspace and the EMS and all intelligence gathered and analyzed for environmental effects are incorporated into such IPB products as the threat overlays, threat description tables, terrain effects matrices, terrain analysis, or modified combined obstacle overlay, and assessments.

EVALUATE THE THREAT

4-31. In collaboration with the CEMA section, the G-2 or S-2 determines threat cyberspace and EW capabilities, doctrinal principles, and tactics, techniques, and procedures used by the enemy in the assigned AO. An enemy's use of the cyberspace and the EMS to accomplish or support their objectives vary. Using input from the various intelligence disciplines, The G-2 or S-2 and CEMA section evaluate the threat, create threat models, develop broad threat COAs, and identify enemy high value targets (HVTs). When creating the threat model, the G-2 or S-2 incorporates cyberspace and EMS consideration to determine how the enemy integrates and uses cyberspace and EW capabilities.

4-32. The enemy will likely have cyberspace and EW capabilities that operate across all warfighting functions. To increase situational awareness, the G-2 or S-2 should identify enemy cyberspace and EMS assets employed in support of each warfighting function. The G-2 or S-2 also evaluates neutral actors and adversaries conducting operations in cyberspace and the EMS throughout the AO and forwards the information to local and Army law enforcement or counterintelligence elements. Neutral actors and adversaries include—

- Nation-state actors.
- Transnational non-state actors or terrorists.
- Criminal organizations or multinational cyber syndicate actors.
- Individual actors, hacktivists, or small groups.
- Insider threats.
- Autonomous systems, software, and malicious code.

4-33. Data gathered by evaluating the threat helps develop threat models that depict how enemy forces typically execute operations, including threat characteristics on how they use cyberspace and the EMS. The threat model also describes how enemy forces historically reacted to various types of cyberspace attacks and EA in similar circumstances relative to OE and overall operation.

4-34. In addition to the threat model, the G-2 or S-2 creates threat capability statements that align with the threat model and include options or other supporting operations the enemy can use to affect the accomplishment of the friendly forces' mission. Threat models guide the development of threat COAs.

DETERMINE THREAT COURSES OF ACTION

4-35. The G-2 or S-2 uses data gathered through threat evaluation to identify and develop the full range of COAs an enemy has available. The G-2 or S-2 collaborates with the CEMA section to develop threat COAs regarding an enemy's capabilities in cyberspace and the EMS. The G-2 or S-2 provides the G-3 or S-3 with information and intelligence necessary for developing friendly COAs to counter those available threats COAs and influence friendly operations. The G-2 or S-2 also collaborates with the CEMA section to develop countermeasures to threat COAs in cyberspace and the EMS. Each threat COA includes identified cyberspace attack and EA-related HVTs such as nodes, command and control centers, communications towers, satellites, internet service providers, fiber optic lines, and local power substations.

4-36. When developing friendly COAs related to countering the enemy's capabilities in cyberspace and the EMS, the G-2 or S-2, in collaboration with the CEMA section, incorporates such considerations as the adversary's historical use of cyberspace and the EMS and the types of cyberspace and EMS-related operations they have conducted. The G-2 or S-2 assists the CEMA section in determining the unit's specific cyberspace and EW assets that can produce desired effects when engaging HVTs.

4-37. The G-2 or S-2 should understand that a cyberspace threat could be operating outside of the unit's assigned AO. An enemy can use proxies worldwide beyond a unit's area of interest. Development of threat

COAs results from first identifying HVTs and HPTs. Threat COAs include templates and event matrices that identify potential objectives, named areas of interest and target areas of interest. A *named area of interest* is the geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected (JP 2-01.3). A *target area of interest* is the geographical area where high-value targets can be acquired and engaged by friendly forces (JP 2-01.3).

4-38. The CEMA section conducts terrain analysis to examine aspects of terrain in cyberspace and the EMS for determining obstacles such as firewalls, port blocks, threat sensors, and jamming capabilities that require immediate mitigation for continued operation. The CEMA section also identifies the various avenues of approach to employ cyberspace attack and EA on enemy cyberspace and EMS capabilities. Through terrain analysis, the CEMA identifies potential weaknesses in friendly forces' posture in cyberspace and the EMS that require additional cover and concealment through such techniques as electromagnetic hardening actions, password protection, emission control, or by incorporating Internet Protocol (IP) hiding techniques.

4-39. During terrain analysis, it is important to identify key locations in cyberspace and the EMS that can become access points. These access points provide avenues of approach or can provide observation and fields of fire where network traffic can be monitored, intercepted, or recorded through SIGINT, cyberspace exploitation, or ES. By identifying cyberspace and EW-related obstacles, avenues of approach, cover and concealment, and observation and fields of fire, the CEMA section can determine locations in those aspects of terrain to consider as key terrains. Key terrains include those major access points for observing incoming threats and avenues for launching cyberspace attack and EA. Terrain in cyberspace and the EMS connected to critical assets on the DODIN are considered as key terrains.

Note. For more information on the IPB process, see ATP 2-01.3.

INFORMATION COLLECTION

4-40. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55). These sensors and assets may include cyberspace operations and EW assets conducting cyberspace exploitation operations, electromagnetic probing, and electromagnetic reconnaissance for information collection.

4-41. Information collection is the acquisition of information and the provision of this information to processing elements. Information collection integrates the intelligence and operations staff functions with a focus on answering the CCIRs, and IRs that assists the commander and staff in shaping the OE and conducting operations. The commander drives information collection coordinated by the staff and led by the G-2 or S-2. The following are the steps of information collection:

- Plan requirements and assess collection.
- Task and direct collection.
- Execute collection.

4-42. Information collection enables the commander to understand and visualize the operation. Information collection identifies gaps in information that require aligning intelligence assets with cyberspace exploitation, electromagnetic reconnaissance, and electromagnetic probing to collect data on those gaps. The *decide* and *detect* steps of targeting also rely heavily on information collection. Enemy cyberspace capabilities identified through information collection assist the CEMA working group in identifying potential targets and key terrain in cyberspace.

PLAN REQUIREMENTS AND ASSESS COLLECTION

4-43. The G-2 or S-2 collaborates with the other staff to receive and validate IRs for collection. The CEMA section provides the G-2 or S-2 with cyberspace and EMS-related IRs requesting information on friendly, enemy, and neutral actors operating in the AO. The CEWO identifies all cyberspace and EMS-related IRs to present to the commander as potential CCIRs. The G-2 or S-2 prepares the requirements planning tools and recommend cyberspace and EW assets for information collection to the G-3 or S-3.

TASK AND DIRECT COLLECTION

4-44. In addition to the G-2 or S-2 using SIGINT for information collection, the G-3 or S-3 may task cyberspace and EW assets to support the information collection effort. In this instance, the CEMA section will assist the G-2 or S-2 by assigning organic EW assets while requesting additional EW and cyberspace assets as required. The G-2 or S-2 is responsible for maintaining the synchronization of all assets used for the information collection efforts.

EXECUTE COLLECTION

4-45. The focus when executing information collection is to collect data that answers CCIRs and IRs for analysis during the IPB process. This information assists in shaping the OE and attaining information on the enemy. Collection activities acquire information about the enemy, including their cyberspace and EMS-dependent capabilities and assets. Collection activities begin shortly after the *receipt of the mission* activities of the operations process and continue throughout preparation and execution activities.

4-46. The G-2 or S-2 executes collection by conducting—

- Intelligence operations.
- Reconnaissance.
- Surveillance.
- Security operations.

Intelligence Operations

4-47. *Intelligence operations* are the tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements (ADP 2-0). Through intelligence operations, the G-2 or S-2 attains information regarding threat capabilities, activities, disposition, and characteristics. Intelligence operations use multiple intelligence disciplines to collect information regarding cyberspace and the EMS to satisfy CCIRs and IRs. However, knowledge attained from the other intelligence disciplines may also provide cyberspace and EMS related insight. In addition to gathering information on peer and near-peer threats through SIGINT, criminal intelligence collects information on cyberspace and EMS-related illegal activities conducted throughout the assigned AO. For more information on criminal intelligence, refer to AR 195-2.

Reconnaissance

4-48. *Reconnaissance* is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (JP 2-0). Reconnaissance produces information about the assigned AO. Through reconnaissance, the G-2 or S-2 can collect information regarding such mission and operational variables as terrain characteristics, enemy and friendly obstacles to movement, and the disposition of enemy forces and civilians. Combined employment of three methods of reconnaissance (dismounted, mounted, and aerial) can result in the location and type(s) of friendly, civilian, and threat cyberspace and EW capabilities operating in the assigned AO. Upon request, the CEMA section supports the G-2 or S-2's reconnaissance efforts by employing EW assets to conduct electromagnetic reconnaissance to collect information in the EMS and request OCO support to conduct cyberspace exploitation in cyberspace.

Surveillance

4-49. *Surveillance* is the systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means (JP 3-0). Surveillance involves observing an area to collect information and monitoring civilians and threats in a named area of interest or target area of interest. Surveillance may be autonomous or part of a reconnaissance mission. Collecting information in cyberspace and the EMS as part of a surveillance mission is also called network surveillance. *Network Surveillance* is the observation of organizational, social, communications, cyberspace, or infrastructure connections and relationships (FM 2-0). Network surveillance can also include detailed

information on connections and relationships among individuals, groups, and organizations, and the role and importance of aspects of physical or virtual infrastructure.

4-50. Information collected through network surveillance and other surveillance types are enablers to the IPB process. This collected information provides insight into enemy cyberspace and EW capabilities and assets. Upon request, the CEMA section supports the G-2 or S-2's surveillance efforts by requesting OCO support to employ cyberspace exploitation or by using EW assets to conduct electromagnetic reconnaissance to conduct surveillance in enemy and neutral cyberspace and the EMS. Information collected through cyberspace exploitation and electromagnetic reconnaissance includes mission and operational variables such as terrain characteristics, enemy and friendly obstacles, and the disposition of enemy forces and civilians.

Security Operations

4-51. *Security operations* are those operations performed by commanders to provide early and accurate warning of enemy operations, to provide the forces being protected with time and maneuver space within which to react to the enemy and to develop the situation to allow commanders to effectively use their protected forces (ADP 3-90). Early and accurate warnings provide friendly forces with time and maneuverability to react and create an opportunity for the commander to employ force protection measures. Cyberspace defense, cyberspace security, and EP include actions that allow early detection and mitigation of threats in cyberspace and the EMS. Additionally, ES missions conduct electromagnetic reconnaissance to attain information about the disposition of enemy threats in the EMS and modify security efforts.

4-52. The ultimate goal of security operations is to collect information on an enemy's COA that provide early warning and continuously disrupt enemy attacks. During security operations, information collected on an enemy's COA in cyberspace and the EMS allows units to take preemptive measures that prevent enemy intelligence, surveillance, and reconnaissance assets from determining friendly locations, strengths, and weaknesses. Security operations also present opportunities to identify HVTs for future cyberspace attacks or EA.

Note. For more intelligence information, see FM 2-0. For more details of information collection, see FM 3-55.

TERRAIN ASPECTS

4-53. *Key terrain* is any locality, or area, the seizure or retention of which affords a marked advantage to either force (JP 2-01.3). Key terrain in cyberspace and the EMS is comparable to terrain in the other domains in that prevailing affords any combatant a position of advantage. Maintaining a secured prevalence in cyberspace and the EMS is a feasible objective when conducting cyberspace operations and EW. Seizing and retaining the entirety of cyberspace and the EMS to the exclusion of all enemies and adversaries is an unobtainable goal. It is also possible for both friendly and enemy forces to occupy the same terrain in cyberspace and the EMS or use the same processes for conducting operations in and through cyberspace and the EMS without knowing each other's presence. Another characteristic of terrain in cyberspace is that virtual components, identified in the logical network layer or the cyber-persona layer, constitutes locality in cyberspace. For this reason, identification of key cyberspace terrain is an essential component of planning cyberspace operations. Like the physical domain, commanders and staff must consider all of the military aspects of terrain. However, unlike the physical domain, commanders and staff must remember that the cyberspace terrain may change at any time. For example, an attacker may manipulate a firewall to create avenues of approach, or the enemy removing a node from the network may be a key terrain.

4-54. Obstacles in cyberspace may include firewalls and port blocks. Avenues of approach in cyberspace can be analyzed to identify nodes and links that connect endpoints to specific sites. Cover and concealment may include hiding IP addresses or incorporating password-protected access to networks and network systems. Cyberspace observation and fields of fire include areas where network traffic can be monitored, intercepted, or recorded. Key cyber terrain provides access points to major lines of communications, key waypoints for observing incoming threats, launch points for cyberspace attacks and mission-relevant cyberspace terrain related to critical assets connected to the DODIN.

4-55. Obstacles in the EMS may include electromagnetic environmental effects, enemy deployment of sensors and radars to detect friendly use of the EMS, and enemy employment of electromagnetic hardening, masking, and security measures. Avenues of approach in the EMS can be analyzed to identify spectrum-dependent systems, devices, and associated infrastructures that connect endpoints to specific locations (precision geolocation). Cover and concealment can include emission control or the implementation of such electromagnetic masking techniques as low-observability, low probability of intercept, and low probability of detection. EMS fields of fire include those areas in the EMS where enemy electromagnetic energy can be detected, identified, and evaluated through electromagnetic reconnaissance.

4-56. Key terrain in the EMS includes frequencies used as access points and launch points to enemy spectrum-dependent systems, devices, and associated infrastructures. Key terrain also includes frequencies used for preemptive countermeasures, observing incoming threats, and critical assets dependent on the EMS. Key physical terrain is also imperative to the success of EW operations. Key terrain that provides superior line of sight over the adversary's position will help ensure friendly forces maintain a marked advantage over the adversary.

4-57. Members of the CEMA working group need to match mission objectives with terrain analysis during planning to determine key terrain in friendly, neutral, and enemy cyberspace (See Appendix A). Correlating objectives with key terrain ensures mission dependencies in cyberspace and the EMS are identified and prioritized for protection. The results from interdependent systems, networks, and infrastructure that support a mission objective may require in-depth analysis to develop customized risk management.

TARGETING

4-58. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). A *target* is an entity or object that performs a function for the adversary considered for possible engagement or other actions. (JP 3-60).

4-59. When targeting for cyberspace effects, the physical network layer is the medium through which all digital data travels. The physical network layer includes wired (land and undersea cable), and wireless (radio, radio-relay, cellular, satellite) transmission means. The physical network layer is a point of reference used during targeting to determine the geographic location of an enemy's cyberspace and EMS capabilities.

4-60. When targeting, planners may know the logical location of some targets without knowing their physical location. The same is true when defending against threats in cyberspace. Defenders may know the logical point of origin for a threat without necessarily knowing the physical location of that threat. Engagement of logical network layer targets can only occur with a cyberspace capability.

4-61. The logical network layer provides target planners with an alternate view of the target that is different from the physical network layer. A target's position in the logical layer is identified by its IP addresses. Targets located by their IP address depict how nodes in the physical layer correlate to form networks in cyberspace. Targeting in the logical layer requires the IP address and access to the logical network to deliver cyberspace effects. The ability of adversaries to change logical layer network configurations can complicate fires and effects against both logical and cyber-persona layer targets, but the operational benefit of affecting those targets often outweigh targeting challenges.

4-62. The inability to target a cyber-persona in a distinct area or form in the physical and logical network layers presents unique complexities. Because of these complexities, target positioning at the cyber-persona layer often requires multiple intelligence collection methods and an extensive analysis to develop insight and situational understanding to identify actionable targets. Like the logical network layer, cyber-personas can change quickly compared to changes in the physical network layer.

4-63. EA is exceptionally well suited to attack spectrum-dependent targets that are difficult to locate physically, cannot be accurately targeted for lethal fires, or require only temporary disruption. The fires support element plans, prepares, executes, and assesses fires supporting current and future operations by integrating coordinated lethal and nonlethal effects through the targeting process. Lethal and nonlethal effects include indirect fires, air and missile defense, joint fires, cyberspace attacks, and EA.

4-64. Targeting is a multidiscipline effort that requires coordinated interaction among the commander, the fires support element, and several staff sections that form the targeting working group. The commander

prioritizes fires to the targeting working group and provides clear and concise guidance on effects expected from all fires, including cyberspace attacks and EA. *Priority of fires* is the commander's guidance to the staff, subordinate commanders, fires planners, and supporting agencies to employ fires in accordance with the relative importance of the unit's mission (FM 3-09). The targeting working group determines which targets to engage and how, where, and when to engage them based on the targeting guidance and priorities of the commander.

4-65. The targeting working group assigns lethal and nonlethal capabilities, including cyberspace attack and EA capabilities, to produce the desired effect on each target, ensuring compliance with the rules of engagement. The CEMA section participates in the targeting working group and provides recommendations for the employment of cyberspace and EMS-related actions against targets to meet the commander's intent and inclusion in the scheme of fires. *Scheme of fires* is the detailed, logical sequence of targets and fire support events to find and engage targets to accomplish the supported commander's objectives (JP 3-09).

4-66. The CEMA section works closely with the fires support element to coordinate and manage cyberspace and EW assets as part of the fire support plan. This process is called fire support coordination and is the planning and executing of fire so that targets are adequately covered by a suitable weapon or group of weapons (JP 3-09).

TARGETING FUNCTIONS

4-67. The G-2 or S-2, in collaboration with the CEMA section and the fires support element, detects, identifies, and locates targets through target acquisition. Effective employment of weapons, including EA and cyberspace attacks, require sufficient intelligence gained through target acquisition. The G-2 or S-2 conducts information collection to provide the fires support element, members of the targeting working group, and members of the targeting board with intelligence information used for targeting. This information includes threat cyberspace and EMS-enabled capabilities that require an individual or combined effect from lethal or nonlethal attacks.

4-68. Targeting occurs continuously throughout operations. Army targeting methodology consists of four functions: decide, detect, deliver, and assess (D3A). These targeting functions occur throughout the operations process. Commanders and staff should also be conversant with joint targeting methodology and understand how each of these processes and methodologies relate, because cyberspace operations and EW are usually coordinated by a joint force commander. Table 4-1, page 4-13, illustrates a crosswalk between the operations process, the joint targeting cycle, D3A, and military decision-making process.

Table 4-1. Targeting crosswalk

Operations Process		*Joint Targeting Cycle*	*D3A*	*Military Decision-Making process*	*Targeting Tasks*
Continuous Assessment	Plan	1. Commander's Objectives, Targeting Guidance, and Intent.	Decide	Mission Analysis	• Perform target value analysis to develop fire support (including cyberspace, electromagnetic warfare, and information related capabilities) high-value targets. • Provide fire support, information-related capabilities, cyberspace, and electromagnetic warfare related input to the commander's targeting guidance and desired effects.
		2. Target Development and Prioritization.		Course of Action Development	• Designate potential high-payoff targets. • Deconflict and coordinate potential high-payoff targets. • Develop a high-payoff target list. • Establish target selection standards. • Develop an attack guidance matrix. • Develop fire support, cyberspace, and electromagnetic warfare related tasks. • Develop associated measures of performance and measures of effectiveness.
		3. Capabilities Analysis.		Course of Action Analysis	• Refine the high-payoff target list. • Refine the target selection standard. • Refine the attack guidance matrix. • Refine fire support tasks. • Refine associated measures of performance and measures of effectiveness.
		4. Commander's Decision and Force Assignment.		Orders Production	• Finalize the high-payoff target list. • Finalize target selection standards. • Finalize the attack guidance matrix. • Finalize the targeting synchronization matrix. • Finalize fire support tasks. • Finalize associated measures of performance and measures of effectiveness. • Submit information requirements to battalion or brigade G-2/S-2.
	Prepare	5. Mission Planning and Force Execution.	Detect		• Execute Information Collection Plan. • Update information requirements as they are answered. • Update the high-payoff target list, attack guidance matrix, and targeting synchronization matrix. • Update fire support, cyberspace, and electromagnetic warfare related tasks. • Update associated measures of performance and measures of effectiveness

Table 4-1. Targeting crosswalk (continued)

Operations Process		*Joint Targeting Cycle*	*D3A*	*Military Decision-Making Process*	*Targeting Tasks*
	Execute	**6. Assessment**	**Deliver**		• Execute fire support, cyberspace attacks, and electromagnetic attacks according to the attack guidance matrix and the targeting synchronization matrix.
	Assess		**Assess**		• Assess task accomplishment (as determined by measures of performance). • Assess effects (as determined by measures of effectiveness. • Refine fire support tasks and associated measures and reengage target if required
Legend: D3A decide, detect, deliver, and assess					

Decide

4-69. The decide function is the first step of the targeting process. It begins with the military decision-making process and continues throughout an operation. The CEMA section conducts the following actions during the decide function of targeting—

- Threat cyberspace and EW-related capabilities and characteristics during target value analysis to identify high-value targets. A *high-value target* is a target the enemy commander requires for the successful completion of the mission (JP 3-60).
- Identifying potential cyberspace and EW-related HPTs. A *high-payoff target* is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (JP 3-60). A high-payoff target is a high-value target that must be acquired and successfully engaged for the success of the commander's mission.
- Specific targets that should be acquired and engaged using a cyberspace attack or EA capability and established target selection standards.
- Location and time that targets are likely to be found through intelligence operations and how long the target will remain fixed.
- Surveillance, reconnaissance, and target acquisition objectives for targets receiving cyberspace attacks or EA and determining if the unit has the necessary cyberspace attack or EA capabilities to deliver appropriate effects.
- Cyberspace and EMS-related IRs essential to the targeting effort.
- When, where, and with what priority should the targets be engaged, and what cyberspace attack or EA capability to employ for effects.
- The level of effectiveness that constitutes a successful cyberspace attack or EA and if the engagement achieved the commander's objective.
- If a cyberspace attack or EA can affect a target, and how and what type of cyberspace attack or EA can create the desired effect.
- How to obtain the information needed to assess a cyberspace attack or EA to determine success or failure, and who will receive and process it.
- Who will be the decision-making authority to determine the success or failure of a cyberspace attack or EA?
- What contingency action will occur if a cyberspace attack or EA is unsuccessful, and who has the authority to direct those actions?
- Identifying the unit's EW assets available for tasking and begin drafting FRAGOS.
- Drafting the RFS for OCO support to meet targeting requirements.
- Collaborating with units at higher, lower, and adjacent echelons for EW support to satisfy identified gaps in EW capabilities.

- Drafting the Joint Tactical Air Request for airborne EA and other necessary EW requesting forms, if required.
- Open communications with the higher command to receive updates on whether anticipated cyberspace attack and EA-related targets have been validated and added to the JTF headquarters' joint target list.
- Discussing cyberspace and EW-related risk that the commander will use to make risk determinations.
- Determining the level of authorities for the engaging targets using cyberspace and electromagnetic attacks.

4-70. During the decide function, the targeting working group identifies target restrictions that prohibit or restrict cyberspace attacks or EA on specified targets without approval from higher authorities. The sources of these restrictions include military risk, the law of war, rules of engagement, or other considerations. The JTF annotates entities within the AO prohibited from attack on the no-strike list and targets with restrictions on the restricted target list.

Detect

4-71. The detect function of the targeting process is the second step of the targeting process; during this step ES capabilities or other target acquisition assets locate and track a specified target to the required level of accuracy in time and space. During the detect function, the G-2 or S-2 coordinates with the targeting working group in developing the information collection plan. Before conducting the deliver function, the targeting team must establish measures of performance and measures of effectiveness for cyberspace and electromagnetic attacks to ensure they meet the commander's objectives.

4-72. The targeting working group focuses on the surveillance effort by identifying named areas of interest and target areas of interest integrated into the information collection plan. Named areas of interest are typically selected to capture indications of adversary courses of action but may be related to conditions of the OE.

4-73. The targeting working group identifies HPTs during planning and war-gaming. Target areas of interest that require specific engagements using cyberspace attack or EA capabilities differ from engagement areas. An engagement area is an area of concentration where a commander employs all available weapons to engage a target. In contrast, a target area of interest engagement uses a specific weapons system to engage a target. During the detect function, the CEMA section conducts the following actions–

- Provides cyberspace and EW-related IRs to determine HPTs that, when validated by the commander, are added to the priority intelligence requirement.
- Tasks EW assets, when required, to conduct electromagnetic reconnaissance to support information collection.
- Updates cyberspace attack and EA-related HVTs and HPTs.
- Determines if identified targets can be affected using OCO or EA (or both), and what type of EA capability can create the desired effect

---

Note. The CEMA section alone cannot determine the type of cyberspace attack capability to use on targets. The CEMA section must coordinate with higher headquarters CEMA staff and appropriate joint cyberspace entities to develop an understanding of availability, feasibility, and suitability of specific cyberspace capabilities.

- Advocating for the nomination of cyberspace attack and EA-related targets to the JTF headquarters' joint integrated prioritized target list and the joint targeting cycle.
- Developing the RFS for OCO support.

Deliver

4-74. The deliver function of the targeting process executes the target engagement guidance and supports the commander's battle plan upon confirmation of the location and identity of HPTs. Close coordination between the CEMA section, intelligence, and fires support element is critical when detecting targets and

delivering cyberspace attacks and EA. The fire support coordinator or fire support officer details fires coordination in the OPLAN or OPORD or target synchronization matrix.

Assess

4-75. The assess function occurs throughout the operations process. During the assess function, targets are continuously refined and adjusted by the commander and staff in response to new or unforeseen situations presented during operations. Combat assessment measures the effectiveness of cyberspace attack and EA capabilities on the target and concludes with recommendations for reattack, continued attack, or to cease an attack. Recommendations for reattack, continued attack, and ceasing EA are combined G-3 or S-3 and intelligence functions approved by the commander. For more information on the targeting cycle and target development process, see ATP 3-60.

CONSIDERATIONS WHEN TARGETING

4-76. The fires support element, in collaboration with the G-3 or S-3 and G-2 or S-2, uses targeting cycles and target development processes to select, prioritize, determine the type of effects, and duration of effects on targets. CEMA's planning, integrating, synchronizing, and assessing cyberspace operations and EW becomes apparent during the targeting process. Three important aspects of cyberspace and EW operations that require consideration during targeting processes are—

- Characteristics of cyberspace and electromagnetic warfare capabilities.
- Cascading, compounding, and collateral effects.
- Reversibility of effects.
- Considerations when requesting OCO support for targeting.

CHARACTERISTICS OF CYBERSPACE AND ELECTROMAGNETIC WARFARE CAPABILITIES

4-77. Cyberspace capabilities are developed based on gathered intelligence and from operational and mission variables attained regarding an OE. In cyberspace operations, cyberspace forces consider such conditions as the type of computer operating system used by an enemy or adversary, the make and model of the hardware, the version of software installed on an enemy or adversary's computer, and the availability of cyberspace attack resources before creating effects on a target.

4-78. EW capabilities are also developed based on gathered intelligence on operational and mission variables attained regarding an EMOE. In EW, targeting planners compare the types and capabilities of known spectrum-dependent devices that enemies use to the availability of EW resources before creating EW effects on a target. Targets include enemy spectrum-dependent devices carried by personnel and spectrum dependent systems used with or in weapons systems, sensory systems, facilities, and cyberspace capabilities that require the use of the EMS.

CASCADING, COMPOUNDING, AND COLLATERAL EFFECTS

4-79. The CEMA section should understand the overlaps amongst the military, other government, corporations, and private sectors in cyberspace. These overlaps are particularly important for estimates of possible cascading, compounding, or collateral effects when targeting enemy and adversary cyberspace capabilities. The same level of consideration is required when targeting enemy and adversary spectrum-dependent devices in the EMS.

4-80. Cyberspace capabilities can create effects beyond the geographic boundaries of an AO and a commander's area of interest. Employing cyberspace capabilities for attack or manipulation purposes within an area of interest require additional authorities beyond those given to a corps and below commander. Effects resulting from cyberspace attack operations can cause cascading effects beyond the targeted system that were not evident to the targeting planners. Cascading effects can sometimes travel through subordinate systems to attain access to the targeted system. Cascading effects can also travel through lateral or high-level systems to access a targeted system. Compounding effects are a gathering of various cyberspace effects that have interacted in ways that may have been either intended or unforeseen. Effects resulting from EA can cause cascading effects

in the EMS beyond enemy or adversary's spectrum-dependent devices, disrupting or denying friendly forces access to the EMS throughout the EMOE.

4-81. Collateral effects, including collateral damage, are the accidental cyberspace or EW effects of military operations on non-combatant and civilian cyberspace or EW capabilities that were not the intended target when implementing fires.

Note. Rules of Engagement or an operations order may limit cyberspace or EW operations to only those cyberspace or EW tasks that may result in no or minimal collateral effects. The CEMA spectrum manager must deconflict the joint restriction frequency list to mitigate EMI before all EW missions.

REVERSIBILITY OF EFFECTS

4-82. Targeting planners must consider the level of control that they can exercise throughout each cyberspace and electromagnetic attack. Categorization of reversibility of effects are—

- **Operator reversible effects.** These effects can be recalled, recovered, or terminated by friendly forces. Operator reversible effects typically represent a lower risk of undesired consequences, including discovery or retaliation.
- **Non-operator reversible effects.** These are effects that targeting planners cannot recall, recover, or terminate after execution. Non-operator reversible effects typically represent a higher risk of response from the threat or other undesired consequences and may require more coordination.

Considerations When Requesting Offensive Cyberspace Operations for Targeting

4-83. The integration of OCO into the targeting process requires both long-term preparation and real-time mission planning during execution activities of the operations process. Due to target development and access to both OCO capabilities and access to an enemy in cyberspace, it is essential to emphasize the necessity for long-term preparation and planning of OCO for deliberate targets and effects.

4-84. When planning for OCO support to attack deliberate targets, the CEMA working group should consider the following:

- Determine if the target is targetable using OCO. Generally, the only potential targets that receive effects from a cyberspace attack are actively functioning in some portion of the information environment (data or information generation, processing, storage, communications, and digital data consumption or destruction).
- Ensure the target has not already been nominated or on an existing targeting list. If it has not already been nominated or placed on a current targeting list, it will require nomination for further target development.
- Consolidate all answered CCIRs and IRs. CCIRs and IRs may include such threat cyberspace intelligence as—links or nodes; associated hardware or software; specific software versions and configurations, communications protocol; physical or logical dependencies; or specific identifiers (IP address, machine access control address, international mobile subscriber identity, or phone numbers).
- Determine if intelligence attained through the IPB also includes information necessary to tailor targeting development on avenues to gain access to an enemy's cyberspace capabilities. Approaches to attain access to an enemy's cyberspace capabilities include—telephony, IP, embedded systems, and radio frequencies.
- The CEMA section is responsible for providing regular updates on a combat mission team's ability to conduct OCO as well as provide updated information on the supported operation.

Note. Access to an enemy's cyberspace capability does not guarantee the success of an employed cyberspace attack. The combat mission team must tailor the capability to create the desired effect on an enemy's cyberspace capability.

RISK MANAGEMENT

4-85. *Risk management* is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0) and an element of command and control. Risk is the exposure of someone or something valued to danger, harm, or loss, and is inherent in all operations. The commander and staff conduct risk management throughout the operations process to identify and mitigate risks associated with hazards that can cause friendly and civilian casualties, damage or destruction of equipment, or otherwise impact mission effectiveness. Aspects of cyberspace defense and security operations and EP missions include risk mitigation measures as part of risk management.

4-86. Risk management is integrated into planning activities and continues throughout the operations process. Risk management consists of the following steps:

- Identify the hazards.
- Assess the hazards.
- Develop controls and make risk decisions.
- Implement controls.
- Supervise and evaluate.

4-87. The CEMA section, as with all staff elements, incorporate risk management into cyberspace operations and EW-related running estimates and recommendations to mitigate risk. The G-3/S-3 coordinates risk management amongst all staff elements during the operations process. For more information on the risk management process, see ATP 5-19.

RISKS IN CYBERSPACE AND THE ELECTROMAGNETIC SPECTRUM

4-88. Risk is inherent in all military operations. When commanders accept risks, they create opportunities to seize, retain, and exploit the initiative and achieve decisive results. The willingness to incur risks is often the key to exposing an enemy's weaknesses that the enemy considers beyond friendly reach. Commanders assess and mitigate risks continuously throughout the operations process. Many risks to the DODIN-A come from enemies, adversaries, and insiders. Some threats are well equipped and well trained, while some are novices using readily available and relatively inexpensive equipment and software. Army users of the DODIN are trained on basic cyberspace security, focusing on the safe use of information technology and understanding common threats in cyberspace.

4-89. Risk management is the Army's primary decision-making process for identifying hazards and controlling risks. The process applies to all types of operations, tasks, and activities, including cyberspace operations. The factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations provide a standardized methodology for addressing both threat and hazard-based risks. Risks associated with cyberspace operations fall into four major categories—

- Operational risks.
- Technical risks.
- Policy risks.
- Operations security risks.

Operational Risks

4-90. Operational risks pertain to the consequences that cyberspace and EMS threats pose to mission effectiveness. Operational consequences are the measure of cyberspace attack and EA effectiveness. Cyberspace intrusions or attacks, and likewise in the EMS, can compromise networks, systems, and data, which can result in operational consequences such as injury or death of personnel, damage to or loss of equipment or property, degradation of capabilities, mission degradation, or even mission failure. Exfiltration of data from

Army networks by the enemy can undermine the element of surprise and result in loss of initiative. Enemy or adversary forces may conduct cyberspace and EMS attacks to exposed friendly networks and capabilities, compromising future cyberspace attacks and cyberspace exploitation missions.

4-91. Friendly forces conducting cyberspace operations and EW encounter many operational risks. Commander and staff consider cascading effects because of employing cyberspace attacks and EA. The CEMA section ensures that the commander and staff understand the characteristics of the various cyberspace and EW capabilities and their associated effects. The CEMA section informs the commander and staff of the reversibility of effects resulting from cyberspace attacks and EA to understand that some effects are irreversible at the operator level. Attaining an understanding of the characteristics, cascading effects, and reversibility effects provide a commander with situational awareness and in determining the acceptable risks when conducting cyberspace operations and EW.

4-92. It is essential to consider risk management when conducting OCO and EA that could reveal friendly locations and intentions to an adversary prematurely. Some OCO or EA effects have a one-time use and once utilized cannot be effectively used again. OCO and EA may also create cascading effects that could hinder other operations.

4-93. Personal electronic device(s) such as smartwatches, smartphones, tablets, laptops, and gaming systems can be a significant OPSEC vulnerability to friendly cyberspace and EW capabilities. The CEWO gathers understanding surrounding risks associated with PEDs from the G2 or S2 and OPSEC and makes recommendations to the commander regarding their usage in the organization.

Technical Risks

4-94. Technical risks exist when there are exploitable vulnerabilities in systems on the DODIN-A, and there are threats that can exploit those vulnerabilities. Nearly every technical system within the Army is networked, resulting in a vulnerability in one system compromising other connected systems, creating a shared vulnerability. These potentially vulnerable networked systems and components directly impact the Army's ability to conduct operations. DCO mitigates risks by defending against specified cyberspace attacks, thereby denying the enemy's ability to take advantage of technical vulnerabilities that could disrupt operations.

4-95. Robust information systems engineering disciplines result in chain risk management, security, counterintelligence, intelligence, and hardware and software assurance that assist the leaders with managing technical risk. Friendly forces examine the technical risks when conducting cyberspace attacks to avoid making friendly networks vulnerable to enemy cyberspace counterattacks. The Army uses a layering approach, using these elements—

- Antivirus and anti-malware programs.
- Employing firewalls.
- Updating firmware and patches.
- Employing network intrusion detection and monitoring sensors.
- Implementing both cybersecurity and physical security measures to mitigate technical risks.

4-96. The elements listed in paragraph 4-95 are essential defensive enablers when implemented effectively and updated regularly.

Policy Risks

4-97. Policy risk pertains to authorities, legal guidance, and international law. Policies address cyberspace boundaries, authorities, and responsibilities. Commanders and decision makers must perform risk assessments and consider known probable cascading and collateral effects due to overlapping interests between military, civil, government, private, and corporate activities on shared networks in cyberspace. Policies, the United States Code (USC), the Uniform Code of Military Justice, regulations, publications, operation orders, and standard operating procedures all constitute a body of governance for making decisions about activities in cyberspace.

4-98. Policy risk includes considering international norms and practices, the effect of deviating from those norms, and potential shifts in international reputation because of the effects resulting from a cyberspace operation. Cyberspace attacks can be delivered through networks owned, operated, and geographically located within the sovereignty of multiple governments. EA can also deliver effects that impact frequencies in the

spectrum owned and operated by commercial, government, and other neutral users. Therefore, it is vital to consider the legal, cultural, and political costs associated with using cyberspace and the EMS as avenues of approach.

4-99. Policy risks occur where policy fails to address operational necessity. For example, a policy emplaced that limits cyberspace operations, which results in low levels of collateral effects, can result in a unit constrained to cyberspace attacks that will not result in the desired outcomes necessary for mission success. A collateral effects analysis to meet policy limits is distinct from the proportionality and necessity analysis required by the law of war. Even if a proposed cyberspace operation is permissible after a collateral effect's analysis, the proposed cyberspace operation or EW mission must include a legitimate military objective that is also permissible under the law of war.

4-100. Policy risk applies to risk management under civil or legal considerations. An OCO or EA mission may pose a risk to host nation civilians and non-combatants in an OE where a standing objective is to minimize collateral damage. During a mission, it may be in the Army's best interest for host nation populations to be able to perform day-to-day activities. Interruptions of public networks may present hazards to the DODIN-A and pose dangers to Army forces because of social impacts that lead to riots, criminal activity, and the emergence of insurgent opportunists seeking to exploit civil unrest.

Operations Security Risks

4-101. Both cyberspace and the EMS provides a venue for OPSEC risks. The Army depends on cyberspace security programs and training to prevent or mitigate OPSEC risks. Commanders emphasize and establish OPSEC programs to minimize the risks. OPSEC measures include actions and information on the DODIN and non-DODIN information systems and networks. All personnel are responsible for protecting sensitive and critical information. EP denies unauthorized access to information that an enemy intercept in the EMS through electromagnetic security operations. For more information on OPSEC, refer to AR 530-1 and ATP 3-13.3.

KNOWLEDGE MANAGEMENT

4-102. *Knowledge management* is the process of enabling knowledge flow to enhance shared understanding, learning, and decision making (ADP 6-0). The four components of knowledge management are people, processes, tools, and organizations. Knowledge management facilitates the transfer of knowledge among the commander, staff, and forces to build and maintain situational awareness and enhance organizational performance. Through knowledge management, information gets to the right personnel at the right time to facilitate decision making.

4-103. During knowledge management, the necessary cyberspace operations and EW-related information and tools from higher headquarters are provided to the CEMA working group in a timely enough manner to make decisions during mission analysis and COA development. Through the knowledge management process, cyberspace operations and EW-related intelligence received through information collection and IO is disseminated for decision making by the CEMA working group. The knowledge management steps are—

- Assess.
- Design.
- Develop.
- Pilot.
- Implement.

4-104. The CEWO is responsible for establishing and overseeing the flow of all cyberspace operations and EW-related information throughout the headquarters staff, including higher and lower echelons. The CEWO is accountable for providing IRs to the G-2 or S-2 to attain essential information needed to understand cyberspace and the EMS within an OE. Information acquired from IRs is also crucial to the CEMA section's ability to appropriately integrate and synchronize cyberspace operations and EW with the operations process.

4-105. The CEMA section and collaborating staff provide meaning to operations by sharing both tacit and explicit knowledge. *Tacit knowledge* is what individuals know; a unique, personal store of knowledge gained from life experiences, training, and networks of friends, acquaintances, and professional colleagues (ATP 6-01.1). All members of the CEMA working group provide knowledge attained from years of operational and