
ARMY CYBER INSTITUTE

WEST POINT, NY

# Distinguishing Electromagnetic Attack from Offensive Cyberspace Actions –
## Assessment, Recommendations, and Framework

**Date:** 20 December 2024 (Revised 27 June 2025)

**Analysis by:** ACI Cyber Operations - Research & Engineering Team (LTC Karl Olson, LTC Joe Catudal, MAJ JC Fernandes, MAJ Dan Burrow, MAJ Ben Allison, CW4 James Turner, CW3 Blane Richoux, Prof. Scott Sullivan)

**Approved by:** COL Todd Arnold

**For Feedback and Comments:**
karl.olson@westpoint.edu

This document was updated from a previous version to consistently align terminology with the Army's adoption of electromagnetic in the context of electromagnetic warfare. Additionally, risk analysis is shifted to contrast "geographically constrained" vs. "logically constrained" rather than "EA" vs. "OCO" categorizations. Other minor edits are further incorporated.

# Table of Contents

# Executive Summary

**Problem:** The Cyber Center of Excellence (CCoE) asked the Army Cyber Institute (ACI) to analyze terminology and metrics used to differentiate electromagnetic attack (EA) and offensive cyberspace operations (OCO) to determine if refining the existing lexicon or adopting an alternate conceptual framework would achieve better clarity.

**Background:** An inherent overlap exists between the cyberspace domain, the electromagnetic spectrum (EMS), and devices which use the EMS. Current terminology usage is often insufficient or misused to characterize certain actions as OCO, EA, or something else. Specifically, the use of terms such as “advanced EA,” “special purpose EA,” and “EA-enabled OCO” attempt to address the overlap but often create ambiguity. This ambiguity presents challenges. First, the military distinguishes cyberspace operations (CO) from electromagnetic warfare (EW), and the resulting characterization of an action can dictate funding, responsibility, and authority. Second, insufficient or poorly used terminology limits the range of actions that can be effectively described and conceptualized. Ultimately, this study seeks to ensure that commanders at echelon can employ EW and cyberspace capabilities to their fullest. It does not seek to redefine the definitions of EA or OCO.

**Approach:** We engaged with the community of practice to understand how operations are being conducted, the potential actions that might be involved, the use of terminology, and the overall context within the operating force. We combined this with reviews of applicable laws, doctrine, and related efforts to inform our analysis and develop recommendations.

**Proposal:** The overlap of cyberspace and the EMS makes a clear separation of EA from OCO infeasible and potentially limiting. Instead, we separate the underlying authorities question from the terminology considerations and propose 1) a layered model to help describe emissions in the EMS to offer deeper understanding and nuance for describing EW actions, and 2) a framework to help commanders and their staffs to better understand EA and OCO actions and their associated risks to aid their decision-making processes.

1. **Layers for describing EMS Transmissions**
   - **Message:** Content, data, or meaning.
   - **Protocol:** Communication rules.
   - **Waveforms:** Modulation (frequency, phase, amplitude) and timing (burst, continuous).
   - **Power:** Strength or intensity of transmission.

2. **Framework for Analyzing EA and OCO Actions**
   - **Delivery:** How the principal effect is delivered to the target.
   - **Depth:** How far the principal effects propagate.
   - **Determinism:** The degree to which the effects are determined prior to launching and to which the effects do not require additional interaction.

These proposals reduce ambiguity by offering means to understand and describe EA and OCO. They should not be interpreted as constraining commanders or narrowing the existing definitions of EA or OCO.

**Justification and Supporting Findings:**
Organized as: **Observation -** Discussion **-** *Significance*

1. **Unless otherwise restricted, commanders at echelon have a broad set of opportunities relating to EW and cyberspace.** These opportunities exceed present narrow views of OCO or EA and will continue to grow. They include electromagnetic attacks that are based on communication protocols or messages rather than purely power or waveforms; and cyberspace actions that rely on close physical proximity, established techniques, or commodity capabilities. *Efforts to address the ambiguity between OCO and EA should enable rather than limit these opportunities.*

2. **Existing doctrine inadequately describes the range of possible actions**. Cyberspace and the electromagnetic spectrum span domains and services. However, terms and concepts are inconsistent and contradictory across the Department of Defense and lack sufficient descriptive ability for the diversity of opportunities on the modern battlefield. *Clarity is needed.*

3. **Establishing a discrete delineation between EA and OCO is impractical.** The formal definitions of EA and OCO are broad and overlap. This provides flexibility to exploit opportunities, especially future opportunities, within the underlying overlap of cyberspace and the EMS. A variety of factors govern whether a commander can execute a specific action in a specific context. *Efforts to precisely bound this space will not directly impact the authority question and may overly restrict a commander's flexibility.*

4. **Comparing OCO to EA is an inherently asymmetric comparison.** Operations, to include OCO, are "a sequence of tactical actions with a common purpose or unifying theme." (JP 1-0) EA, as a form of fires, is a tactical action. It may be part of a cyberspace operation or operation conducted in another domain. Alternatively, cyberspace actions or operations may set conditions for an EA. *OCO and EA must be compared at the levels of action. In many instances, the appropriate comparison is between cyberspace attack and EA.*

5. **The fundamental nature of cyberspace creates a different risk profile.** EW activities are typically limited by power or line of sight to a specific geographic area, while in cyberspace the limiting constraint is often the logical layer. These differences in geographic risk and bounds underly the distinct restrictions on cyber operations and the need to classify actions as either EA or OCO. *Understanding cyber or EW actions requires understanding this risk.*

6. **The complexity and speed of future conflicts require an adaptable approach to managing the risk of cyberspace and EW actions.** The opportunities present in the EMS and cyberspace will continue to change and grow and the capability-countermeasure cycle will occur down to the lowest echelon. AI, open-source tools, 3D printing, automation in the targeting process, and other developments will only increase these trends. To compete in such an environment, the Army and Joint Force need an approach that supports understanding and scoping risk so that decisions can be made at the appropriate time and echelon. *The proposed framework provides granularity and adaptability missing from a rigid delineation between EA and OCO.*

# Distinguishing Electromagnetic Attack from Offensive Cyber Actions

## I. Introduction

### Background

A fundamental coupling exists between the electromagnetic environment and the cyberspace domain. The electromagnetic spectrum (EMS) is a maneuver space (JP 3-85) which can be used to conduct operations.. Communication, control, and sensing capabilities routinely rely on electromagnetic transmission and/or emission to function. Electromagnetic spectrum operations (EMSO) are the coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment (JP 3-85). Cyberspace is defined as a global domain within the information environment, consisting of interconnected networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors (JP 3-12).

The EMS routinely serves as the physical layer for transmissions in the cyberspace domain. Even when wireless communications are not used, an overlap in this space persists. Wired communications modulate electrical and/or optical signals in shared protocols to send and receive data, and the physical infrastructure underpinning the cyberspace domain emits incidental EMS signatures, which can similarly be exploited by EW capabilities[1].

This coupling is especially apparent in the context of military operations, specifically between electromagnetic attack (EA) and offensive cyber operations (OCO). EA involves the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-85). Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains (JP 3-12). While OCO affects digital systems connected logically and EA affects entities adjacent to the EMS, they both include second and third order effects which may cascade outside the domain or environment.

### Problem

Use of the EMS increasingly involves digital systems. These systems interact with other systems and become more pervasive in daily life. As the overlap between EA and OCO grows, and their distinct qualities become less clear. A lack of clarity in this evolving space negatively impacts commanders' decision-making processes and their ability to create shared understanding. Ambiguous language in doctrine increases the difficulty of conceptualizing available effects, limiting their development, training, and application within military operations. Additionally, it degrades the ability to communicate

[1] Note: For this document, we conform to the convention of using EMS when referring to electromagnetic signals not confined to an artificial transmission line. Where applicable, we are explicit regarding transmissions through wired mediums such as fiber, coaxial cable, CAT 5/6, etc.

and coordinate effectively within and across services–a key requirement for actions that can cross physical boundaries to span the domains of air, land, sea, and space.

Previous Army efforts attempted to distinguish between OCO and EA through metrics, such as code execution or target hop count, and terms, such as *Special Purpose EA* (SPEA)[2] or *RF-enabled cyber*.[3] However, these prior efforts required increasingly nuanced metrics and terminology to address the various edge-case scenarios. Instead of adding clarity, attempts to definitively characterize every action as either EA or OCO have compounded complexity.

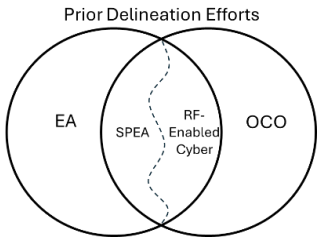


*Figure 1: Previous attempts to delineate EA from OCO*

## Approach

The inherent overlap between the EMS and cyberspace makes defining a clear delineation between EA and OCO infeasible. The total set of possible actions is large and continues to change as technology and operations evolve. Additionally, the factors governing the employment of certain actions—to include operational context, rules of engagement, constraints on the use of a capability, and acceptable risk—can be nuanced and vary from one instance to the next. Instead, we propose clarifying the problem space by providing tools to enhance understanding. Specifically, we propose a model for describing the EMS transmissions composing those actions (Section II), a framework to analyze actions (Section III), and other individual recommendations related to the problem (Section IV). These are flexible tools that can be used to analyze and describe EA and cyberspace actions as part of existing staff processes, thereby simplifying the problem posed by the overlap.

The need to distinguish between offensive cyberspace operations and electromagnetic attack is grounded largely in risk. While the differences between the EMS and cyberspace result in differences in materiel, personnel, and training, they also result in different risk implications. These risk considerations drive differences in authorities. Prominent to these distinctions in risk are the ability to bound the risk geographically, the requirements for secrecy for both operations and capabilities, the risk of escalation, and the overall uncertainty. Commanders and their staffs can use the framework to better understand cyberspace or EW actions in this broader context and regarding risk. (See Appendix A for additional discussion)

Refined terminology does not change the underlying legal and risk considerations, nor does it sufficiently describe the overlap between CO and EW. However, our analysis of existing doctrine and use of terminology across the community suggests that current doctrine is unclear. Terms are often used inconsistently, and the existing taxonomy is not adequate to clearly communicate the nuances of electromagnetic activities, specifically those relating to EA. In Section II, we propose a model based on abstraction layers to enhance our ability to describe electromagnetic transmissions and thus EA. (See Appendix D for an analysis of cases where existing terminology is insufficient, and Appendix E for our doctrine analysis).

Our findings are based on our analysis of the desired end state (enabling effective operations by clarifying ambiguity) and comparing it to the current state. We initially focused on understanding the current state of authorities, terminology, and operations both within the Army and across the other

[2] We argue for the discontinued use of SPEA in Section II.

[3] Related efforts include the Army's Starblazor Report and 120 Day Study. See Appendix C for a discussion of previous works.

services. We applied this understanding to a growing set of operational examples and used this to refine both the analysis framework and the descriptive model.

**Problem**

The distinction between OCO and EA is unclear which creates challenges relating to authorities and responsibilities, along with limiting the commander's ability to visualize and describe actions.

**Foundational Premises**

- Tools, techniques, and systems that leverage or apply effects within the EMS and cyberspace will continue to evolve. Any solution must support future applications.
- The decision to conduct an EA or cyber attack is primarily a matter of authorities and risk. Terminology and doctrine will not change underlying legal and operational considerations.
- Commanders should have maximum latitude to operate and deploy effects within their AO consistent with legal and ethical standards.

**Research Questions**

- What is the current laws, policy, doctrine, and usage of terms? (Appendix B, E)
- What are examples of actions that fall within and outside the overlap? (Appendix A, D)
- What areas of EA and OCO are separable and what is the complexity or remaining overlap? (Section III)
- What criteria can we use to distinguish between the two while minimizing complexity? (Section III)
- What other considerations have bearing on this problem now and in the future? (Section II, Section IV)

**Proposals**

| Analysis Framework | |
|---|---|
| **Delivery:** How the effect is delivered to the target system. |  |
| **Depth:** How far the effects propagate beyond the initial target. |  |
| **Determinism:** Degree to which the effects are determined prior to launching and without additional interaction. |  |

| Layers of EMS Transmissions | |
|---|---|
| Message | Content, data, or meaning |
| Protocol | Communication rules |
| Waveform | Energy modulation and duration |
| Power | Strength or intensity of transmission |

*Figure 2: Research Summary Graphic*

# II. Layered Model for Describing Transmissions

The modern battlefield abounds with possibilities to exploit the EMS for advantage, and the applications continue to evolve with technology and human ingenuity. Developing a layered model provides a common foundation for describing these actions now and in the future. Abstraction layers are commonly used in communications and technology. They allow practitioners to focus on the salient facets of a given situation. When discussing computer networking, the layers of the OSI and TCP/IP models are commonly used. These models are sometimes referred to as protocol stacks or network stacks. We propose a similar model to describe EMS transmissions using transmission power, waveforms, communication protocols, and signal meaning or content as the starting point to help establish common terminology and understanding by which to describe methods, actions, and effects surrounding electromagnetic warfare.[4]

| | Layers of EMS Transmissions | |
|---|---|---|
| Interpreted (defined by humans) | Message | Content, data, or meaning |
| | Protocol | Communication rules |
| Physical (defined by physics) | Waveform | Energy modulation and duration |
| | Power | Strength or intensity of transmission |

*Figure 3: Layer Model of EMS Transmissions*

- **Messages** are the information or meaning communicated by a transmission. They may be conveyed as a simple signal or more complexly encoded using physical characteristics of the transmission. Message-based attacks cause an effect by manipulating the information being communicated to higher-level systems and ultimately the user. They may include sending transmissions with false verbal orders or fake telemetry data for the purpose of deceiving the enemy or manipulating their behavior.
- **Protocols** are the rules through which information exchange occurs. Protocol-based attacks exploit these protocols to have an effect and may include attacks such as 802.11 de-authentication.
- **Waveforms** are the characteristics of the energy emission through which data may be encoded. They are described by properties that include frequency, phase, and amplitude modulation along with bandwidth and duration (burst vs continuous). Waveform-based attacks manipulate the modulation and other aspects of the waveform to have effects.[5]
- **Power** is the strength or intensity of electromagnetic transmission. In EA, it is a measure of the energy being directed. Power-based attacks often focus on delivering overwhelming power to interfere with the ability of a signal to receive a signal. They also include EMPs, lasers, sonic disruptions, and other effects based primarily on the transmission of energy.

**Note**: Common usage of SPEA primarily falls in the protocol layer of this model with some overlap on the message layer. Conversely, in "RF-enabled cyber" the lower layers generally provide transport for message-based effects.

[4] These layers are meant to describe transmissions in general. While we apply them to describe EA, they may also be used for other purposes such as describing signals collection.

[5] The proximity of the frequency and power levels relative to other users in the EMS affects a commander's risk assessment for fratricide or collateral damage.

## Model Considerations

Like similar models, higher layers in the "stack" build upon lower layers, and some actions might not fit neatly into one layer or might be a combination of layers. The purpose of this model is not to add complexity by necessitating strict characterization of attacks, but rather to simplify communication by providing a shared conceptual model as a starting point. We fully expect this model to yield statements such as, "it is primarily a power-based attack that exploits the protocol timing for maximum effect," which can serve to support risk analysis and quickly measure which category of authorities may best be applied.

While SPEA and RF-enabled OCO provide similar utility, we prefer this proposed model because it is based on the characteristics of the transmission. It provides descriptions that are independent of changing authorities or conceptions of EA and OCO. Additionally, the term ***Special Purpose*** in *Special Purpose Electromagnetic Attack* was perceived as distinguishing SPEA from EA rather than being a type of EA. Rather than enhancing understanding, this perceived distinction created additional confusion.

# III. Analysis Framework for EA and OCO Actions

The goal of this framework is to help commanders and their staff better understand cyberspace or EW actions. They may use its concepts of **delivery**, **depth**, and **determinism** to analyze the action from

> **Note:** Comparing OCO to EA is an inherently asymmetric comparison**.** EA is a tactical action, an attack. Operations, to include OCO, are "a sequence of tactical actions with a common purpose or unifying theme." (JP 1-0) EA may be an action within a cyberspace operation and cyberspace actions or operations may set conditions for an EA.

"launching" by friendly forces through the effects on the initial targets and beyond. In some cases, actions may be clearly EA or clearly a cyberspace attack. In other instances, characterization is less clear. Regardless of the characterization, the analysis process identifies the sequence and systems involved in an action, the possible effects, and the risk. From a targeting perspective, it helps to understand weaponeering and refine collateral damage estimates.

## Delivery

The commander and staff consider ***how the effect is delivered to the targeted system***. The focus is determining what, if any, third party systems the action may transit from the last friendly system[6] to the initial[7] target. The simplest case is an effect delivered without any intermediate systems. For instance, an operator might fire a bullet at a target, emit high power at a certain frequency, or have direct physical access to an adversary computer system. Alternatively, the effect may involve the use of third-party network infrastructure, RF infrastructure, or other related infrastructure. By analyzing delivery, units can understand the unintended effects or collateral damage to both intermediate systems and receiving systems that are not the intended target.

---

[6] Note: The last friendly system, or firing system, is the last friendly system through which an action traverses before eventually impacting an adversary system. There may be one or more of these systems (for instance multiple jammers or a device jamming one signal while another device transmits a false signal). When assessing the action, units generally ignore systems prior to these final friendly system(s). Independent of this framework, units consider factors such as classification, wartime reserves, and constraints on specific tools.

[7] Note: For delivery, the focus is on the adversary systems receiving the action or effect prior to any other systems of the adversary. This may be one or more systems. The propagation of effects from these initial targets falls under the concept of "depth."

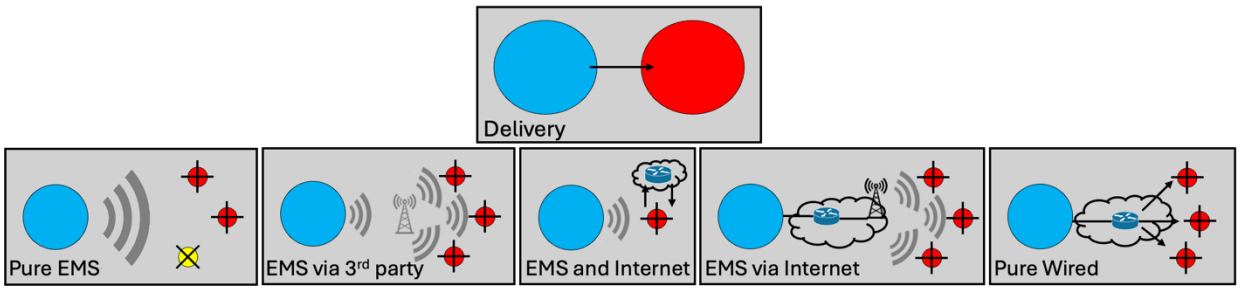



*Figure 3: Delivery of an effect from the last friendly system to the initial target may purely use the EMS (bottom left), may not use the EMS at all (bottom right), or by other methods.*

Generally, an action that is purely electromagnetic attack will use wireless transmission and will not traverse third-party computer networks to reach the target while a pure cyberspace attack may transit the internet or other third-party infrastructure, to include external connections from the target. An attack whose delivery does not involve electromagnetic energy cannot be EA.[8]

## Depth

Effects can propagate deliberately or inadvertently from one system to another. Analyzing ***how far the effect propagates,*** beyond the initial target[9] or the boundary of the adversary system, helps commanders understand the potential scope of the effects and bound risk both conceptually and geographically. For example, destroying enemy tanks by targeting an adjacent ammunition pile has greater depth than engaging the tanks directly. However, with both attack methods, the destruction of the tank may have the same second-order effects on the larger enemy system – the tank may have contained the enemy commander or been a support by fire position that was critical to the enemy's maneuver plan. Within cyberspace or the EMS, an attack that causes a targeted system to propagate a self-destruct message to other systems would have greater depth than an attack targeting those other systems directly.

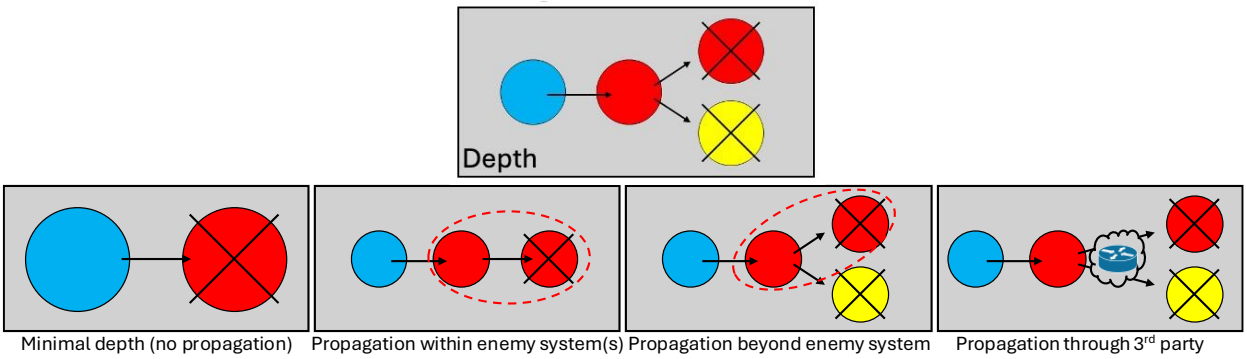



*Figure 4: Depth increase as the effect propagates beyond the initial target or boundary of the adversary system.*

Generally, there is greater uncertainty and risk of collateral damage as effects propagate. The primary concern associated with depth is when the effect leaves the adversary's broader system and impacts

[8] Anti-radiation missiles and chaff are defined to be EA and may be exceptions to this general rule.
[9] An attack may target a system of systems and therefore the effects may involve a sequence of systems. For our purposes, the initial target is the first such system.

third-party systems. Traditionally, EA is used to affect a receiving system or an adjacent component within a larger system. Thus, the depth of EA tends to be low. In contrast, computer communications and applications often rely upon external infrastructure—even for internal functions. Consequently, cyberspace actions often traverse various nodes before delivering effects, and these effects can have significance and unintuitive depth. Increased depth makes it harder to localize effects geographically and increases the risk of effects on third-party systems and outside the intended area of operations or theater.

## Determinism

For a potential action, units assess ***the degree to which the effect is determined prior to launching and without additional interaction***. Understanding determinism requires understanding the payload being delivered. The unit must analyze the range of possible effects, the range of systems that may be affected, the interaction required by the user, and the associated probabilities of each. Determinism increases as the possible outcomes decrease, and confidence in those outcomes increases. When considering collateral damage and accidental risk, it is often sufficient to identify the upper bound—the systems that may be affected and the maximum possible effect. However, the commander must often weigh that against the probability of achieving at least the minimum required effect on the desired target(s). The more deterministic the outcome, the more accurate the assessments of collateral damage, operational effectiveness, and overall risk.

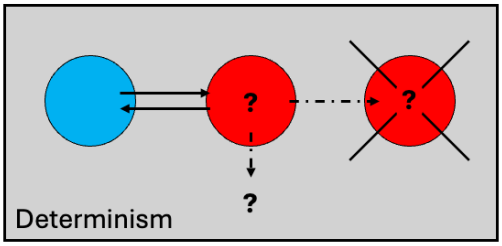



*Figure 6: Determinism describes the degree to which the effect is determined prior to launching and without additional interaction.*

The effects of indirect fire are relatively deterministic. They can be estimated based on the terrain, weather, ballistics, blast radius and similar factors, and they can be tailored through round and fuse combinations. While defective rounds occur, high explosive rounds cannot cause nuclear or chemical fallout except when hitting specific chemical or nuclear materials. Additionally, most munitions cannot be redirected after firing.

EA, such as jamming, tends to be similarly deterministic with the effects reasonably estimated based on power, distance, and frequency. However, more sophisticated attacks may involve increased interaction and thus be less deterministic. Additionally, EA may rely on non-deterministic preparatory work conducted in cyberspace during an earlier phase of the current operation or as part of an earlier operation. The attack or payload may be based on computer logic, but the outcome is deterministic and relies on minimal user interaction beyond preparatory configuration or setup.

Actions that comprise Offensive Cyberspace Operations are, more often, non-deterministic. They require decision making—often regarding how to maneuver or “pivot” through cyberspace—which

increases the range of possible outcomes.[10] Even when an attack is staged, incomplete or uncertain understanding of the target systems and networks can reduce determinism which may also have implications for depth.

## Application Considerations

This framework does not definitively characterize all actions as EA or OCO. Rather, it is a lens through which a commander can view an action to inform assessments of legal authority, collateral damage, and operational necessity. The commander may decide to avoid the action, initiate the action, collect more information, modify the planned action, or elevate the decision to a higher commander. Moreover, this approach recognizes that some subset of actions can be either EA or cyber, and the authority for either may apply. In analyzing these concepts, we note the distinction between operations and actions. Many actions can be combined in sequence or simultaneously as part of an operation and to achieve converging effects. To apply this framework, commanders start with an action intended to have an effect. For more complex scenarios, they can analyze the component actions.

This framework focuses on the elements of risk that are distinctive when comparing actions in the physical domains to the cyberspace domain. Using the framework provides greater understanding for other existing processes and concepts, such as rules of engagement, wartime reserves, classification levels, or target discrimination. In both contexts, there remains room for human error in both assessment and execution.

This framework used the concept of “systems.” Systems are nesting and hierarchical. The appropriate level of granularity will vary by context. For instance, the theater army may consider the “integrated air defense system” a singular system while an EW team might target a specific receiver used by one of the anti-aircraft weapon systems within the larger IAD system. Appendix A provides examples of applying this framework to operational problems.

While the purpose of the framework is not to establish a firm differentiation between EA and OCO, applying the analysis process can reveal if one of the differentiating features is present, if an attack falls within both EA and OCO, or when such characterization is ambiguous.

[10] Note: Under this framework, the opportunity or requirement for user interaction generally reduces determinism when the action is initiated. While certain user interactions, such as abort mechanisms, may increase determinism, decision making generally increases the possible outcomes and decreases determinism. In some cases, the actions relating to a decision point can be evaluated independently.

## Electromagnetic Attack

Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called EA. (JP3-85)

## Offensive Cyberspace Operations

Missions intended to project power in and through cyberspace. Also called OCO. (JP 3-12)

## Analysis Process

For a proposed attack, analyze the delivery, depth, and determinism.

### Delivery

| | |
|---|---|
| How is the effect delivered to the target?<br>Is the effect delivered wirelessly?<br>Does delivery transit third-party systems?<br>Which transmission layers are involved? | EA must include directed energy in delivery. Delivery through the internet or 3rd-party computing networks is normally not EA. Power and waveform attacks are generally EA. Protocol-based attacks are often EA. Message-based attacks may be EA but often need more analysis. |


### Depth

| | |
|---|---|
| Is the effect limited to the initial target?<br>Is "pivoting" required?<br>How far does the effect propagate?<br>Will the effects extend to 3rd-party systems? | EA effects may propagate, but attacks that require pivoting across networked nodes to reach the target are typically not EA. |


### Determinism

| | |
|---|---|
| Is it fire and forget?<br>What are the possible outcomes?<br>How certain are those outcomes?<br>Is any interaction required after launching? | EA are typically "fire and forget." Attacks that require interaction, learning about the target, or modification of the attack method after launching are generally not EA. |

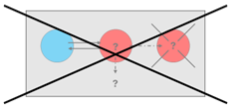


*Figure 7: Framework overview for understanding effects and relationships with EA or OCO.*

**Output**

Understanding of the functioning, sequence, and elements of the attack to inform collateral damage estimates, risk assessment, and analysis of authorities.

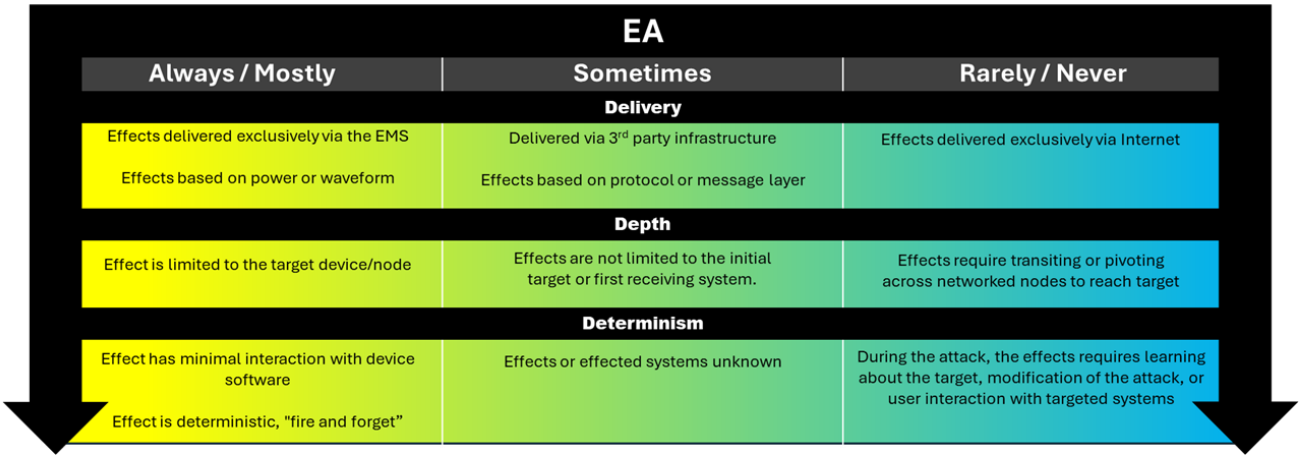



*Figure 8: Output of applying the framework helps to understand an effects relation as EA.*

# IV. Recommendations & Future Work

## Recommendations

In addition to the two primary proposals, our research yielded several additional observations and recommendations. We present our salient recommendations here, leaving smaller points, observations, further discussion, and rationale to the supporting appendices.

1. Preserve the broad definitions of EA and Cyberspace Operations and the resultant overlap.
   **Discussion:** Changing doctrine does not directly impact the legal authorities or the risks. Attempts to create a clear separation will unnecessarily increase complexity and constrain commanders and their staff. Broad definitions preserve the space for future experimentation and capabilities.

2. Review and validate the proposed framework as an analysis tool for EA and OCO actions. Update doctrine as appropriate.
   **Discussion:** As discussed throughout the paper, such a framework enables the analysis necessary to understand the actions and answer questions regarding authorities.

3. Promulgate the proposed layered model, or similar, to assist in describing EA and other EMS transmissions. Update doctrine as appropriate.
   **Discussion:** The desire to define SPEA highlights a shortfall of existing terminology. The proposal addresses this shortfall in a manner that is descriptive and not constraining.

4. Take a broad approach to the development of techniques and software solutions for electromagnetic attack.
   **Discussion:** Strategic and operational context shape the authorized actions. There are increasing opportunities in the overlap area, and the consensus is that commanders will have greater authorities as the intensity of operations increase to LSCO. The development of materiel solutions

must account for the possibility of more liberal authorities, and the likely opportunities present within each.

5. Be judicious when defining new terms.
   **Discussion:** Poor terminology can increase complexity and reduce clarity. Our assessment is that existing doctrine is unclear with terms being used incorrectly.
   A. When possible, avoid defining new terms. Instead, describe concepts using the simplest terminology based on common meaning.
      **Discussion:** This reduces jargon, ensures terminology keeps pace with technology changes, and fosters communication that is descriptive rather than rigid.
   B. When a new formally defined term is required, ensure consistency with Joint doctrine.
      **Discussion:** EW and cyberspace operations spans services, and EW and cyber professionals will likely communicate across service boundaries. There will continue to be service-specific terms, but they should not contradict or redefine joint terminology.

## Areas for Future Work

1. Use the proposals to inform organizational decisions (DOTMLPF-P) that enable rapid development of EW and cyberspace materiel solutions at echelon.
   **Discussion:** The modern battlefield requires the ability to rapidly develop hardware and software solutions to exploit opportunities and counter enemy capabilities. For instance, the Army may decide that corps require the capability to generate attacks focused on certain layers of our layered model (e.g. message or protocol) and the division could focus on lower or less sophisticated ones. Similarly, the risk framework may inform policies or ROE.

2. Mature functional integration of EW and SIGINT
   **Discussion:** Similar to the issue between OCO and EW, there is an overlap between signals intelligence (SIGINT) and electromagnetic sensing (ES). The policies and procedures designed to protect the value of SIGINT and SIGINT capabilities limit the tactical and operational flexibility to sense and act on signals in the EMS. The integration of these capabilities will ensure optimized and flexible employment and may help craft electromagnetic attacks based on observed signals.

3. Enable broader cyberspace actions at echelon.
   **Discussion:** Cyberspace presents opportunities beyond traditional OCO for units at every echelon. However, doctrine and policy do not effectively illustrate these opportunities nor are these potential capabilities addressed through the other components of DOTMLPF-P. Commanders should have a broad understanding of the opportunities present at their echelon and the Army should broadly allow for and enable these opportunities, commensurate to the delegation and acceptance of risk.

4. Explore operational control measures relating to EW and Cyberspace.
   **Discussion:** Control measures, such as those for fire control, are effective tools for commanders. They assist commanders and their staff to communicate and understand what action is permitted and prohibited. They are predominantly graphical and tied to terrain. However, there are limit control measures (graphical or otherwise) that pertain to cyberspace operations and EW. An example might be a graphic to represent the effect area and frequency for jamming.

# V. Conclusion

A primary challenge of this effort was the desire to establish clear boundaries between EA and OCO while not constraining commanders. Although we would like to cleanly separate EA from OCO, such a solution is unattainable and would not address the entirety of the problem. Instead, our approach decouples the authorities aspect from the terminology aspect and attempts to address each individually. First, the problem of authorities and responsibilities is a legal matter largely independent of internally defined terms. Rather than trying to characterize an action as SPEA, RF-enabled OCO, EA, or OCO, the analysis framework supports the legal analysis and determination. Second, a common vernacular and coherent taxonomy is necessary for communicating these actions. The proposed abstraction layers provide a conceptual model for describing transmissions. As a result, the overlap area is less opaque and somewhat reduced.

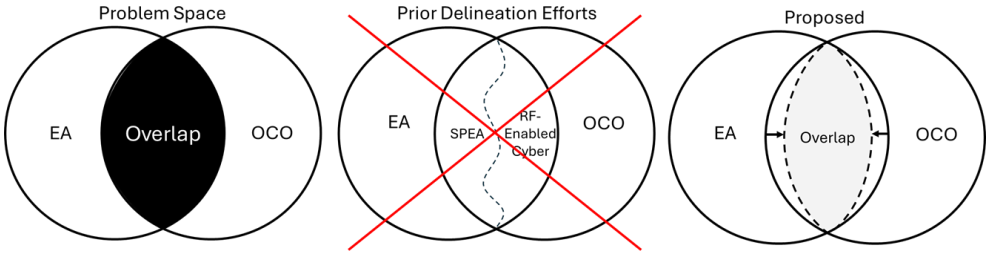



*Figure 9: The proposals reduce and clarify the overlap rather than attempting a strict delineation.*

The number of military applications falling within this overlap area will continue to grow. Attempts to distinguish them through rigorous terminology complicate the problem and risks constraining ourselves. Instead, the Army must be able to operate in the overlap area, for it is at the gaps and seams where opportunities are found. Our proposals enable exploiting opportunities by providing adaptable tools to understand and communicate with them.

# VI. Summary of Enclosures

Our appendices contain our supporting analysis and additional details or reviews. The below list summarizes the materials found within each appendix.

**Appendix A** presents the application of our proposed framework using demonstrative examples and known edge cases.

**Appendix B** presents an overview of salient legal points intended to generate discussion and considerations regarding EA. We further include a legal assessment framework to serve as a starting point for assessing the application of EA from a legal perspective. This is not intended to be an exhaustive legal review of every nuance.

**Appendix C** consolidates prior Army efforts (Starblazor Report and 120-day study) to differentiate EA from Cyber and provides additional comparison of the associated recommendations to our proposed framework.

**Appendix D** reviews the emerging environment and applications of EA and how present capabilities align or fail to align to current understanding and terminology found in doctrine.

**Appendix E** is our review of service and joint doctrine and terminology surrounding EA and cyberspace attack, which was used to guide our understanding of the problem space and alignment of recommendations.

**Appendix F** is a compilation of EW and cyber terms and definitions present within service and joint doctrine, consolidated as a singular reference.

# Appendix A – Framework Application and Boundary Examples

## I. Overview

This section provides additional information and examples on how to apply the concepts of delivery, depth, and determinism to analyze attacks. It begins by introducing general patterns that are found throughout a range of attacks. It then uses the framework to analyze a series of scenarios that illustrate the blurred space between EA and OCO. Finally, we present additional terms and concepts that may be useful in understanding and applying this framework.

Each scenario presents a vulnerable system, a capability which exploits that vulnerability to create an effect, and an analysis of delivery, depth and determinism associated with employing that capability. Based on this analysis, it assesses whether the risk profile is geographically bounded, as in traditional EA, or logically bounded, as is common in OCO. When applicable, additional discussion is provided.

The purpose of the examples is not to classify the action as EA or OCO, but rather to demonstrate the application of the framework to better understanding risk. Additionally, the assessment of the risk is not an assessment of severity but rather an evaluation of the nature of the risk. The risk associated with EA tends to be bounded geographically while risk from cyberspace operations may not be and may have other salient features (See “Additional Concepts” at the end of this appendix for a discussion of these features).

See Appendix D for examples of real-world capabilities and scenarios.

## II. General Cases

The diagrams below illustrate some of the common patterns observed in EA and OCO. Complex attacks are typically compositions of simpler patterns.

### Systems of Systems and Abstraction

Systems of systems proliferate on the modern battlefield. At the highest level of abstraction, the friendly forces launch attacks on the system that is the enemy. However, when analyzing more granularly, an attack may involve transmission from multiple friendly platforms and target multiple distinct enemy systems (Figure 8). The echelon, ambiguity of the attack, and other operational considerations dictate the balance between abstraction and granular detail.

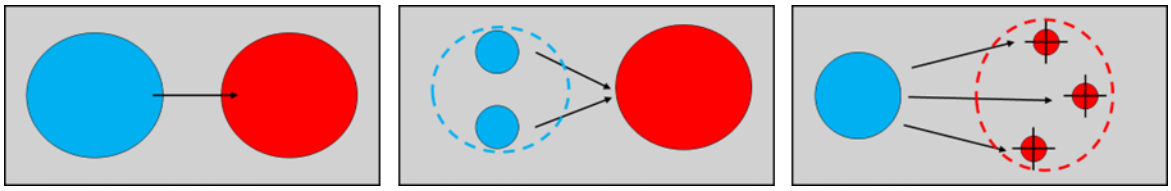


*Figure 1: The level of abstraction provides different perspectives to view the same attack.*

## Patterns of Delivery

The figures below highlight some of the common models for delivery effects by OCO or EA.

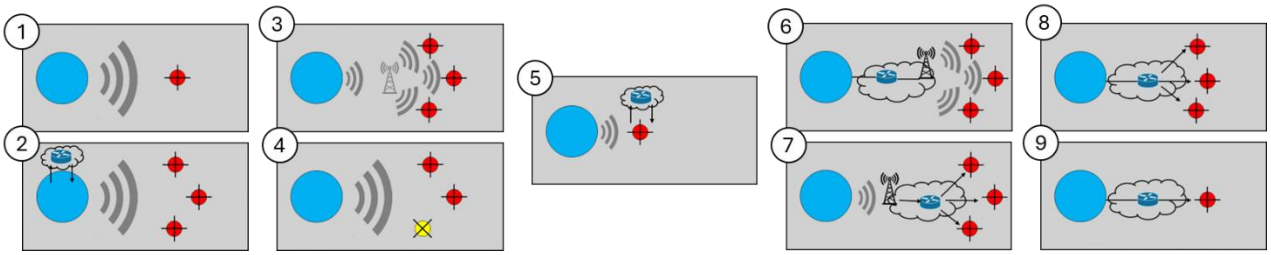



*Figure 2: Delivery Patterns*

The attacks in diagram 1 through 4 are delivered to targets exclusively though the EMS, these include attacks that might use external networks prior to the launching system(s) (2), retransmission by a third party (3) and potential for collateral damage to third-party receivers (4). If the attack is restricted to the transmission protocol and below, these attacks are generally considered EA despite data transiting. However, analysis of determinism and depth may reveal risk considerations that otherwise preclude the action.

In Figure 9, diagrams 6 through 9, the attacks transits computer networks during delivery, either in conjunction with directed energy / wireless transmissions (6 and 7) or independent of them (8 and 9).[11] These attacks are rarely geographically constrained.

Diagram 5 is perhaps the most ambiguous attack pattern. Under this pattern, the attack relies on the target's use of external network connections. Units must perform more analysis on actions that follow this pattern to understand the nature of external interaction. It could be that a special signal triggers an update process that makes the target unavailable, or it could involve the transmission causing the target to download a payload for subsequent effects.

## Depth and Patterns of Propagation

Propagation describes the ability for a capability to hop through multiple nodes of the target system. Attacks propagate (2-6) or do not (1). They may propagate through nodes without causing effects (2, 3, 6) or cause effects in subsequent nodes (4, 5). The attack may also propagate outside the enemy system as part of the propagation method (6) and causing collateral damage (3,5,6). Analyzing how the attack is delivered between nodes can help understand the risk. Determinism and depth are closely related because there is usually some uncertainty in the propagation.

[11] Even in these cases, portions of the network routing may be wireless, such as internet links provided by cellular or satellite transmission. However, in these patterns the attack is agnostic of the physical transmission medium.

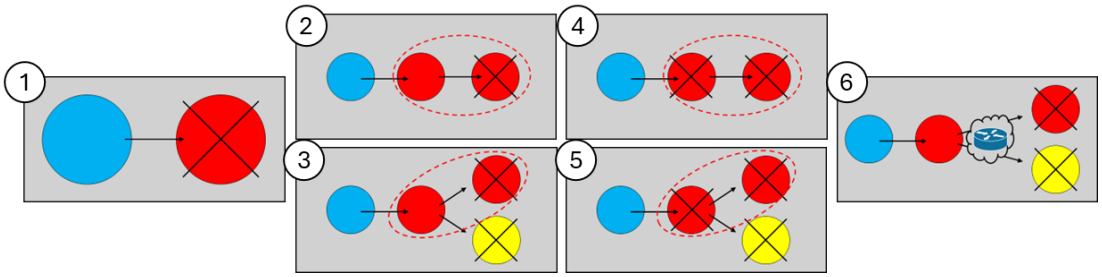



*Figure 5: Propagation Patterns*

## Combining Patterns

Applying the analysis framework involves analyzing both the delivery mechanisms and depth. As seen below, the overall behavior of the attack may be a combination of patterns presented. It may also vary based on the level of abstraction during the analysis.

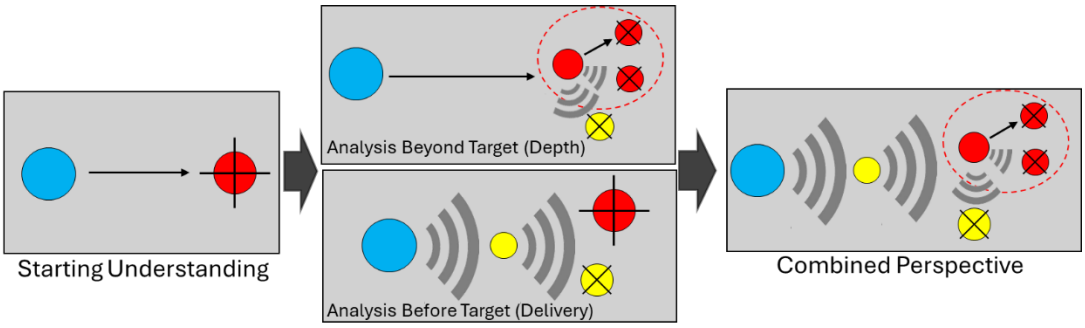



*Figure 6: Combining analysis of depth and delivery provide greater understanding of the attack.*

In the diagram above, both depth and delivery reveal the potential for a third-party system to be affected. Additionally, understanding the attack's propagation involves the concepts of both depth (how far) and delivery (what mechanism).

## Overlaying Determinism and Uncertainty

Each portion of an attack sequence can have uncertainty or require interaction. For instance, user interaction may be required to move beyond the first node and the propagation depth, propagation method, and eventual effects can all be uncertain. This potential for non-determinism is overlaid onto the analysis of delivery and depth (See Figure ).

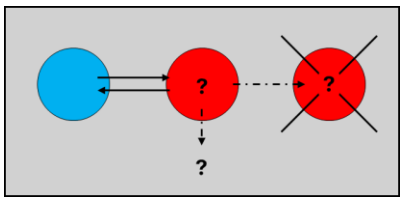



*Figure 5: Attack Uncertainty*

# III. Analysis Framework Examples

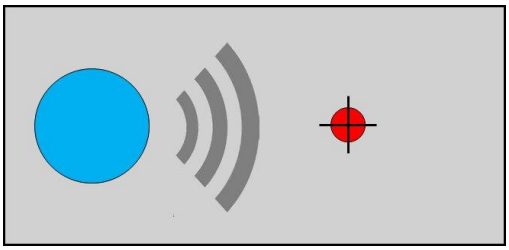


## 1a. The Vulnerable WiFi Quadcopter

**Vulnerability:** A quadcopter is controlled exclusively via line-of-sight 2.4GHz Wi-Fi. The quadcopter manufacturer left a diagnostic credential hard-coded in the firmware that can be leveraged to log into the quadcopter and force it to fall out of the sky.

**Capability:** A notional, portable, hand-held capability leverages the hardcoded credentials to connect to the quadcopter over 2.4GHz Wi-Fi, initiate a TCP session with the quadcopter, log in, and send a command to disable the quadcopter. No interaction from the operator is required beyond the launch of the capability. The capability is equipped with Wi-Fi and will succeed so long as it is within range of the quadcopter's Wi-Fi without requiring external dependencies.

**Delivery:** The capability is delivered from the transmitting device to the target device entirely over EMS.
**Depth:** The effect is limited to the initial target.
**Determinism:** The capability is push-button and will always behave in the same way




***Evaluation:*** *Risk profile is geographically bounded.*

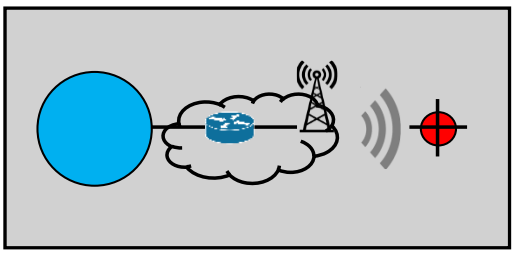
**Discussion:** Because the effect is delivered directly from the transmitting device to the target using a deterministic effect, this capability matches the risk profile of Electromagnetic Attack.

## 1b. The Vulnerable LTE Quadcopter

**Vulnerability:** A quadcopter has only an on-board LTE antenna and is controlled by its operator over the internet. The quadcopter manufacturer left a diagnostic credential hard-coded in the firmware that can be leveraged to log into the quadcopter and force it to fall out of the sky.

**Capability:** A packaged capability uses the internet (outside blue space) to connect to the quadcopter, initiate a TCP session, log in, and initiate a command to disable the quadcopter.

**Delivery:** While the delivery from the LTE network to the quadcopter is EMS-based, the capability requires transport over the internet after launch and is not delivered directly over EMS.



**Depth**: Effect is limited to the initial target.

**Determinism:** The capability is push-button and will always behave in the same way.


***Evaluation:*** *Risk profile is not geographically bounded.*

**Discussion:** The “delivery” evaluation flags that this capability uses the internet to deliver its effect and as such, the risk is not isolated to a physical geographic area. While the effect itself is geographically bounded, the delivery mechanism increases the overall risk. For example, it may implicate third-party internet services outside of the AOR, leading to response actions by the enemy against these third parties.

## 2a. Sensor Jamming

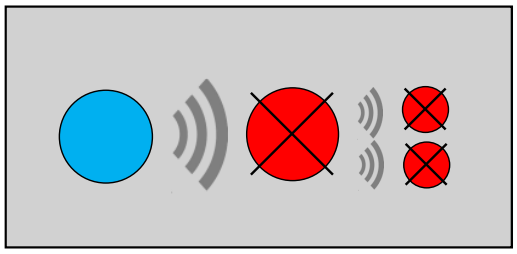
**Vulnerability:** A hypothetical Integrated Air Defense System has sensor endpoints that can be overwhelmed with RF energy, causing them to malfunction and become blind to enemy air activity.

**Capability:** A hypothetical capability can leverage RF spectrum to deliver a signal to the sensor and deny its ability to see enemy aircraft and thus report incorrect data. This data is ingested into the larger integrated system and prevents the system from correctly identifying hostile aircraft.

**Delivery:** Capability is a power-based effect that operates entirely over the EMS.

**Depth:** The effect does not cross into the logical layer. While the effect has second-order consequences that impact a larger system and other devices operating on the same frequency, this does not cause logical propagation.

**Determinism:** The capability is push-button and performs the same every time




***Evaluation:*** *Risk profile is geographically bounded.*

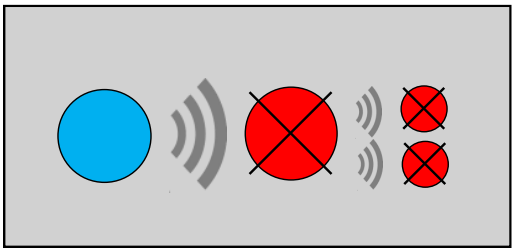
**Discussion:** The “depth” evaluation for this capability is somewhat nuanced. A useful thought experiment when evaluating depth is to replace the capability with a kinetic weapon. If destroying a sensor has a similar effect, then the risk for the action is likely geographically bounded.

## 2b. Sensor Exploitation

**Vulnerability:** A hypothetical Integrated Air Defense System's sensor endpoints possess a vulnerability such that a well-crafted signal can allow delivery of commands to an on-board processor.

**Capability:** A hypothetical capability uses the electromagnetic spectrum to deliver a signal to the sensor, exploit the vulnerability, and leverage this exploitation to cause the sensor to report incorrect data into a larger system. This, in turn, prevents the system from correctly identifying hostile aircraft. The capability is push-button and does not require further interaction from the capability operator nor depend on adjacent network devices to succeed.

**Delivery:** The capability is an exploitation-based effect that operates entirely over the EMS. Within the model described in this paper, the exploit operates at the message-layer.



**Depth:** The direct effect is limited to the initial target. While the effect has second-order consequences that impact a larger system, the effect from the capability and the risk associated with the capability are limited to the initial target. Also note that because this is not a message-layer-based attack, the impact to other devices using the same frequency is lower than a power-based attack.

**Determinism:** The capability is push-button and performs the same every time.


***Evaluation:*** *Risk profile is geographically bounded*

**Discussion:** It is important to distinguish between the capability and the vulnerability in this case. The vulnerability in this system may allow for actions that exceed those used in the capability. However, the capability itself is limited, so risk analysis must be limited to the capability.

## 2c. Propagating Payload

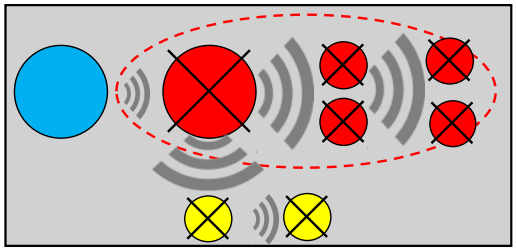
**Vulnerability:** The enemy is using a special hand-held radio system that has a vulnerability such that a well-crafted signal can enable command execution on the on-board computer for the radio.

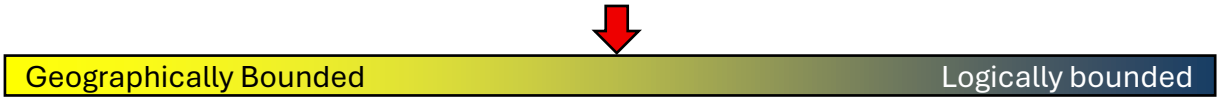
**Capability**: A hypothetical capability utilizes RF spectrum to exploit and infect enemy transceivers with a worm-like payload. The payload disables the operator's send and receive functions on the radio. Additionally, once the enemy device is infected, it utilizes that infected transceiver to deliver the same payload to other vulnerable devices within RF range.

**Delivery: T**he capability is delivered entirely within the EMS.

**Depth:** The direct effect is not limited to the target system but may propagate to third-party systems as well.

**Determinism:** The capability performs the same way against any vulnerable system; however, the number of affected nodes is unbounded by the capability.






**Evaluation:** *Risk profile is not bounded to the area of responsibility*

**Discussion:** Even though everything occurring in this scenario is occurring in the EMS and does not touch internet-connected devices, the risk of a propagating worm-like payload is very different from traditional EA. There is a very real risk that this could spread outside of the intended targets. Note here that the worm-like behavior is high risk in both OCO and EA.

## 3. Counter UAS Force Protection

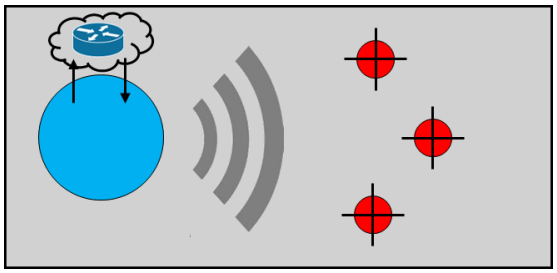
**Vulnerability:** A hypothetical integrated network of sensors supports a counter-UAS force protection system that uses server-based automation (AI) to identify and respond to emerging threats.

**Capability:** The system has the capacity to detect and neutralize unidentified UAS using spectrum-based EW capabilities that are both ground-based and mounted on autonomous UAS.

**Delivery:** Regardless of whether the platform is ground-based or mounted on a flying platform, the capability is delivered over EMS.

**Depth:** The effect is limited to the target UAS or other devices in range operating on the same frequency

**Determinism:** Capability performs the same every time. Whether or not a human is in the loop to push the button does not impact the evaluation of the capability as EA.




**Evaluation:** *Risk profile is geographically bounded.*

**Discussion:** Using autonomous systems or cloud-based classifiers to identify valid targets is a red-herring to discussion of whether a capability is EA. Whether or not a human is in the loop in the targeting process is not particularly relevant to whether a capability is EA. However, having a human in the loop is very relevant when determining the overall risk of a capability. In this case, one should define the bounds of the automated system within acceptable risk.

## 4. Counter UAS Swarm via Pivot

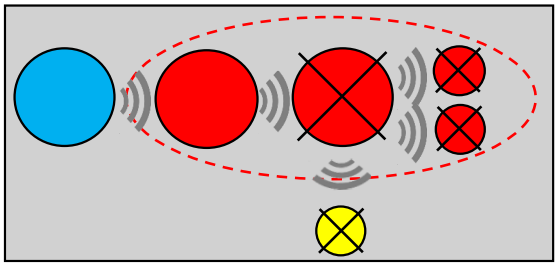
**Vulnerability:** A hypothetical swarm of enemy UAVs operate in a mesh network with implicit trust between nodes. If one of the nodes is compromised, it is feasible to leverage that trust to pivot from one node to take control of the entire swarm.

**Capability:** A hypothetical capability against a swarm of quadcopter UAVs can utilize the RF spectrum to exploit one UAV, propagate through the mesh network, and cause the entire swarm to fall out of the sky.

**Delivery:** The capability is delivered entirely over EMS.

**Depth:** The direct effect is not limited to the initial target. In this case, there is no clear bound for the risk. There is a chance for the effect to exploit and pivot outside of the intended target or targets.

**Determinism:** The capability is push-button and performs the same every time.




**Evaluation:** *Risk profile is not bounded to the geographic area of responsibility*

**Discussion:** In this case, the framework failed to definitively characterize the risk. This does not mean that the capability is not EA. Rather, further review is necessary: if the target is the entire swarm and the capability is known to prevent itself from propagating outside of its target, then the risk is likely consistent with EA. However, if there is a chance the capability could exploit devices of the swarm, then the risk may not be inconsistent with EA.

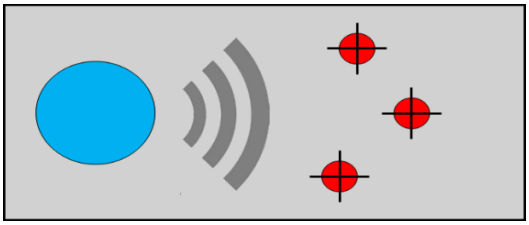
## 5. Counter UAS Swarm via Direct Engagement

**Vulnerability:** A hypothetical swarm of enemy UAVs operate in a mesh network with implicit trust between nodes. If one of the nodes is compromised, it is feasible to leverage that trust to pivot from one node to take control of the entire swarm.

**Capability:** A hypothetical capability against a swarm of quadcopter UAVs can utilize the electromagnetic spectrum to individually engage with each device and cause it to fall out of the sky and crash. The capability does not pivot or utilize the mesh network to succeed. The capability is limited to devices that can range directly and is directional in nature

**Delivery: T**he capability is delivered entirely over EMS.

**Depth:** Because the capability is not pivoting into the mesh network, it is clear the direct effect is limited to the target. There is some risk that it could impact other devices operating on the same frequency within range.



**Determinism:** The capability is push-button and performs the same every time.


**Evaluation:** *Risk profile is geographically bounded.*

## 6. Remotely-Controlled Capability

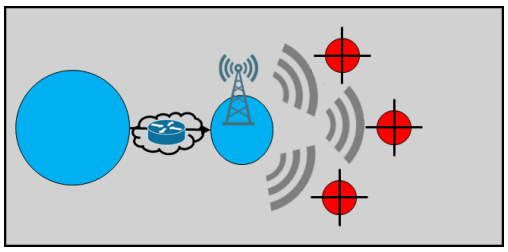
**Vulnerability:** A friendly, LTE internet-connected UAV is outfitted with an RF transceiver and a software-defined radio. An operator remotely controls the UAV over the internet via the LTE connection.

**Capability**: The software-defined radio can disrupt enemy targets on a separate frequency without impacting LTE.

**Delivery:** Although the capability is remotely controlled, the capability is delivered entirely over the EMS.

**Depth:** The impact of the disrupting function is geographically constrained to the commander's area of responsibility.

**Determinism:** The jamming function behaves the same every time it is triggered.




**Evaluation:** *Risk profile is geographically bounded.*

**Discussion:** When evaluating the delivery and depth of a capability, the evaluation starts with the final friendly asset. This could include a remotely operated transmitted via wire, or in this case, a remotely operated wireless device. How friendly forces control friendly assets is not relevant to determining whether capabilities delivered by those assets are geographically bounded.

If the LTE connection used to control the UAV is from a commercial provider, the commander must consider the implications of the liabilities of dual-use infrastructure. This risk is distinct from those associated with the UAV's capabilities.

## 7. EA via Computer Exploitation

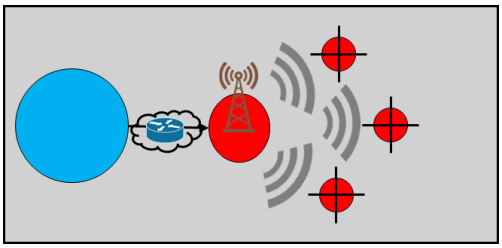
**Vulnerability:** A hypothetical enemy has an internet-connected system that also has an onboard software defined radio that can transmit at high power. This system is vulnerable to computer exploitation over the internet.

**Capability**: A hypothetical capability can exploit the existing vulnerability over the internet. The capability enables access to the SDR, which can be used to create interference on various frequencies.

**Delivery:** The target is the enemy system that is exploited over the internet (having to traverse an unknown number of systems from launch point).

**Depth:** The direct outcome is to enable access to the enemy system. Subsequent actions which use that access to create interference would be geographically constrained by the frequency and power of the transmitter.

**Determinism:** The capability is push-button and enables access every time it is used against a vulnerable system.




**Evaluation:** *Risk profile consistent with Offensive Cyberspace Operations*

**Discussion:** This scenario describes a sequence of actions to create the effect. These initial actions are associated with OCO, while the latter actions are associated with EA. However, because of the OCO elements, the overall risk profile is logically bounded rather than geographically bounded.

The capability is not being delivered by a remotely-controlled friendly asset; as such, the risks are distinct from the remotely-controlled capability scenario.

If the actions were separated and evaluated distinctly, then the jamming actions are consistent with the risks of EA. However, the overall risk of the operation must be evaluated holistically, not individually and distinctly.

## 8. Executable Code

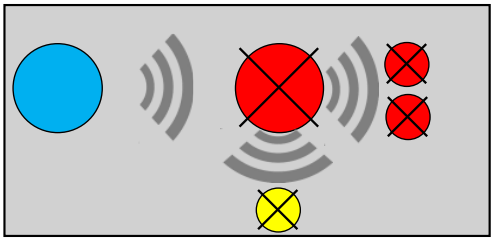
**Vulnerability:** An enemy compound uses a small-office-home-office wireless router to connect various remote sensors over Wi-Fi as well as to reach back. The router is vulnerable to a public vulnerability that allows one to remotely upload new firmware to the router without authentication or authorization.

**Capability**: Using EMS over line of sight, a handheld device can connect to the router, upload new firmware and introduce new executable code that will introduce heavy packet loss in all traffic, rendering it unusable. This will severely degrade compound communication.

**Delivery:** The capability is delivered entirely within the EMS.

**Depth:** The direct effect may not be limited to the target but will be regionally bound.

**Determinism:** The capability performs the same way against any vulnerable system.




**Evaluation:** *Risk profile is geographically bounded.*

**Discussion**: Note here that there is some risk that other network devices will be impacted by this activity. The risk is bounded to the devices within the range of the WiFi network and may still be acceptable. However, because the impact could spread beyond the initial target, closer analysis may be necessary.

Also note that the presence of “executable code” is irrelevant to this evaluation. From the perspective of a computing device, data is code and code is data. All forms of EA against computing systems succeed by influencing execution of code on a processor. Any evaluation of a capability as EA that considers executable code is prone to confusion.

## 9. Tuning Capability Parameters

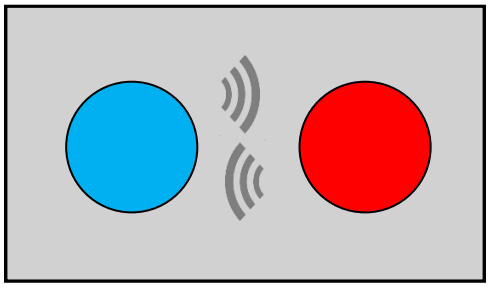
**Vulnerability:** An enemy communication system has a vulnerability in which a well-crafted signal can cause a receiver to cease functioning. Each device can be configured in a variety of ways, and the vulnerability can only be triggered if the attacker is able to craft a signal in a way that is tailored to the target device's configuration.

**Capability**: Using the EMS, the capability operator uses the capability to probe the target device and uses this information to configure the capability. Once all parameters are set in the capability, the operator triggers the final payload, and the target device ceases to operate.

**Delivery:** Both the probing and the final payload take place entirely over EMS.

**Depth:** The probing and direct effect is limited to the initial target and other devices within geographic range that are using the same frequencies

**Determinism:** The capability performs the same way against any vulnerable system. The parameters allow for tuning the capability within a fixed set of configurations, but the actual capability is still push-button.




**Evaluation:** *Risk profile geographically bounded.*

**Discussion**: The determinism test is not intended to limit the ability of the capability operator to modify parameters of the capability. Instead, it is meant to scope EA capabilities down to those which are pre-packaged and predictable. The risk is consistent even if the capability is tunable.

## 10. Interactive Console

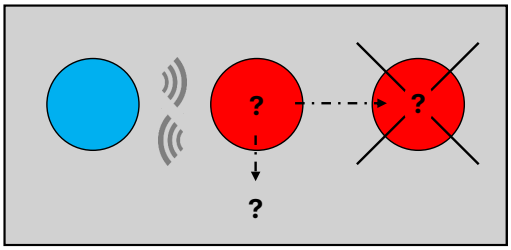
**Vulnerability:** An enemy communication system hosts a Wi-Fi network that can be leveraged to connect to the device over TCP/IP. The system exposes an interface over these protocols that can be leveraged to execute commands.

**Capability**: Using the EMS, the capability operator can connect to the enemy system over Wi-Fi and gain command execution. The capability operator then uses these commands to identify a misconfiguration in the device and elevate privileges to an administrator. Finally, the capability operator uses this to corrupt the file structure of the system and cause it to stop working. The capability operates on the message-layer and is directional in nature.

**Delivery:** All communication occurs over the wireless spectrum.

**Depth:** The direct effect is limited to the initial target.

**Determinism:** The capability requires human interaction to connect to the device, identify further vulnerabilities, exploit those vulnerabilities, and then use elevated access and knowledge of the system to cause an effect. This is not deterministic.





**Evaluation:** *Risk profile is geographically bounded.*

**Discussion**: The use of TCP/IP here is not disqualifying as EA. However, the lack of a well-defined, deterministic, packaged capability increases the risk of this action for further scrutiny. This scenario characterizes what might be considered proximal Cyberspace operations. This framework shows that the non-deterministic nature of these operations have elevated risk, but are still geographically bounded. If a capability developer automated and validated the steps so that they became deterministic, this risk in this action would be lowered.

## 11. Transmission Line Attack

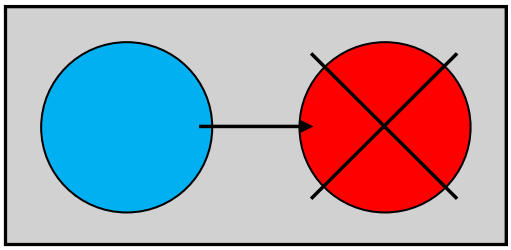
**Vulnerability:** An enemy system is remotely accessed and controlled by the enemy via a transmission line cable that runs a significant distance between the enemy position and the remote system.

**Capability**: When physically attached to the transmission line, the capability can send a signal over the transmission line that uses high power to destroy the enemy system.

**Delivery:** The delivery occurs over transmission lines, but in a single point-to-point nature consistent with Electromagnetic Attack.

**Depth:** The direct effect is limited to the initial target.

**Determinism:** The capability consistently destroys the enemy system.




**Evaluation:** *Risk profile is geographically bounded.*

**Discussion**: EA is not limited to wireless-based attacks. This scenario describes an EMS transmission that uses power or waveform to destroy an enemy system. This scenario is consistent with the risks of traditional EA.

If the situation was modified such that the capability utilized a message or protocol EMS transmission to trigger a denial-of-service condition in the target system and retained the direct connection to the target system without additional nodes, the scenario would still have a risk profile consistent with EA.

However, if the scenario was modified further such that the denial-of-service condition was triggered over a local area or wide area network (such as the internet or a military network), then the risk profile would be closer to OCO.

## Other Scenarios

- An enemy fortification is using wireless CCTV that has a vulnerability that allows it to be monitored remotely. A friendly capability can exploit the CCTV and remotely monitor the feed. Note: here, there is no effect to evaluate. This is categorically not an Electromagnetic Attack.
- A Cyber Capabilities Developer embedded within a unit can identify a weakness in an enemy system and craft a capability that is consistent with Electromagnetic Attack when evaluated against the Delivery, Depth, and Determinism framework. The developer provides this capability for use in the field. The developer's status as a member of the Cyber Mission Force is irrelevant to understanding whether the capability qualifies as EA.

# Additional Concepts

## Electromagnetic Attacks via a Transmission Line

The EMS consists of the range of frequencies of electromagnetic radiation from zero to infinity (JP 3-13.1). Most doctrinal references to the EMS assume that the signal is free to propagate through a vacuum or the atmosphere in many directions, but electromagnetic signals may be confined to a transmission line as well. These lines can transmit a variety of energy from powerlines carrying 0Hz DC voltage through fiber optics used to transmit electromagnetic radiation in the infrared, visible, and ultraviolet bands. While different in terms of medium, the concepts and considerations with regard to conducting an EA are similar.

## Cyberspace Risk Considerations

**Interconnectedness and Geographic Bounds**. Unlike the physical domains, the effects of cyberspace actions are often hard to bound geographically. Within the physical domains, physics limit potential effects to a specific geographic area and permit the use of special control measures. For EW, effects are typically limited by power and line of sight. However, computer networks transmit messages based on the logical configurations of the network which can be independent of physical geography (within certain physical constraints). Additionally, activities within cyberspace often involve third-part infrastructure and services. Therefore, risk from a cyberspace operation may not be constrained to an area of operation, crossing international boundaries and boundaries of organizational responsibility.

**Secrecy**: Secrecy—and thus classification—is often necessary to preserve the effectiveness of cyberspace capabilities and operations. The risk is twofold. First, if the vulnerability or exploitation is known, it can often be mitigated against, negating a potentially critical capability. Second, disclosure of operations occurring below the threshold of conflict can have negative implications at the national strategic level. EW also has secrecy considerations, like cyberattacks; some EA capabilities can be negated if known. Similarly, EW can be used for non-lethal effects and below the level of armed conflict. However, these concerns are less pronounced. Related concepts include wartime reserves, signature collection and analysis, and escalation.

**Wartime reserves**: In the context of secrecy, wartime reserves are capabilities that are kept in reserve so that their effectiveness is not diminished when used in war. Cyberspace and EW capabilities can be retained in reserve. The decision to do so is based on opportunity cost.  For cyberspace capabilities in particular, retaining a capability in reserve might not be practical or worthwhile.

**Escalation:** Both EW and CO can be used for non-lethal effects and below the level of armed conflict. However, detection and attribution of these actions by other parties can lead to escalation in hostilities and jeopardize national interests.

**Uncertainty**: The technical complexity and unknown aspects of system and network design can increase uncertainty about the resultant effect and the affected systems. The interconnectedness of cyberspace means that this uncertainty is not geographically bounded and may include numerous third parties across the globe. Uncertainty exists in all operations to include EA but the geographic scope is often relatively certain providing limits on the possible outcomes.

## Analysis Concepts

**Executable code:** At an intuitive level, executable code is an indicator of OCO. However, some attacks can abuse normal paradigms regarding input and execution. Many counter UAS techniques

leverage methods for how commands are executed. In this context, definitions of when “input that triggers execution” becomes “executable code” are complex and based on computer science concepts. For instance, while buffer overflows and injection attacks might transmit specific commands, they might also merely trigger the target to execute commands already on the system. We find the combination of “determinism” and “message-layer” a simpler tool to capture a similar concept.

**Pivoting** is revealed and analyzed through applying the proposed framework. Pivoting through third-party systems impacts delivery while pivoting within a target network impacts depth. Manual pivoting is an interactive process that will increase determinism.

**Jump boxes** and **redirectors** are closely related to the idea of pivoting. They use intermediate systems in the delivery of the effect. They are most associated with cyberspace operations.

**Precursor Actions** such as effect staging and remotely controlled effect launch may be necessitated by system functionality requirements or as a measure to reduce components of risk. Conceptually, remote actions to stage and trigger the launch of an effect are management pre-cursor functions separate from the actual launching of an effect itself.

**Duration or nature of effect**: While the nature of the effect is an important factor when considering risk and collateral damage, this analysis applies equally to both EA and cyberspace attacks and is not a distinguishing factor of either. Both EA and cyberspace attacks can have a range of effects that include reversable, transient, non-destructive, destructive, and lethal effects. Both can also be used to deceive and to gain information.

**Interactive operations**: Operator interaction with intermediate or adversary systems during an attack violates the concept of determinism and generally indicates the attack is part of a cyberspace operation.

**Tool exposure or compromise:** For capabilities that exploit software vulnerabilities, use of the capability may exposure the vulnerability and prevent future use. This is an important risk consideration. However, this consideration is associated with the specific tool and generally a separate consideration from the analysis framework presented. Similar considerations apply to certain electromagnetic warfare capabilities.

# Appendix B - Legal Analysis & Framework for EA Procurement and Employment

*Disclaimer: This is not intended to be a comprehensive in-depth legal review, but a short overview of overarching considerations relating to terminology use and the overlap of EA and cyber effects within the larger legal landscape. A separate follow-on study to provide a more comprehensive assessment of specific legal issues associated with EA actions, including the consideration of intel authorities, is recommended.*

## Overview

The distinction between military doctrine and law is crucial. Military doctrine consists of fundamental principles that guide the actions of military forces in support of objectives. Broadly speaking, it provides a common framework for understanding how to conduct operations. It is not prescriptive but offers authoritative guidance to facilitate consistency and effectiveness of commanders in military operations.

In contrast, law provides boundaries regarding what operations can and cannot be conducted, and mandatory limitations regarding who may conduct what operations and how they may be conducted. As such, law supersedes doctrine. Legal doctrine refers to the established principles and precedents guiding the interpretation of laws.

Neither military nor legal doctrine are fixed and can evolve over time to reflect the fluid nature of both war and governing laws. While military doctrine must be in alignment with the governing legal considerations, ambiguity and uncertainty can arise, particularly when evolution of military practices and technologies outpaces guiding regulation or law. To the extent that doctrine may appear to conflict with law, it must give way to the legal rule.

## EA and Cyber Authorities

The fact that Electromagnetic Attacks and cyber-attacks can be difficult to distinguish based on their objects and effects has resulted in commander confusion as to the applicability of relevant legal authorities. Much of this confusion stems from the siloed nature of “cyber” and EA operations in practice.

While the Secretary of Defense is primarily responsible for cyber authorities within the Department of Defense, many aspects have been delegated to USCYBERCOM as the lead combatant command. While USCYBERCOM may further delegate these authorities to lower echelons or other combatant commands as necessary, the present reality is that *little delegation occurs, and application of cyber effects remain closely controlled*.

Conversely, EA authorities nest within the given authorities of combatant commands in support of operations for which they are tasked. These authorities are often delegated to lower echelons based on specific mission sets, roles, and operational need. As such, *it is assumed that commanders at all echelons will have the authority to broadly conduct EA within the scope of their mission, military boundaries, and appetite for risk*.

As a legal matter, the question of whether any given commander possesses the authority to engage in a specific attack is an affirmative one. Rather than assessing whether other entities are empowered to engage in a particular attack, commanders should instead focus on whether they possess the requisite authority to engage in the attack in question. Thus, in the context of EA, the relevant legal question is whether the attack is an electromagnetic one that has been properly delegated and within the operational confines broadly set out in the "Legal Analysis Workflow for EA Effects" section below.

## Legal Landscape for EA

In investigating the legal landscape for employment of EA effects we make several broad observations:

1. The legal definition of "attack" differs from common doctrinal usage of the same term, especially in relation to that which is carried out through the electromagnetic spectrum. Many effects employed during an EA are unlikely to arise to the legal threshold necessary to be considered an attack in war. Legal opinion surrounding what constitutes an attack, particularly within the cyber realm, recognize "disabling" or "loss of functionality" as thresholds to be considered an attack. However, "degradation" or "temporary" effects, such as jamming, likely do not[12].

2. The application of legal doctrine to emerging EA capabilities and usage are underdeveloped, with only a handful of recent articles exploring parts of the problem space[13]. However, there is a strong correlation to cyber, particularly with the variance of effects that may occur, from temporary to more permanent, and associated considerations, which can serve as strong references for the Electromagnetic Attack space.

3. Legal considerations appear to primarily consider the means, thresholds, and objectives when assessing whether or not an action is legally permissible. In the case of EA, actions that use the electromagnetic spectrum or electromagnetic energy to cause actions that meet the threshold of an attack are likely to be broadly considered EA attacks. However, actions that do not rise to the threshold of an attack (temporary or non-permanent actions) likely do not[14]. However, there is no terminology distinction for these lower threshold actions in doctrine, and the use of "Electromagnetic Attack" may pose challenges for legal reviews of effects that would not normally meet this threshold.

4. There are many considerations that impact the decision and application of electromagnetic warfare systems. While deconfliction and differentiation from cyber is one and the main focus of this report, the relationship to intel and the role of intercepting and processing signals and the potential conflict with Title 50 actions requires further examination. In many cases, the capability and requirement to process signals by a commander in his battlespace will require application of technology that will likely overlap with intelligence authorities and definitions. This space needs to be investigated and clarified to prevent the stagnation of capability development for EW.

[12] Attack (international humanitarian law), Cooperative Cyber Defence Centre of Excellence (2024). Available from https://cyberlaw.ccdcoe.org/wiki/Attack
[13] Lawless, R. and Nasu, H., Electronic Warfare and the Law of Armed Conflict, The Lieber Institute, West Point Publishing, (2024). Available from: https://lieber.westpoint.edu/electronic-warfare-law-armed-conflict-2/
[14] Vincent L. DeFabo, Rethinking Cyberspace Operations: Widespread Electromagnetic Jamming by States Indicates Cyber Interference Is Not a Use of Force, 86 J. AIR L. & COM. 219 (2021). Available from: https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jalc86&id=236&men_tab=srchresults

## Discussion

The broader takeaway from these points is that the legal landscape likely allows for a much broader range of EA effects to be applied than doctrine would presently consider and that the legal overlap in considering cyber and EA questions, from a legal perspective, is likely substantial. However, from an actual employment standpoint, the delegation of authorities granting employment will likely differ by echelon, particularly with cyber, and it is assumed that the employment of EA, specifically within a commander's operational space, will have a broader opportunity for employment and use. Stated more precisely, commanders can likely leverage authorities governing use of EA to deliver a broader range of effects than present doctrine might consider and would otherwise be categorized as cyber. We should recognize this overlap as an opportunity and not a problem to be solved.

# Legal Analysis Workflow for EA Effects

## Overview

The flow chart below depicts a basic analysis with major legal considerations for approaching issues involving the purchase or use of operational capabilities and the subsequent consideration of whether and how those capabilities can be used by the units or agencies acquiring those capabilities, particularly as they relate to EA.[15]

In many instances, military units will have the ability to purchase new technologies to advance capabilities and address their mission needs; however, questions arise as to whether those units can purchase those capabilities in the first place and then subsequently use them for specific purposes given their assigned missions and authorities. This flow chart is intended to present a general method to approach these issues, and not necessarily specific to a particular type of activity, unit, or authority. In many cases, classified doctrine, policy, and directives must also be consulted for specific acquisition and use cases.

Legal advisors may refer to this chart when advising clients about whether specific EA capabilities fit their authorities, mission, and purpose.

[15] Note: This chart is not intended to represent the only way this issue might be approached. It is presented as a method to help incorporate many of the major legal considerations. It is limited due to the inability to depict classified authorities and other relevant processes (e.g., deconfliction processes, policy directives). Legal advisors should always consult their higher operational headquarters to ensure they have all the relevant directives and policies required to analyze a particular issue.

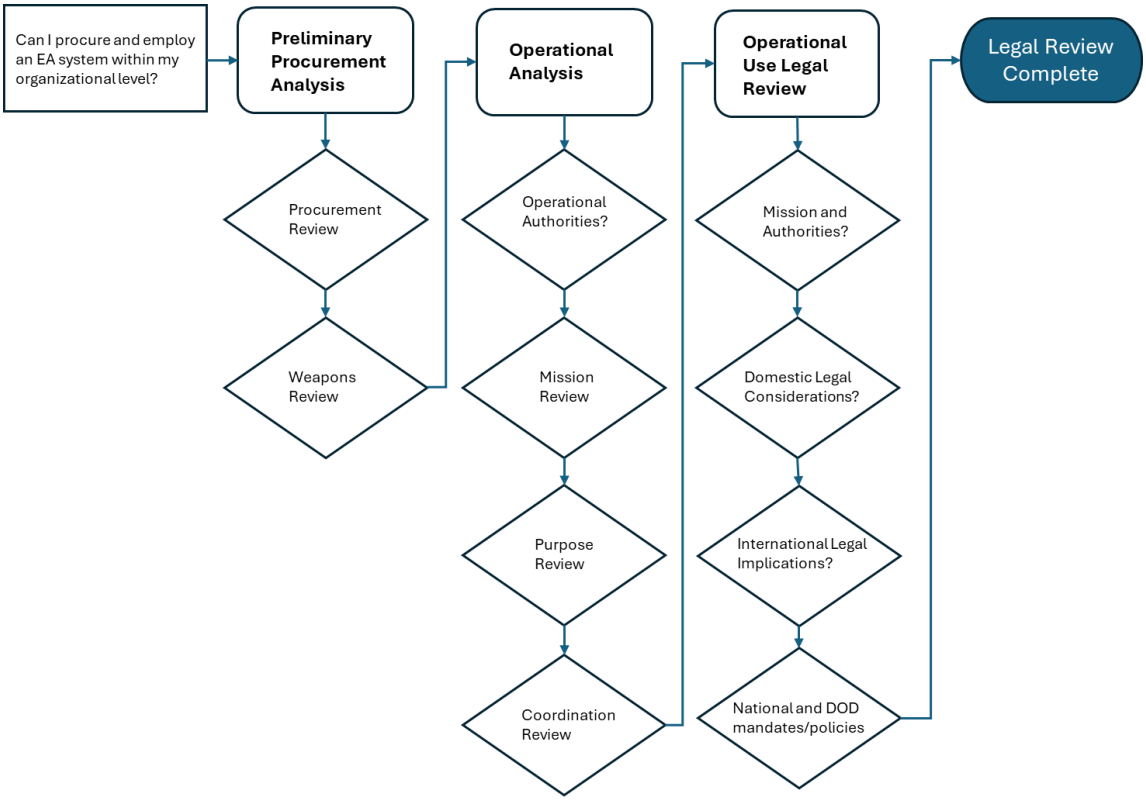



*Figure 1: Legal Analysis Workflow for EA Procurement and Operational Employment.*

## Part 1: PRELIMINARY PROCUREMENT ANALYSIS:

**PROCUREMENT**. Are you purchasing something to carry out the envisioned EA and do you have the approved funding and proper authorization to accomplish that procurement?

- **Go through general acquisitions and procurement analysis.**
  - For example, some general procurement questions may include whether there has even been money appropriated and allocated to the purchasing unit for this specific or general purpose. If applicable, are you purchasing from an approved vendor, etc.? Does the DFARs or FARs mandate specific procedures or rules for the acquisition?
- **Follow applicable laws and DOD policies for the acquisition of IT items and COTS items.** An ATO or Supply Chain Risk Assessment may be required depending on the type of item purchased, just to name a few of the many considerations when acquiring IT equipment.
- **Procurement of major IT investments may require additional procedures and approvals.**

**WEAPONS REVIEW**. Is your EA system a "weapon" as defined by Army regulations or policy?[16] If a weapons legal review is required, has that capability undergone a weapons review and obtained approval for acquisition?[17]

Importantly, just because a capability receives legal approval to be procured, it does not necessarily mean that it is legally approved for a particular use case. Each individual operational use of a

[16] See Army Regulation 27-53, Legal Review of Weapons and Weapon Systems.
[17] Note: If you are assigned to a joint command, you may need to consult multiple service requirements regarding what qualifies as a "weapon" and what is required for a weapons legal review.

capability needs operational use approval and is dependent on specific unit missions and authorities, as well as other legal considerations for how the capability is used. This leads to the second part of the analysis: operational issues.

**Part 2: OPERATIONAL ANALYSIS:**

**OPERATIONAL AUTHORITIES**. If planning to employ an operational capability, is the unit or organization acting pursuant to authorized operational authorities?

- In most cases, if a unit is planning to deploy operational capabilities, then the unit would likely need to be operating under ***operational authorities*** (in an operational chain of command) and not ***service authorities*** (under a service chain of command; i.e., under "train, man, and equip" authorities) to use operational capabilities. For example, if you are operating at a unit that is designed as a service-specific unit, under Title 10, "train, man, and equip" authorities, then you most likely do not have operational authorities. In contrast, if you are at a unit that falls under a Combatant Command, then you likely fall under operational authorities. Operational authorities flow through the SECDEF down to the Combatant Commands. Until a unit is assigned under a COCOM, it is likely under the service chain of command and does not have operational authorities. To better understand your unit's force management structure, consult with Force Management Managers at your unit, review C2 Orders, and become familiar with the Global Force Management Implementation Guidance (GFMIG).

**MISSION**. Does your use of EA or another capability fit your mission?

- **Does the unit/organization have delegations and authorities through operational mission control?**
    - Consult unit mission authorities (C2 orders, delegation memos, EXORDs). (Practice Tip: Follow EXORD authorities through the CoC to ensure that operational authorities flow through the proper chain of command from SECDEF down to the unit.)
    - *NOTE: Do not just rely on OPORDs or PLANORDs to determine mission authorities. An untrained legal advisor may approve those OPORDs or PLANORDs without following the chain of authorities. Follow the law and be able to trace the proper operational chain of command to the authorities to ensure your legal mission authorities for the unit/organization.
- **Do you have all relevant ROEs and is your use of EA consistent with them?** Do you have a basic ROE that must be followed? Do you have an authorized EW ROE for the envisioned operational use? Did the proper authority approve the requested ROE (consult classified ROE policy)? Possession of a properly issued, EW-specific ROE is indicative that use of EA capabilities is appropriate, at least insofar as it is consistent with that ROE.
- **Are there any other specialized policies that are applicable?** In some cases, classified policies that are specific to the type of planned activity might exist. In many cases, units/organizations that do not have statutory or chartering authority for the type of activity planned, should reach out to those organizations that do (e.g., IC organizations or special operations units) to determine if there are specific policies and delegations for the activity planned.

**PURPOSE**. Does the purpose for your use of EA or other related activity fit the purpose of your specific mission and op authorities?

- Is your use of EA purely ***tactical***? Could it be considered ***strategic***? If there are strategic implications, then it is likely restricted to a strategic-level organization for authorization or delegation.
- Are you planning to use the capability for ***intelligence*** or ***operational*** purposes or potentially ***both***? If for intelligence purposes (or both), then ensure your organization or unit has operational intelligence missions and authorities. As stated above, consult with combat service support agencies or other organizations that may have such authorizations to determine whether there are applicable policies or other considerations relevant to the planned activity.
    - *NOTE: Do not execute any intelligence activities or intel-related activities without proper intelligence oversight capabilities. If your unit does not have proper intelligence oversight capabilities or personnel, then it is a good indication you do not have an intelligence mission and authorities to conduct that activity. Consult specific EXORDs or chartering policies to determine specific mission purposes and authorizations.

**COORDINATION**. How much does your use of EA look, feel, or have consequences like another activity overseen by another combatant command, combat service support agency or other organization (even outside the DOD)? In contrast, how much does it look, feel, or have consequences like traditional EW activities?

- The more it looks like OCO, the more policy and deconfliction discussion is appropriate.
- In many cases there are established processes and procedures in place for specific activity deconfliction and coordination. If your unit is not aware of these processes, then consult through higher chain of command up through the COCOMs or CSS agencies.

## Part 3: OPERATIONAL USE LEGAL ANALYSIS:

After ensuring proper procurement, mission, and authorities, then each capability must also be analyzed for legality in its proposed use. NOTE: Each use case should typically be accompanied with a unit plan or CONOP that details the proposed use of the capability and outlines the activity authorities that support the capability use.

- A legal analysis by the supporting legal offices (through the operational chain of command) should consider the following:
    - (1) Mission and Authorities (as discussed above). Units may have to also consult classified authorities to determine the full scope of authorities and delegations. This also must take into consideration ***who*** is the proper authority to approve the capability use or activity proposed.
    - (2) Domestic Legal Implications.
    - (3) International Legal Implications; and
    - (4) National and DOD mandates and policies regulating the approval and use of the capabilities (likely must consult classified authorities and policies).

## Part 4: Policy/Prudential Considerations

Even if all legal requirements are met, the commander employing affect must still weigh certain policy and prudential considerations implicated by the envisioned use of EA. First, the commander must first consider whether deconfliction, even if not formally required, should be undertaken. While analytically distinct, certain EA may disrupt ongoing or prospective cyber operations.

More generally, the consideration of other operational risks might be counseled in favor of abstention or deconfliction. Such an assessment will require balancing many competing factors and considerations against the perceived value of return. While each employment of an EA capability will require its own assessment, planning factors might include:

- Risk of capability loss/recovery by enemy systems
- Risk of interference to both civilian and friendly systems within a geographic space
- Risk of detection and counter-ops
- Risk of propagation of effect. While many EA effects will be temporary in nature, deterministic payloads targeting processing functions may unintentionally propagate if target functionality and handling is not precisely known.
- Scope of impact: Do the targets and intended impact meet legal requirements for targeting, scope, impact, etc.?
- Geographic bounds – Is the intended effect controlled within a commander's area of operations, or will the effect be perceived outside these bounds of authority?

# Part II – Supporting Research Products

# Appendix C - Prior Army Efforts to Differentiate EA from Cyber

Content can be found in CUI version of report.

# Appendix D - Emerging Environment Review

## Overview

One particular point of interest in our research was to understand where applications of EA were already pushing the bounds of understanding or terminology in practice. As efforts in Ukraine and Israel have demonstrated the rapid evolution present within this domain, we leverage examples from each to demonstrate where bounds are already beyond our present doctrinal understanding of what may be considered for Electromagnetic Attack. This is not an exhaustive list of examples, but demonstrative unclassified selections used to both understand and identify where bounds of EA overlap with cyber are already being pushed in practice.

## Assessment of Current Operations

The cases presented below are real-world examples of wireless attacks and trends in EW capability development that expand traditional descriptions of EA or blur the lines between doctrinal EA and OCO effect terminology. We map the features of these examples (left column) to related characteristics derived from current doctrinal terms (right column) in Figure 1. The doctrinal terms in the right column are not exhaustive but were selected for their close relationship to the real-world case features to highlight how examples may be perceived at present.

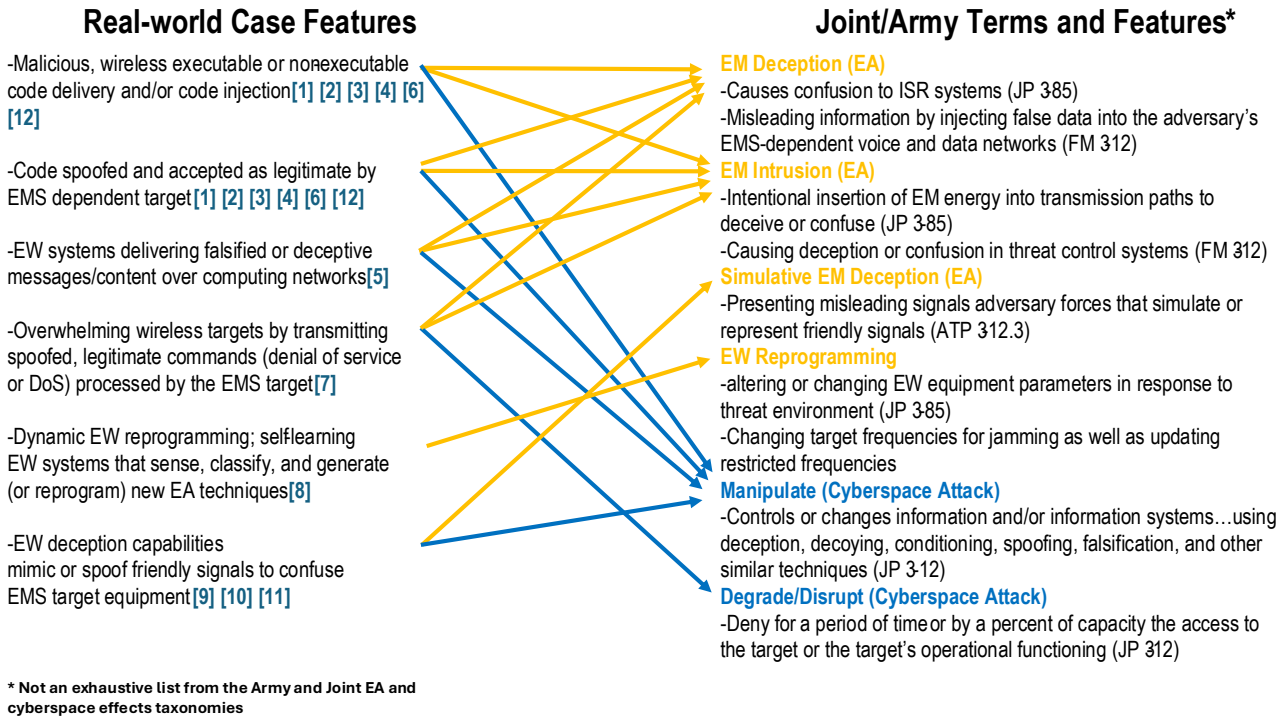



*Figure 1: Mapping of real-world examples leveraging EA by their features to current Joint/Army doctrinal terms. Numbers align to examples which follow below [1-12].*

From the chart, we observe that many real-world features map or align to characteristics of both cyberspace attack and Electromagnetic Attack (EA). This highlights the challenge of differentiation between EA and cyber based on the effect according to current doctrine. However, this should not be viewed as a problem (broadly), but an opportunity that can be leveraged to give commanders flexibility in applying effects and the methods that they may use to do so. However, the multiple mappings within each domain's unique terms do support the need for a more robust phrasing or taxonomy to distinguish categorization more precisely. Our layered framework model (power, waveform, protocol, and message) presented in our main report can serve as an aid to enhance and clarify EA effect terminology.

## Selection of Real-World Examples of EA Application

The selected real-world cases are numbered according to the footnote found in the preceding mapping chart with footnotes linking to the references used. Within the summaries, we highlight in ***(bold)*** the distinguishing features of the examples.

***1. Counter Unmanned Aerial System (C-UAS) employment in Afghanistan and Israel***

**Overview**: Theaters of Operation in Afghanistan and Israel have employed C-UAS systems that employ tailored protocol attacks. These techniques ***exploit communication protocols*** used between the ground control station (CGS) and small UAS (sUAS). ***Commands are delivered by the C-UAS system and processed by the sUAS computing system***, causing disruption or takeover of the sUAS. Similar systems have been developed by Israel Defense Industry[18] [19] [20].

**Distinguishing feature(s):** Deterministic command injection using known protocols.

***2. TETRA injection attack***

**Overview**: TETRA wireless devices are vulnerable to ***injection attacks*** that can cause disruption to services. In this example, TETRA radios are used to enable critical infrastructure communication. This wireless attack is conducted by ***inserting malicious and unsanitized data which match protocols used*** by the target system that could then be used to disrupt services to the operation of the target[21].

**Distinguishing feature(s):** Deterministic command injection using known protocols.

***3. Wireless code injection (IoT Example)***

**Overview**: Previously employed in cellular and in wireless local area networks, code injection is now being discovered in IoT networks. Code injection leverages vulnerabilities in a system in which input is improperly sanitized and is executed by a dynamic runtime or processor. In this attack, ***code is delivered to and accepted by the target as authentic,*** subsequently granting the

[18] CACI International, Inc., "Is Modernizing the Kill Chain," April 7, 2022, https://events.afcea.org/tip21/CUSTOM/pdf/caci_wp.pdf.
[19] Pavlo Kryvenko, "Ukrainian Drones vs Russian Jamming," News, *New Geopolitics Research Network* (blog), June 10, 2024, https://www.newgeopolitics.org/2024/06/10/ukrainian-drones-vs-russian-jamming/.
[20] Israel Aerospace Industries, "IAI'S ELTA SYSTEMS UNVEILS NEXT GENERATION DRONE GUARD COUNTER UNMANNED AIRCRAFT SYSTEM (C-UAS) | IAI," IAI Press Releases, November 21, 2018, https://www.iai.co.il/iais-elta-systems-unveils-next-generation-drone-guard-counter-unmanned-aircraft-system-c-uas.
[21] Kim Zetter, "Code Kept Secret for Years Reveals Its Flaw—a Backdoor," *Wired*, accessed December 17, 2024, https://www.wired.com/story/tetra-radio-encryption-backdoor/.

attacker privileged access or the ability to disrupt the services of the target. Code injection delivered by EA is localized to the target system[22].

**Distinguishing feature(s):** Deterministic code injection.

***4. EA vs Cellular networks in Afghanistan***

**Overview:** EA systems employed in Afghanistan provided counter communications effects in support of base force protection. These EA systems ***delivered spoofed, protocol-based commands*** that disrupted target devices' connections to legitimate cellular towers[23] [24].

**Distinguishing feature(s):** Deterministic spoofing by wirelessly delivering known protocols directly to the target devices.

***5. EW delivery of Short Message Service (SMS) texts***

**Overview:** Russians have employed UAS platforms with EW payloads to deliver ***deceptive SMS messages*** through cellular networks. In these cases, the SMS texts were ***inserted into the cellular network*** and targeted at Ukrainian mobile devices and with the intent to ***mislead and deceive[25].***

**Distinguishing feature(s):** Deterministic delivery of deceptive information using known protocols.

***6. Selection of Beast+ as the Terrestrial Layer-System (TLS)- Manpack***

**Overview:** The U.S. Army approved the Beast+ (CACI developed) as the selected EW system for TLS-Manpack. This system possesses attacks that are designed to ***exploit vulnerable communication protocols*** used in digital radio and UAS command links[26].

**Distinguishing feature(s):** Deterministic disruption of communications using known protocols.

***7. Wireless denial of service (DoS) attacks***

**Overview**: Wireless DoS attacks can be accomplished using a variety of methods. Typically, a flood of ***packets that use standard wireless communication protocols are delivered to the target***. As the target processes these packets, the system is overwhelmed causing a denial of services to legitimate hosts/clients[27].

**Distinguishing feature(s):** Deterministic disruption of communications using known protocols.

***8. EW Deception capabilities***

**Overview:** Vendors such as CACI and Motorola have developed tools to ***generate signals which mimic legitimate friendly emissions***. These signals could be ***delivered to and processed by***

---

[22] Haitham Ameen Noman and Osama M. F. Abu-Sharkh, "Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review and Practical Implementations," *Sensors (Basel, Switzerland)* 23, no. 13 (June 30, 2023): 6067, https://doi.org/10.3390/s23136067.
[23] Defense Advancement (DA), "Counter-UAS (CUAS) Equipment | Counter-Drone Equipment Suppliers," *Defense Advancement* (blog), accessed December 17, 2024, https://www.defenseadvancement.com/suppliers/military-cuas/.
[24] Kris Osborn, "US Army Is Making Some Sweeping Changes to Its Electronic Warfare Technology," Text, The National Interest (The Center for the National Interest, September 9, 2016), https://nationalinterest.org/blog/the-buzz/us-army-making-some-sweeping-changes-its-electronic-warfare-17657.
[25] Army Recognition Group, "Russian Troops Using Leer-3 Able to Jam Ukrainian Army Mobile Phone Si," Global Defense News, October 20, 2022, https://armyrecognition.com/news/army-news/2022/russian-troops-using-leer-3-able-to-jam-ukrainian-army-mobile-phone-signals-within-30-km.
[26] CACI International, Inc., "EW/ECM Technologies," 2024, https://www.caci.com/ew-ecm.
[27] Patrick Tucker, "In Ukraine, a US Firm Tests a Promising Tool against GPS Jammers: Cell Phones," Defense One, September 30, 2024, https://www.defenseone.com/technology/2024/09/group-ukraine-testing-newest-weapon-against-gps-jammers-cell-phones/399952/.

***adversary computing systems to deceive and mislead*** the adversary. These systems have been employed in training environments and are at prototype or above maturity. These systems exemplify EA deception capabilities.[28] [29]

**Distinguishing feature(s):** Spoofed friendly emissions which will not directly affect adversary systems.

### *9. Dynamic EA reprogramming in Ukraine Kursk Offensive*

**Overview:** ***Rapid reprogramming*** and EA techniques on the front line is credited to success of EW operations to neutralize Russian drone capability. Swift EA reprogramming led to the effective neutralization of Russian Intelligence, Surveillance, Reconnaissance (ISR) capabilities so that Ukraine could advance rapidly through the Kursk territory. Software defined radios employed by the Ukrainian military highlight their advantage by overcoming legacy EW reprogramming efforts that would take months to be accomplished[30] [31].

**Distinguishing feature(s):** Reprogramming EW systems by itself does not change the limited range and deterministic nature of EW payloads.

### *10. Future of EW-based Machine Learning (ML)*

**Overview:** Revelations from the war in Ukraine describe how machine learning (ML) algorithms are crucial in adapting to a dynamic EMS and aiding in drone warfare. Static EW protocols are ineffective because the enemy is continuously changing techniques. Current and future warfare require ***dynamic, cognitive EW processes*** (enabled by ML) ***that classify and process signals then modify EA techniques*** to respond to the dynamic nature of the EMS based threat environment.[32] [33]

**Distinguishing feature(s):** By itself, signal classification is a passive and deterministic action with no strategic risk.

### *11. Defense Industry Development of Cognitive and ML-EW Capabilities*

**Overview**: Defense industry companies such as BAE, Northrup Gorman, and SRC are developing smart ***EW systems that learn and rapidly react*** to threats in the EMS (in milliseconds). These systems ***dynamically generate new EW payloads and custom jamming techniques.*** [34] [35] [36]

---

[28] CACI International, Inc., “CACI SMART Is Modernizing the Kill Chain.”
[29] Mark Pomerleau, “Army Expects to Mature Electromagnetic Spectrum Decoy and Obfuscation Systems in FY ’25,” *DefenseScoop* (blog), March 22, 2024, https://defensescoop.com/2024/03/22/army-electromagnetic-spectrum-decoy-obfuscation-systems-2025/.
[30] Kollen Post and Aaron Mehta, “Inside Ukraine, Startups Try to Edge Russia in the Electronic Warfare Race,” Breaking Defense, June 10, 2024, https://breakingdefense.com/2024/06/inside-ukraine-startups-try-to-edge-russia-in-the-electronic-warfare-race/.
[31] David Zikusoka, “The Future of War Is Electromagnetic,” *New America* (blog), December 4, 2023, http://newamerica.org/future-frontlines/blogs/the-future-of-war-is-electromagnetic/.
[32] Army Recognition Group, “Russian Drones Now Equipped with Electronic Warfare Systems to Counter Ukrainian Interceptors,” Global Defense News, October 17, 2024, https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/ukraine-russia-conflict/russian-drones-now-equipped-with-electronic-warfare-systems-to-counter-ukrainian-interceptors.
[33] Joseph Trevithick and Tyler Rogoway, “Cognitive Electronic Warfare Could Revolutionize How America Wages War With Radio Waves,” The War Zone, July 7, 2020, https://www.twz.com/34606/cognitive-electronic-warfare-could-revolutionize-how-america-wages-war-with-radio-waves.
[34] Charlotte Adams, “Cognitive Electronic Warfare: Radio Frequency Spectrum Meets Machine Learning,” *Avionics Magazine*, August 2018, https://interactive.aviationtoday.com/avionicsmagazine/august-september-2018/.
[35] BAE Systems, “BAE Systems Demonstrates Cognitive Electronic Warfare Capabilities at Northern Edge 2023,” BAE Systems | United States, September 2024, https://www.baesystems.com/en-us/feature/bae-systems-demonstrates-cognitive-electronic-warfare-capabilities-at-northern-edge-2023.
[36] BAE Systems, “Electronic Countermeasures,” Commercial, 2024, https://www.baesystems.com/en/product/digital-electronic-warfare-system-dews.

**Distinguishing feature(s):** Deterministic payloads do not alter their effects after delivery and are limited in delivery and depth.

***12. Ukraine 'redirecting' Iranian-designed kamikaze drones back to Russia***

**Overview**: Ukrainian EW systems are ***spoofing satellite navigation signals*** to protect against long-range drone attacks. These systems ***send custom messages using GNSS protocols to redirect enemy UAS to a specified region***[37]**.**

**Distinguishing feature(s):** Spoofed GNSS messages follow specific protocols, resulting in deterministic effects on navigation to a specific regions.

[37] Henry Samuel, "Ukraine 'Redirecting' Iranian-Designed Kamikaze Drones Back to Russia," *The Telegraph*, November 28, 2024, https://www.telegraph.co.uk/world-news/2024/11/28/ukraine-redirect-iranian-designed-drones-to-russia/.

# Appendix E - Doctrinal Summary by Service and Terminology Analysis

## Section I: Organization, Overview, & Observations

This appendix focuses on our efforts to assess and understand the doctrinal approaches of each service with regard to EA and Cyber actions. Because of the many efforts conducted in support of this review, we have separated this appendix into three main sections, as follows:

Section I: Organization, Overview & Observations

Section II: EA and Cyber Doctrine Review/Summary

Section III: Supporting Products

A) Identification and Frequency of Terms
B) Key Phrases and Language of EA, Cyber Attack, and Related Terminology of Interest
C) Metrics for EA and Cyber Attack Terms

### Overview

As our foundational effort, we first sought to understand how each service approached electromagnetic warfare and cyberspace operations, first broadly, and second as it more narrowly relates to EA and cyberspace attacks. A comprehensive survey of relevant terminology usage revealed over 120 U.S.G. publications describing activities related to either EA or Cyber from unclassified sources alone. This collection[38] included everything from Presidential Policy Directives (PPD) and National Strategic documents to Chairman of the Joint Chiefs of Staff (CJCS), Department of Defense, Armed Services, and NATO publications. While not every publication provided additional depth or value to our understanding, the breadth of documents investigated and their resulting differences with respect to phrasing and understanding were important to help understand the problem space more broadly and the needed nuance that would be required to provide any recommendations.

Primarily, this publication review enabled a number of outcomes, to include assessing how far we would be able to deviate from joint doctrine in further bounding or defining new terminology, determining where bounds between EA and cyber already exist in doctrine and prior language, and assessing opportunity for possible synergy between services and joint doctrine if a new term or definition was desired.

[38] See *Appendix G* for a complete list of reference citations.

## Notable Observations:

In assessing how to differentiate EA from cyber, several high-level observations were made because of this doctrine review:

**1) Services do have precedent for re-defining space within the electromagnetic operating environment (EMOE) using service specific doctrinal terms.** As one example, the Air Force has established *airborne electromagnetic attack*[39] as a doctrinal term to differentiate the Air Force's focus on delivery of EA via airborne platforms from the wider operating environment.

**2) There is a precedent in doctrine to recognize stronger overlap between EA and cyber.** Space force considers all their operations to simultaneously be cyberspace operations and EMS operations.[40] This is primarily a result given the nature of their operating domain, however, recognition and distinction are important.

**3) Army doctrine introduces terminology and phrases that serve to blend the lines between EA and cyberspace attack more than the other services.** Use of terminology that hints towards delivery of data within EW phrasing is mostly an Army occurrence while other services remain more closely aligned with the vagueness of joint doctrine here.

**4) Examples or clarifying rationale within doctrine could help clarify bounds for what is broadly considered either cyber or EA actions and where overlap is expected to occur.** While joint doctrine primarily relies on "the delivery of electromagnetic energy", of which encoded data payloads would accurately be considered, clarifying terminology or examples would serve to strengthen this understanding.

**5) Doctrine, as written, leans towards language and descriptions which favor classifying effects as cyber which could otherwise be considered EA.** This is primarily a result of vagueness surrounding EW terminology and a more descriptive and direct approach within cyber doctrine.

# Section II: EA and Cyber Doctrine Summary and Review

## Joint Electromagnetic Warfare & Cyber Doctrine Overview and Summary:

*Notes:*

1) *There is very limited Space Force doctrine at present. The doctrine that exists is very nascent and limited in scope, offering extremely high-level guidance compared to other services.*
2) *Select doctrine located within the classified domain. While this was reviewed as part of our assessment, we do not include the associated content here. In reviewing the classified doctrine, we found that it did not substantially alter findings or rationale in any way.*
3) *While many additional reviews of tangential doctrine and broader service assessments and analysis were completed in support of this effort, we only present the relevant information,*

[39] AFDP 3-85, *Electromagnetic Spectrum Operations* (Washington, DC, USA: U.S. Dept. of the Air Force, 2023), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf.
[40] SDP 3-0, *Operations Doctrine for Space Forces* (Washington, DC, USA: U.S. Space Force, Dept. of the Air Force, 2023), https://www.starcom.spaceforce.mil/Portals/2/SDP%203-0%20Operations%20(19%20July%202023).pdf?ver=nHRhKpy49XVtcSVRaQRNNg%3d%3d.

*summaries, and takeaways that we believe are valuable to understanding here. These are primarily drawn from the primary doctrinal resources for each service (3-85 and 3-12 or similar).*

**Joint EMSO Doctrine Overview (JP 3-85)**

Within joint doctrine, the electromagnetic spectrum (EMS) is defined as a maneuver space for the conduct of operations within the broader electromagnetic operational environment (EMOE). The EMOE encompasses a much broader set of considerations than the EMS which include the actual and potential radiation, conditions, circumstances and influences that may affect the employment of capabilities and decisions of the commander.

Within the EMOE, joint electromagnetic spectrum operations (JEMSO) are conducted to achieve desired objectives and end states. JEMSO operations are separated by actions that occur within the continuum of conflict, from peacetime to war. During peacetime, these include readiness and management operations to ensure adequate access to the EMS and deconflictions across the joint community and coordinating host nations. During conflict, JEMSO shifts towards EMS superiority and maneuver, leveraging coordinated actions to exploit, attack, protect and manage the EMOE.

Similarly, electromagnetic warfare (EW) encompasses a range of actions using electromagnetic and directed energy to control the EMS or attack the enemy. EW is further categorized into three principal set of actions: electromagnetic attack (EA), electromagnetic support (ES), and electromagnetic protection (EP), which recognize the offensive, defensive, and support opportunities that are necessary to maintain superiority of the EMS.

Within EA activities, several effects are identified which include effects to destroy, degrade, disrupt, and deceive. Similarly, ES activities present two main effects: detect and exploit. EP presents no further sub-categorization or identification of unique effects. However, EP is differentiated from defensive EA by recognition of efforts to ensure operation of systems in congested and contested environments while defensive EA is a set of EA actions used to protect from a targeted physical attack.

Several further EW capabilities and activities are identified which do not precisely fit within the above construct. These include directed energy, countermeasures, probing, meaconing, geolocation, and frequency deconfliction actions.

Relating these terms together, we can present joint EMSO doctrine and the hierarchical relationship of associated terminology as follows:

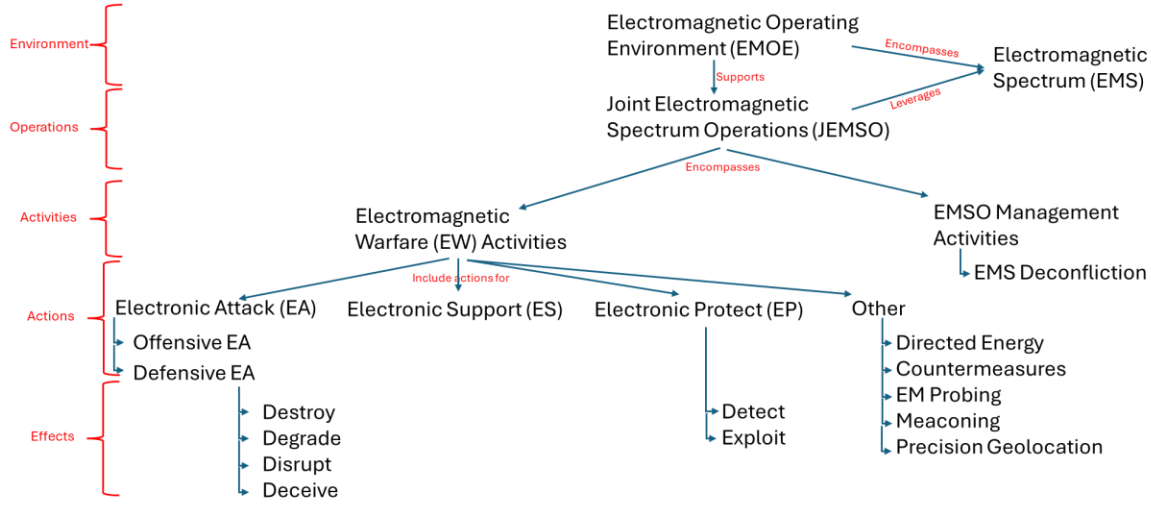



*Figure 1. Joint EMSO Doctrinal Terminology Hierarchy*

**Joint Cyber Doctrine Overview**

Within joint doctrine, cyberspace is part of the information environment and is dependent upon systems within the physical domains of air, land, maritime, and space. The information environment is an aggregation of individuals, organizations, and systems that collect, process, disseminate, or act on information. Cyberspace can best be described in terms of three interrelated layers consisting of the physical network, the logical network, and the cyber persona.

Cyberspace operations use network links and nodes within the physical domains, in conjunction with logical functions, to create effects first in cyberspace and then, as needed, in the physical domain. Distinction is made to differentiate cyberspace-enabled activities, which utilize cyberspace for their functionality, from cyber missions, which encompass offensive, defensive, and DODIN operations.

Within the delineation of cyberspace missions, defensive operations are further categorized into internal defensive measures (DCO-IDM) and response actions (DCO-RA), which are differentiated by system or network ownership. DCO-IDM occurs within the DODIN while DCO-RA occurs within external environments under the permission of the owner of the effected system or network.

Several cyberspace actions are further identified, which include cyberspace security, defense, exploitation, and attack. From these, only cyberspace attacks include further sub-categorization of manipulate and deny actions, the latter of which is broken down into degrade, disrupt, destroy, and deny effects.

Relating these terms together, we can present joint cyber doctrine and the hierarchical relationship of associated terminology as follows:

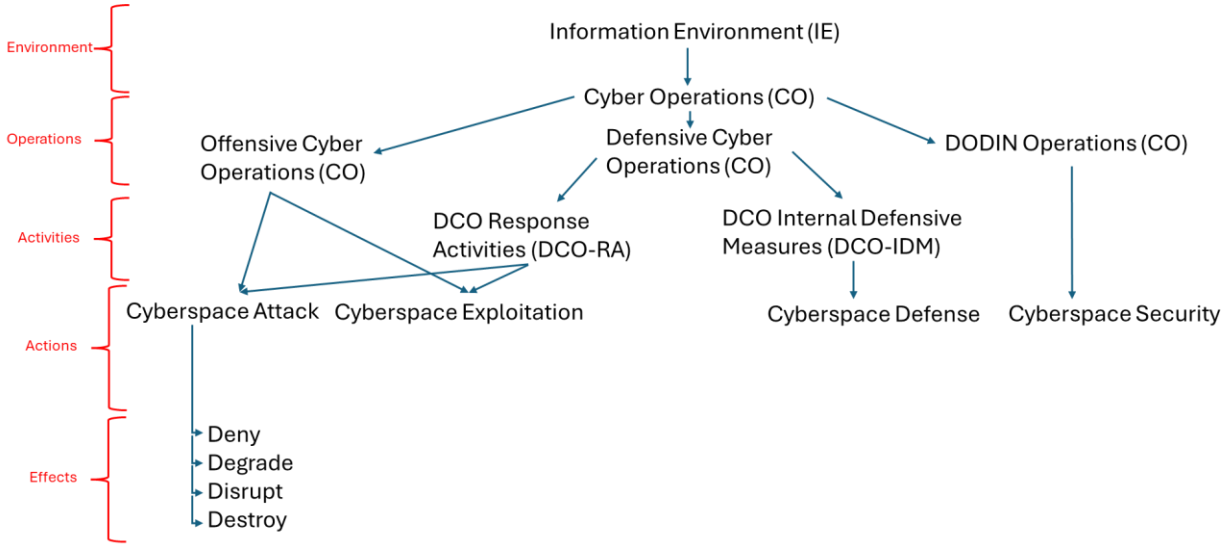



*Figure 2. Joint Cyber Doctrinal Terminology Hierarchy*

## Service Doctrine Deviations:

While joint doctrine serves as a common baseline of understanding to synchronize the services, we note several deviations related to each service, as follows:

**Army Doctrine Overview.**

The Army's doctrine for Electromagnetic Warfare (EW) and cyberspace operations reflects close alignment with joint doctrine[41] while emphasizing the theoretical integration of these domains under the concept of Cyberspace Electromagnetic Activities (CEMA). CEMA combines cyberspace operations (CO), electromagnetic warfare (EW), and spectrum management operations (SMO) into a single framework aimed at supporting maneuver warfare and dominance in contested information environments. Unique to the Army, CEMA cells serve as specialized organizational structures established at multiple echelons to plan, synchronize, and coordinate EW, CO, and SMO efforts. This organizational construct facilitates integrated planning with Joint Electromagnetic Spectrum Operations (JEMSO) and ensures the Army can adapt its operations to dynamic battlefield conditions.

Army doctrine also emphasizes the conceptual overlap between Electromagnetic Attack (EA) and cyberspace attack more than other services, particularly through its recognition of EA's potential to enable cyber effects. For instance, ATP 3-12.3[42] highlights actions such as injecting malicious data or probing system vulnerabilities via electromagnetic means, bridging the gap between traditional EW and cyber capabilities. This perspective stems from efforts like the 120-day study and the Starblazor report[43], which addressed the doctrinal and operational challenges of aligning EW and cyberspace operations. While these studies reflect a clear recognition of the complexity in synchronizing these domains, operational integration of EA and Offensive Cyberspace Operations (OCO) remains limited.

[41] A notable departure from Joint Doctrine is the Army's usage of the terms *friendly*, *threat*, and *neutral cyberspace*, to describe *blue*, *red*, *and gray cyberspace*, respectively (FM 3-12).
[42] ATP 3-12.3, *Electromagnetic Warfare Techniques* (Washington, DC, USA, 2023), https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1026337.
[43] U.S. Army Cyber Center of Excellence, "120-Day Study"; U.S. Army Cyber Center of Excellence, "Starblazor Report."

The Army's focus on spectrum management as a distinct pillar further sets its doctrine apart, enhancing planning and synchronization without driving the tactical convergence of EW and cyberspace operations.

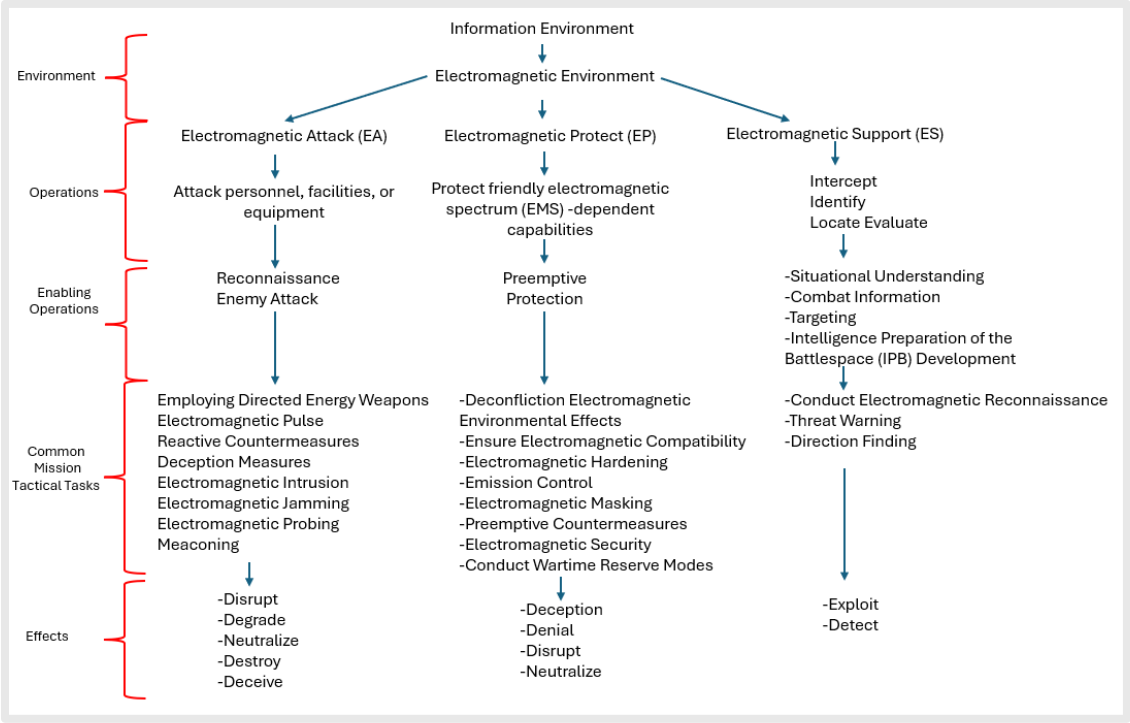



*Figure 3. Army EMSO Doctrinal Terminology Hierarchy*

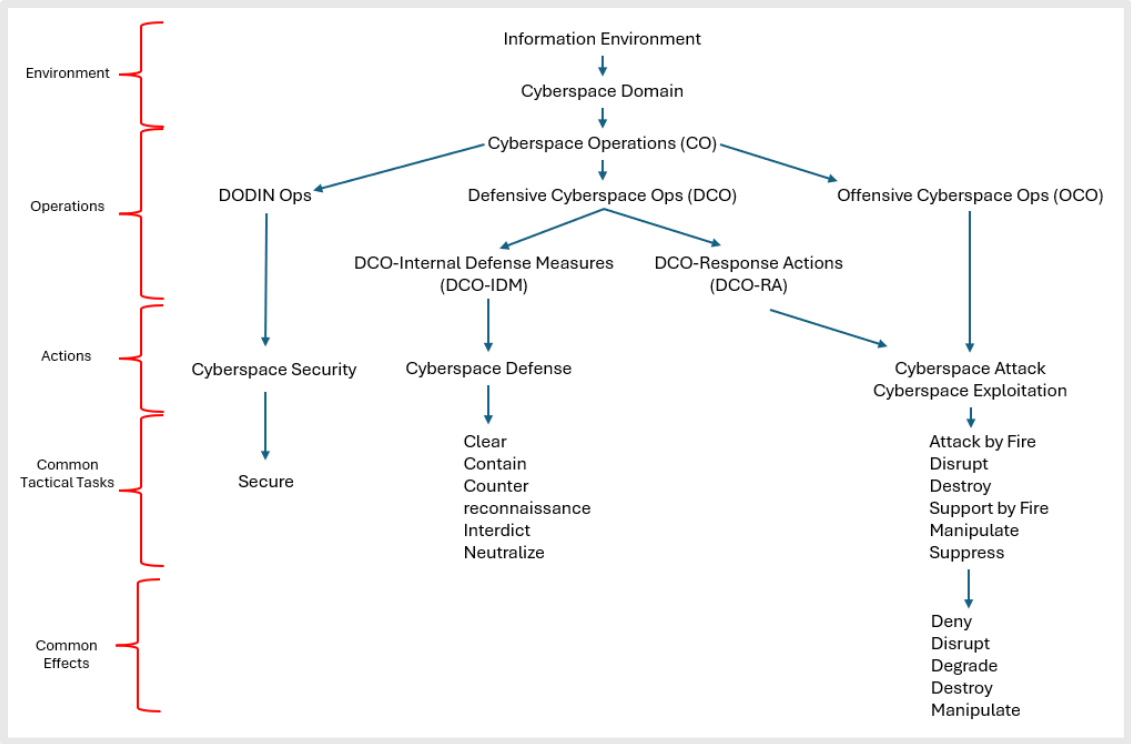



*Figure 4. Army Cyber Doctrinal Terminology Hierarchy*

**Air Force Doctrine Overview.**

The Air Force deviates from joint doctrine by tailoring EMSO terminology to emphasize its unique operations environment in the air domain. Terms such as *airborne electromagnetic attack, airborne offensive EA*, *airborne defensive EA/self-protect*, and *airborne electromagnetic support* reflect the Air Force's focus on integrating EW capabilities with airborne platforms to achieve air superiority.[44] These terms align closely with joint concepts but emphasize the Air Force's domain-specific operational needs rather than introducing fundamental new doctrinal concepts. They further extend EMSO to both offensive and defensive categorizations to ensure flexibility in operations across the air, space, and cyberspace domains, highlighting the importance of synchronization in contested environments.

The Air Force further expands joint doctrine on EW deception effects by distinguishing between *manipulative*, *simulative*, and *imitative effects*, offering additional nuance to the use of EMS to achieve deception. [45] Manipulative effects, for example, involve influencing communication signals to convey threat activity on adversary systems, providing a potential avenue for shaping the information environment.[46] However, the details of how these effects are applied in theater remain intentionally vague, contrasting with the Army's stronger emphasis on data delivery over the EMS. This abstraction reflects the Air Force's focus on leveraging advanced airborne platforms and cross-domain capabilities, maintaining doctrinal flexibility while emphasizing operational agility in highly dynamic EMS environments.

[44] *AFDP 3-85*, 11–13.
[45] *AFDP 3-85*, 8–9.
[46] *AFDP 3-85*, 9.

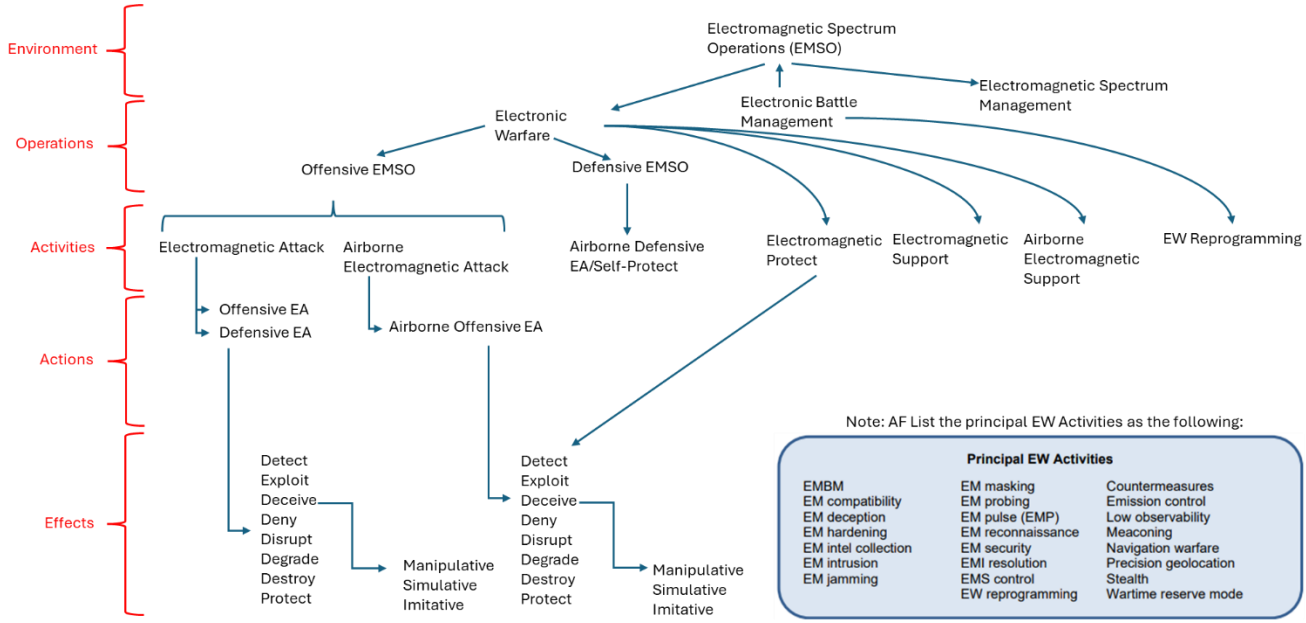



*Figure 5. Air Force EMSO Doctrinal Terminology Hierarchy*[47]

[47] *AFDP 3-85*, 7 (Chart).

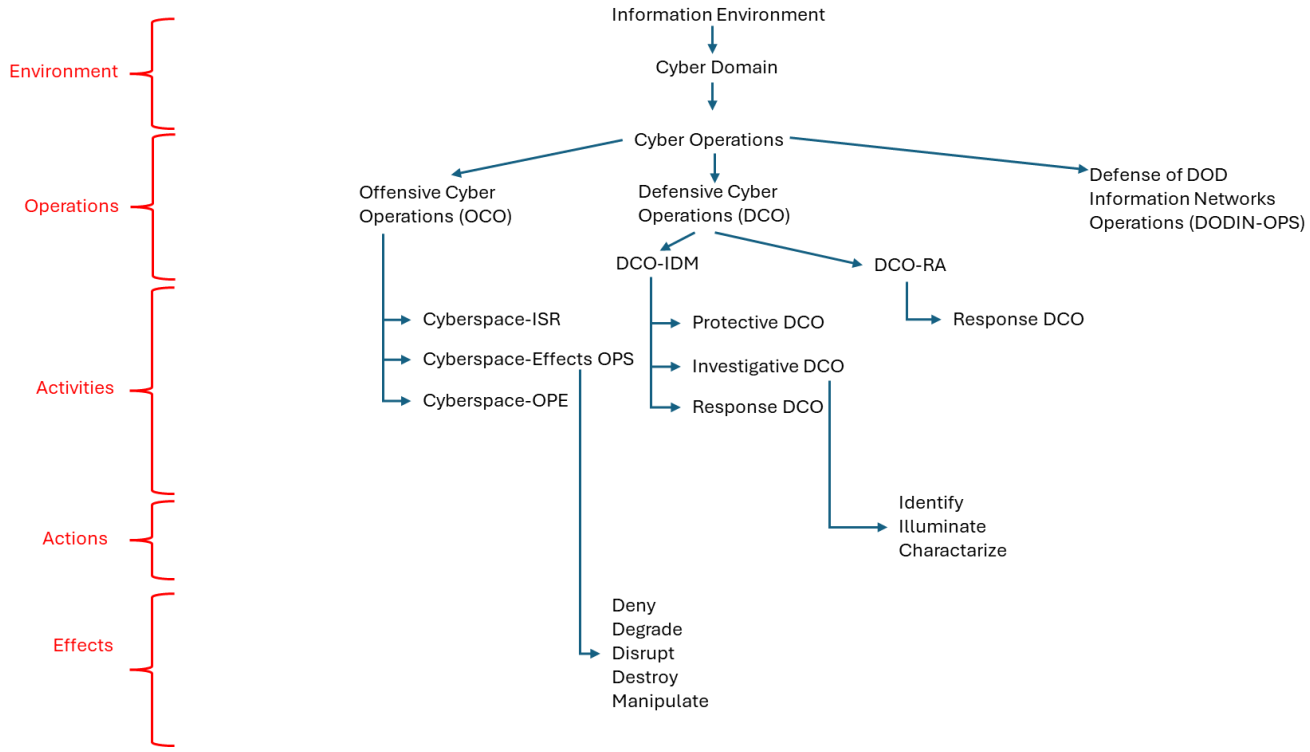



*Figure 6. Air Force Cyber Doctrinal Terminology Hierarchy*

**Space Force Doctrine Overview**

Like the Air Force, Space force suffers from precision of terminology and boundaries (e.g., conflating traditional DODIN network operations, such as "traffic monitoring," as a cyberspace capability or defining "spoofing" solely as an Electromagnetic Attack measure by which false data is injected into communication systems, for example). Their doctrine tends to favor the target and domain in which the effect is manifesting in as boundaries between OCO and EA. More precisely stated, EA are effects manifesting solely in the EM environment, while OCO may leverage EA towards a target, the end target effect always manifests in the cyber domain. Again, this very limited approach ignores the more nuanced understanding and opportunity that EA can deliver. This is possibly a result of the very nascent state of most of the cyber doctrine and a possible approach to quickly establish baseline understanding for the service, recognizing a need for further refinement later.

(No terminology hierarchy graphics due to lacking material information)

**Navy Doctrine Overview.**

Relevant Navy doctrine addressing EW and cyberspace operations emphasize their integration at all echelons under the umbrella multi-domain concept of *"information warfare (IW)*" (NDP-1). Army and Joint doctrine tend to treat these domains as distinct but interrelated, with specific roles and authorities assigned to each, but the Navy does not. A key concept driving consolidation of effects irrespective of domain is the Naval strategy of *battlespace dominance*, with the *battlespace* representing all domains relevant to the area of operations and essential mission tasks. The Navy views agility and

synchronization of capabilities as the most important characteristics for gaining tactical advantage and maintaining superiority within the operational environment.

Another term unique to the Navy that embodies this approach of convergence is *electromagnetic maneuver warfare (EMW)*, which is the Navy's warfighting approach to dominate the EMS, which it views as essential to enable freedom of action in all Navy mission areas (NTP 6(F)). In its model, EA/ES/EP are the three functions of EMW's operational arm, known as *electromagnetic spectrum operations (EMSO)*, along with spectrum management/operations, and meteorology and oceanography capabilities. Navy doctrine is written in a way to maximize flexibility during complex, multi-domain operations, and thus avoids being overly prescriptive in distinguishing between EW and Cyberspace operations. The Navy's EMW Concept embodies the interplay between EW and cyberspace, viewing them as one fluid information environment that is in constant flux and key to securing maritime superiority and control.

(No terminology hierarchy graphics due to source classifications)

**Marine Corps Doctrine Overview.**

Like the Navy, the USMC emphasizes the integration of EW and cyber within the broader scope of its *maneuver warfare* philosophy. The USMC's doctrine prioritizes rapid adaptability and operational flexibility, with a strong focus on the *Marine Air-Ground Task Force* (MAGTF) structure, where EW and OCO are seen as complementary capabilities that enhance overall maneuver and command-and-control (C2) capabilities. Marines focus on exploiting information and EW to create battlefield advantages that align with its expeditionary mindset, heavily emphasizing the importance of information superiority and agile coordination of effects between EW and cyber at all echelons, with primary emphasis on small-unit operations.

Marine doctrine allows for EW and CO to dynamically interact, with EW assets providing direct support for CO through localized EMS denial, while CO might be employed to disrupt enemy EMS-reliant C2 systems. Marine doctrine emphasizes the importance of speed to seize tactical advantages in highly contested information environments. The Marine Corps views ground-based EW capabilities as essential for enhancing the lethality and survivability of MAGTF forces in such conditions.

(No terminology hierarchy graphics due to source classifications)

**Intel (NSA/Army SIGINT) Doctrine Overview.**

NSA policy does not describe terms related to electromagnetic effects but focuses solely on legal aspects when conducting "electronic surveillance."[48] The reviewed policies describe NSAs mission to conduct Signals Intelligence (SIGINT) activities (including electronic surveillance), intelligence oversight responsibilities, and the legal process required to conduct these activities to protect U.S. citizens' fourth amendment rights.

Further reading into National and Army based signal intelligence (SIGINT) publications focuses on differences between Electromagnetic Support (ES) and SIGINT. Documents such as ATCAE Pub 3-13

[48] National Security Agency, "NSA/CSS POLICY 12-3: Protection of Civil Liberties and Privacy of U.S. Person Information When Conducting NSA/CSS Mission and Mission-Related Activities" (Department of Defense, February 15, 2022), https://media.defense.gov/2022/Feb/22/2002942549/-1/-1/0/NSA_CSS_POLICY_12-3_SIG_20220215.PDF.

and USSID 305 attempt to clarify the authority process for leadership, and they describe the differences between SIGINT and ES as a function of who is tasking the asset, what purpose the asset is tasked for, and what product the asset is providing. There is minimal discussion of effects other than that both SIGINT and ES can provide support to EA operations.

**NATO Doctrine Overview.**

The Electromagnetic Environment (EME) is considered a distinct environment from cyberspace. The most prominent overlap is when Electromagnetic missions and operations (EMO) support cyberspace operations through the EMS as a physical layer (AJP-3.6, p2-6). While NATO strictly adheres to conducting defensively aimed cyberspace operations, OCO can be conducted through Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions (SCEPVA) (AJP-3.20, p17, and Enclosure 1 to MCM-0112-2018). ATP-3.6.2 V1 Draft B implies Electromagnetic Activities consist primarily of applying directed energy. However, the EW actions described to “achieve effects” are not strictly bound and can require more advanced techniques than directed energy. This doctrine also stresses that all users of the EME are accountable for Electromagnetic Defence, which desired effects include deny, degrade, disrupt, protect, deceive, and neutralize.

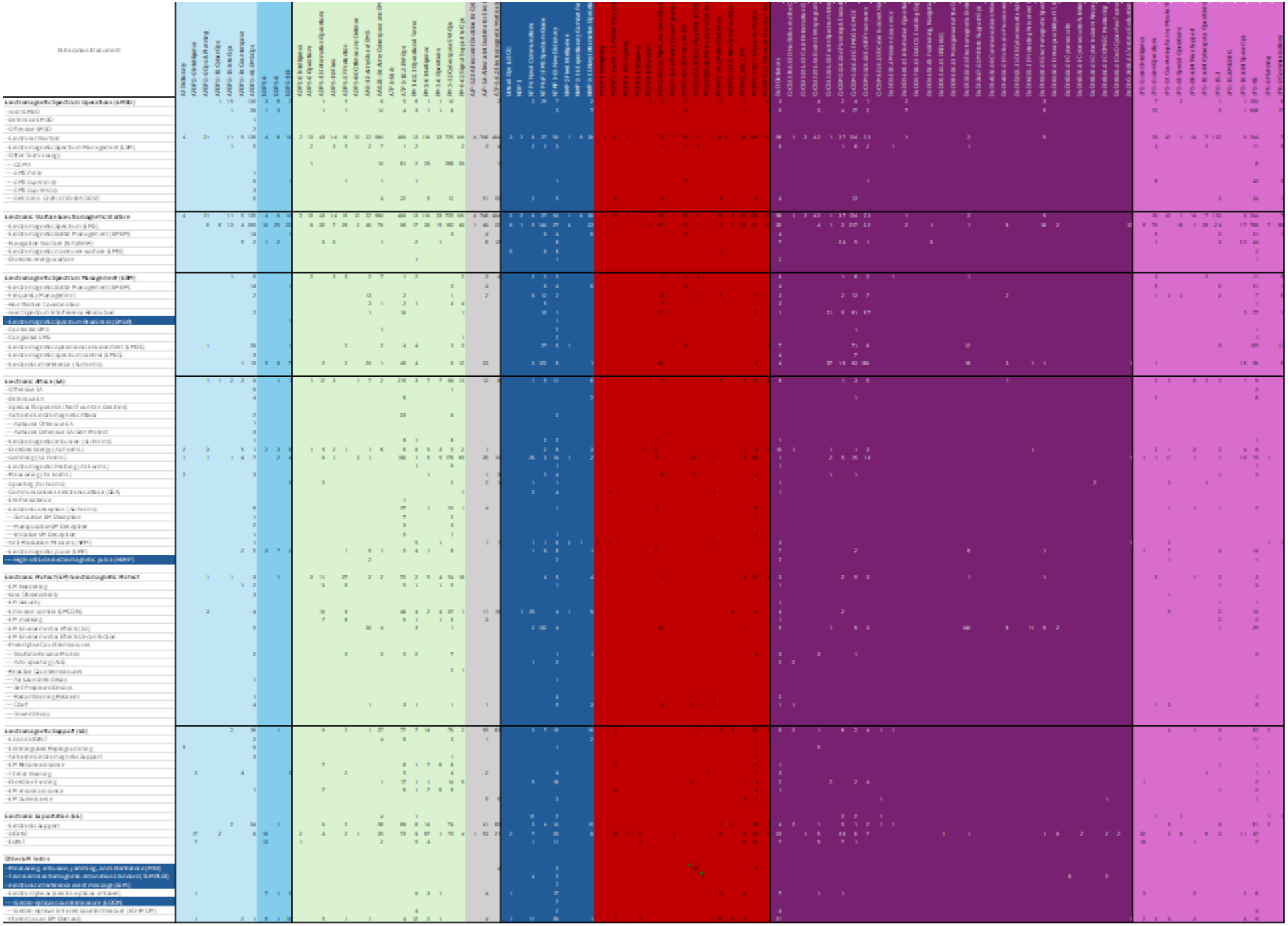
*Note: The United States holds reservations against current cyber and EA NATO doctrine with the use of specific terms, including achieving effects, international vs humanitarian law, and other terms not explicitly agreed upon by NATO.*

# Section III: Supporting Data Products

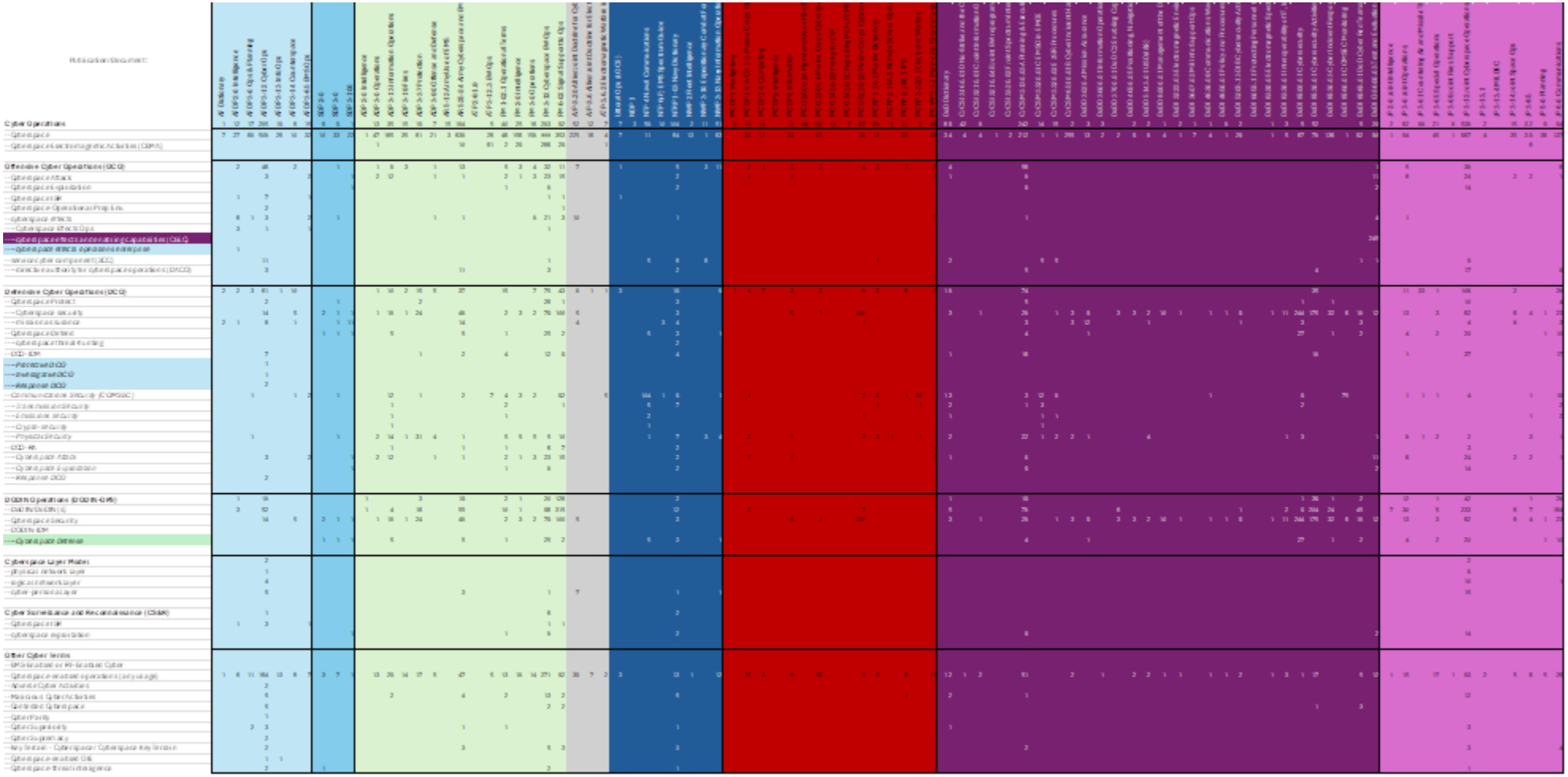
## Item A: Terminology Identification and Occurrences

The following three tables highlight the terminology surrounding electromagnetic warfare and cyber within doctrine, and their occurrence by service and publication. The following tables are also included in the associated “Terminology.xlsx” spreadsheet for easier and interactive viewing.

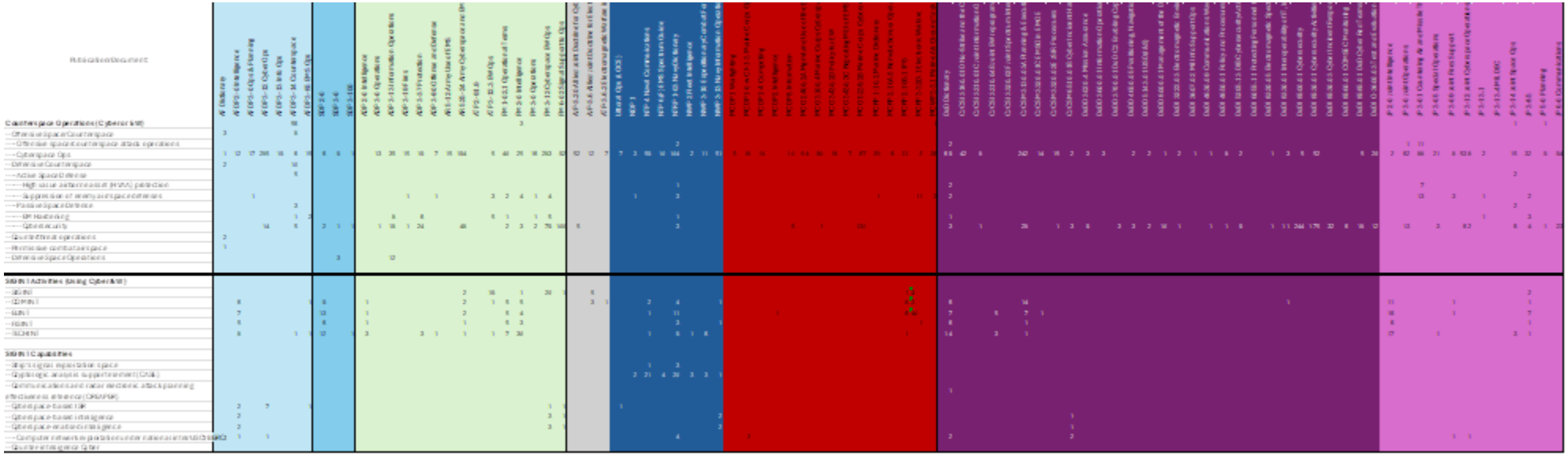
## Table 1: Electromagnetic Warfare Terminology and Doctrinal Usage Count



## Table 2: Cyber Terminology and Doctrinal Usage Count



## Table 3: Counterspace and Intel-Related Cyber and EW Doctrinal Usage Count



# Item B: EA and Cyber Attack Doctrinal Language and Phrasing

Below are select terminology and phrasing pulled from doctrine which were studied to understand usage, current bounds of definitions, and opportunity to either leverage or develop terminology based on broad service usage and possible need. All segments are quoted from the primary reference doctrine publication. We present these here for quick reference.

**Joint Cyber Doctrine (Primarily JP 3-12):**

“Cyberspace attack capabilities create fires in and through cyberspace and are often employed with little or no associated physical destruction. However, modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domains."

“Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains. Unlike cyberspace exploitation actions, which are often intended to remain clandestine to be effective, cyberspace attack actions will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.”

“Manipulation, as a form of cyberspace attack, controls or changes information, information systems, and/or networks in gray or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques.”

“Countermeasures …in support of an OCO mission, they may be cyberspace attack actions that spoof or otherwise negate the effectiveness of adversary sensors or defenses. As part of a DCO-RA mission, they may be used to identify the source of a threat and/or use non-intrusive or minimally intrusive techniques to interdict or mitigate threats.”

“Cyberspace attack capabilities create fires in and through cyberspace and are often employed with little or no associated physical destruction. Even if effects can be created independently and are sufficiently justified, a technical analysis is still required to determine if the capabilities can operate as planned in the same environment without interference or increasing the chances of unwanted detection.”

“Because CO can often be executed remotely, through a virtual presence enabled by wired or wireless access, many CO do not require physical proximity to the target but use remote actions to create effects, which represents an increase in operational reach not available in the physical domains.”

**Joint Electromagnetic Warfare Doctrine (Primarily JP 3-85):**

“Offensive EA describes the use of EA to project power in support of operations within the time and tempo of the scheme of maneuver. In many cases, these activities suppress a threat for only a limited period of time. Examples include employing self-propelled decoys; jamming radar or C2 systems; using antiradiation missiles to suppress air defenses; using EM deception techniques to confuse intelligence, surveillance, and reconnaissance (ISR) systems; and using DE weapons to disable personnel, facilities, or equipment and disable or destroy materiel (e.g., satellites in orbit, airborne optical sensors, or massed land forces). “

"EA is the … use of EM energy, including DE or antiradiation weapons, to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Typical EA capabilities include EM jamming and intrusion. EM intrusion involves the intentional insertion of EM energy into transmission paths to deceive or confuse enemy forces."

"Electromagnetic attack (EA) systems, to include directed energy (DE) (e.g., radio frequency [RF] jammers, laser dazzlers, millimeter wave, microwave capabilities), that transmit energy through the EMOE to disrupt or degrade an enemy's ability to receive signals, deliver data payloads supporting cyberspace operations (CO), or disable and destroy targets (e.g., electronics of vehicles, vessels, and unmanned aircraft systems' control modules) susceptible to high-energy EM radiation."

**Army Cyber Doctrine (Primarily FM 3-12):**

"Cyberspace attacks deny the enemy's ability to access cyberspace by hindering hardware and software functionalities for a specific duration of time."

"Commanders can use cyberspace attacks that temporarily but completely deny an enemy's ability to access cyberspace or communication links to disrupt decision making, ability to organize formations, and conduct command and control."

"Manipulation, as a form of cyberspace attack, controls or changes information, information systems, and/or networks in gray or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques."

**Army Electromagnetic Warfare Doctrine (Primarily FM 3-12):**

"Electromagnetic attack is a division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and considered a form of fires." (Note: borrowed from JP 3-85 definition.)

"EA requires systems or weapons that radiate electromagnetic energy as active measures and systems that do not radiate or re-radiate electromagnetic energy as passive measures."

"EA Deception Measures: Electromagnetic deception uses misleading information by injecting false data into the adversary's EMS-dependent voice and data networks to inhibit the effectiveness of intelligence, surveillance, and reconnaissance sensor systems."

"Electromagnetic Intrusion: is the intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. (FM 3-85) (Borrowed from JP 3-85.) Electromagnetic intrusion can also create deception or confusion in a threat aircraft's intelligent flight control system..."

"Electromagnetic Probing: Electromagnetic probing is the intentional radiation designed to be introduced into the devices or systems of an adversary for the purpose of learning the functions and operational capabilities of the devices or systems. Electromagnetic probing involves accessing an enemy's spectrum-dependent devices to obtain information about the targeted devices' functions, capabilities, and purpose."

"Three types of EW deception:
*Simulative* - Simulative electromagnetic deception attempts to represent friendly notional or actual capabilities to mislead threat forces. Simulative electromagnetic deception includes the use of systems that give off emissions indicative of a particular organization.

*Manipulative* - Manipulative electromagnetic deception uses communication or noncommunication signals to convey indicators that mislead the enemy. Manipulative electromagnetic deception seeks to eliminate, reveal, or convey misleading indicators of friendly intentions.

*Imitative* - Imitative deception mimics threat emissions with the intent to mislead them. Imitative deception normally requires approval from higher echelon commands since it risks compromising friendly SIGINT efforts. Imitative deception presents false information to the threat and affects decision making. Imitative electromagnetic deception requires equipment capable of convincingly duplicating the emissions of enemy equipment to be effective." (ATP 3-12.3)

**Air Force Cyber Doctrine (Primarily AFDP 3-12):**

"OCO may exclusively target enemy cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading denial effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, and other high-value targets. All cyberspace operations missions conducted outside of blue cyberspace with intent other than defending blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions."

"OCO may create effects on adversary systems across multiple domains. Effects may be temporary, long-term, or permanent. By design, OCO may exclusively target adversary cyberspace functions or create cyberspace effects with manifestations in physical domains"

"Cyberspace Effects Operations: Cyberspace actions that create various direct effects in cyberspace and manipulations that can manifest as denial actions in the physical domains"

"Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."

"Cyberspace attacks may disrupt or deny space-based or terrestrial-based computing functions used to conduct or support satellite operations and to collect, process, and disseminate mission data." (AFDP 3-14)

Offensive Counterspace Operations are undertaken to negate an adversary's use of space capabilities. These operations target an adversary's space capabilities (space, link, and ground segments, or services provided by third parties), using a variety of reversible and non-reversible means." (AFDP 3-14)

**Air Force Electronic Warfare Doctrine:**

"EW...is waged to secure freedom of action in portions of the electromagnetic spectrum.... It can create significant standalone effects....by generating various levels of control, denial, detection, exploitations, and related effects through the EMS." (AFDP 3-0)

"EMSO are coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment to achieve the commander's objectives. Electromagnetic warfare (EW) is both a type of fires and an enabling capability." (AFDP 3-13)

"EMSO contributes to the success of OIE by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EMS while protecting friendly freedom of action." (AFDP 3-14)

"RF weapons concepts include ground and space-based RF emitters that fire highpower bursts of EM energy at a satellite, imparting disruptive EM fields into the wiring and electrical components in order to upset and possibly damage the computer processing subsystems." (AFDP 3-14)

"Offensive EMSO are used to deceive, disrupt, degrade, or destroy the enemy's ability to use the EMS." (AFDP 3-85)

"EW encompasses military actions using electromagnetic and directed energy (DE) to control the EMS or to attack the enemy. This includes radio or radar frequencies, IR, visible, ultraviolet, and any other free-space electromagnetic radiation such as wireless cyberspace applications." (AFDP 3-85)

"Most EMS activities occur outside of cyberspace; however, many CO require the use of the EMS to establish a communications path to the targets, especially at the tactical level." (AFDP 3-85)

**Space Force Cyber Doctrine:**

**"**Cyberspace attacks can target any of the three segments of a space system by targeting transmitted data or the terrestrial or orbital systems that use or collect the data, or that maintain the operations of the spacecraft." (SFDP 3-100)

"Operators and cyberspace capabilities can detect, observe, and report indications of electromagnetic interference or issues with link integrity through network monitoring (e.g., data packet loss)." (SFDP 3-100)

"Due to the distributed nature of space operations, all space operations are simultaneously cyberspace operations and EMS operations." (SFDP 3-0)

**Space Force Electromagnetic Warfare Doctrine:**

"Electromagnetic warfare assets can monitor the electromagnetic spectrum to detect and characterize electromagnetic interference." (SFDP 3-100)

"Spoofing is a form of electromagnetic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is the real signal it is trying to receive. Adversaries can spoof the downlink from a spacecraft to inject false or corrupted data into communications systems." (SFDP 3-100)

**Navy Electromagnetic and Cyber Doctrine:**

*Note: Most Navy and Marine Corps doctrine is located in the classified domain. While the majority of the associated doctrine is not classified, we exclude from this section to prevent derivative documentation requirements except for select unclassified doctrine phrases of interest.*

**Marine Corps Electronic Warfare:**

"The Marine Corps approach to EMSO reflects a five-element design. This design provides the intellectual foundation for how the Marine Corps approaches EMSO to maintain EMS superiority in a congested, contested, and competitive EMOE. (a) Network-enabled systems. (b) Networks and connectivity. (c) Common data sources and formats. (d) Common service framework. (e) Common user environment."

"Marines must also use their creativity and find innovative ways to combine new technology with legacy capabilities for maximum effect. This is particularly true in rapidly changing high-tech areas such as cyberspace, electromagnetic spectrum operations, and space-based capabilities. It is up to the commander and staff to combine these capabilities with fires, maneuver, and relevant partner activities to adhere to our combined arms and maneuver warfare philosophy. " (MCDP 8)

**NATO Electromagnetic Warfare Doctrine:**

"Electronic attack (EA) involves the use of electromagnetic (EM) energy for offensive purposes. EA includes capabilities that can limit an enemy's ability to operate in the EME. In addition, EA capabilities project power through the EME to neutralize an enemy. Typical EW capabilities of

EA include jamming, deception and neutralization. EA can be employed to degrade, disrupt, deceive, destroy or deny an adversary's or enemy's ability to conduct EMO; attack their command and control (C2) systems; deny their intelligence, surveillance and reconnaissance (ISR) capabilities; disrupt computer equipment; destroy system equipment and diminish adversaries' or enemies' opportunities to shape or exploit the operating environment." (AJP-3.6, 3.5 & 3.5.1)

"EW actions are divided into the following tasks:

(a) Monitor. To survey a dedicated part of the EMS and record activities within it.

(b) Detect. Discovering the presence of electromagnetic emissions.

(c) Identify. The determination of the origin, nature and characteristics of emissions.

(d) Locate. Determining the position of specified emitters of interest.

(e) Report. A written or spoken account of the result of an executed task or an observed situation.

(f) Analyse. An investigation of electromagnetic radiations to determine their tactical significance and imminent operational use.

(g) Imitate. The transmission of messages or signals in the enemy's wireless communication channels with the intention of deceiving the enemy.

(h) Spoof. Creation of false targets primarily used for deception.

(i) Jam. Radiation, reradiation or reflection of EM energy with object to deny effective use of an adversary's EM dependent equipment or systems." (ATP-3.6.2 DRAFT B, 1.4.3)"

"Applicable EW Actions in support of Offensive Operations:

- EA can prevent the enemy from communicating over specific networks and force them to communicate over networks which can be intercepted by friendly force ES systems (herding).
- EA can target media networks to prevent an enemy from disseminating information adverse to friendly forces and preventing the spreading of misinformation.
- EA can target land-based air defence systems to enable air assets supporting land operations.
- EA can reduce the detection range and accuracy of EM dependent weapon systems reducing threats to NATO Land forces.
- EA can overwhelm the optics devices on enemy weapon systems to prevent observation of friendly force units.
- EA can target enemy C2 nodes severing the flow of communication from all enemy command echelons.
- EA can reduce the enemy's ability to use EM-dependent surveillance, positioning, and navigation systems.

- EA capabilities such as lasers and high-power microwaves used against enemy electronic equipment which does not depend on the usage of the EME but is an integral component of their systems' electronic hardware.
- EA can conduct masking to shape an enemy's perception of friendly force operations such that they react in a manner supporting friendly force objectives." (AJP-3.6.2 DRAFT B, 2.3.1-3)

**NATO Cyber Doctrine:**

"NATO cyberspace operations are solely defensive in nature and focus on protecting NATO's mission networks. EW contributes to this defence by enabling freedom of maneuver through the EME for uninterrupted service of the mission networks." (AJP-3.6 4.14 & 4.15)

# Item C: Terminology Distinguishing Words and Phrases

**Overview of EA/Cyber & Related Doctrine**

A survey of joint and service-specific military doctrine and terminology reveal a variety of unique considerations for the application of EW and cyberspace capabilities, with the Joint Publications (JP) serving as a common terminology foundation. Analyzing the definitions of each term within their wide diversity of applications reveals four key areas of distinction. Existing doctrine distinguishes EA and OCO by domain environment, method of application, target characteristics, and military objective. To highlight these differences, we analyzed the existing definition for each action from Joint doctrine using these four metrics. We then looked at unique considerations within each military service branch and allied doctrine before delving into areas of overlap and ambiguity that a framework would necessarily have to address.

**Electromagnetic Attack.**

***Definition:*** *"Division of electromagnetic warfare involving the use of* electromagnetic energy, *directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires." (JP 3-85)*

***Distinguishing features:***

1. **Domain.** The most fundamental characteristic of EA is that it occurs within the EMS operational environment. Because EA is identified first as a *division of electromagnetic warfare* (e.g., a type of military action leveraging the EMS), we can conclude that EA cannot occur without direct interaction with the EMS.
2. **Method.** EA leverages or manipulates electromagnetic energy to affect the target, which includes types of directed energy (DE) (e.g., a beam of EMS energy, atomic, or subatomic particles) and antiradiation weapons (e.g., anti-radiation missile (ARM), etc.).
3. **Target(s).** Because the attack occurs over the EMS, its primary targets are systems that leverage or rely on the EMS, which includes personnel (e.g., who are sensitive to

fluctuations in light, sound, heat, etc.), facilities, and equipment (which use a variety of sensors and telemetry for capabilities, command & control, communications, etc.)

4. **Objective.** EA seeks to deceive, disrupt, degrade, or destroy the enemy's ability to use the EMS to affect their operations and enable friendly freedom of maneuver in the information environment.

***Related Characteristics (Pulled from service doctrine phrases):***

- Requires radiation of electromagnetic or directed energy.
- Can be used to learn functions and capabilities of systems through probing mechanisms (Army).
- Can Destroy, Degrade, Disable, Disrupt, Deceive enemy EMS-dependent systems.
- Can deliver data payloads supporting cyberspace operations
- Assist in compromising availability and integrity of modulated data traversing EMOE
- Passive or active
- Limits enemy's ability to operate in EME (NATO)
- Project power through the EME (NATO)
- Most occur outside of cyberspace (Air Force)
- Can target media networks to prevent information dissemination (NATO)
- Can sever C2 nodes disrupting information flow (NATO)

**Offensive Cyberspace Operations.**

***Definition:*** ***"****Cyberspace operations intended to project power by the application of force in or through cyberspace." (JP 3-12)*

***Distinguishing features:***

1. **Domain.** OCO is conducted within the cyberspace domain, which is distinct from the EMS. Cyberspace is defined as a global domain within the information environment, consisting of interconnected networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors (JP 3-12, FM 3-0). Unlike EA, which directly interacts with the EMS, OCO is confined to digital networks and software systems, even if their second and third order effects cascade into other domain environments.

2. **Method.** OCO employs actions in cyberspace to achieve desired effects by applying force through cyber means. This includes techniques such as exploiting vulnerabilities in software, penetrating networks, and altering or manipulating information in cyberspace. These methods differ from EA in that they do not rely on electromagnetic energy or physical force but instead focus on using cyber capabilities to disrupt or degrade adversary operations. Though, it is important to recognize that portion of the path to the intended target may cross EMS boundaries (e.g., Wi-Fi connectivity to target, etc.).

3. **Target(s).** The targets of OCO are entities operating in or through cyberspace. This could include information systems, databases, or networked infrastructure that are essential for command and control, communication, and other critical functions. Unlike

EA, which targets equipment or systems relying on the EMS, OCO focuses on digital environments where adversaries' cyber capabilities or information systems are housed.

4. **Objective.** The primary objective of OCO is to project power by applying force in or through cyberspace. This can involve denying, degrading, disrupting, or destroying information or systems vital to an adversary's operational capabilities, much like EA's goal in the EMS. However, the key distinction is that OCO seeks to influence or control the cyber domain, achieving outcomes that impair adversary operations by manipulating their digital infrastructure. Because power projection often has strategic and geopolitical implications, cyberspace operations are often planned, executed, and authorized at higher echelons than EA actions.

***Related Characteristics:***

- Often employed with little or no associated physical destruction
- Can modify or destroy computers that control physical processes
- Effects apparent to system operators or users, either immediately or eventually.
- Require technical analysis to determine if capabilities can operate as planned and without interference.
- Hinders hardware and software functionalities (Army)
- Control enemy ability to access cyberspace (Army)
- May cause irreversible corruption, loss of data and information, or physical damage to hardware. (Army)
- Conducted outside of blue space (AF, Navy)
- Exclusively targets cyberspace functions or creates first-order effects in cyberspace (Air Force & Navy)
- Temporary, long-term, permanent effects (Air Force)
- May disrupt or deny space-based or terrestrial based computing functions
- May rise to the level of use of force with physical damage or destruction

# Part III – Glossary and Consolidated List of References

# Appendix F - Glossary of Electromagnetic Warfare and Cyberspace Operations Terminology

*The following terms and definitions are provided for reference and sourced directly from Joint Cyberspace and Electromagnetic Warfare Publications (current at the time of writing). These include doctrinal texts from the U.S. Department of Defense, Joint Chiefs of Staff, the service branches, and NATO. Variations in the usage of certain terms (e.g., cyber/cyberspace, electronic/electromagnetic, cybersecurity/cyberspace security, etc.) are retained as presented in the source material. See Appendix G for complete reference citations of each publication. This glossary includes terms not used in this report and serves as a byproduct of near-exhaustive research of joint and service doctrine as it relates to Offensive Cyber and Electromagnetic Warfare.*

***active electronic countermeasures —*** The impairment of enemy electronic detection, control, or communications devices/systems through deliberate jamming or deception. (NTRP 1-03)

***adverse cyber activities (ACA) —*** The Air Force term for friendly actions or natural events, disasters, or accidents that inadvertently achieve the same effects as malicious cyberspace activity (AFDP 3-12)

***Air Force information networks (AFIN) —*** The set of Air Force information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, 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." Derived from JP 6-0, Joint Communications System, and Department of the Air Force Policy Directive (DAFPD) 17-2, Cyber Warfare Operations. (AFDP 3-12)

***airborne defensive electromagnetic attack/self-protect (DEA/SP) —*** Activities [that] use onboard EA with electromagnetic-type countermeasures. There may be DEA/SP capabilities that can provide survival benefits for other aircraft (e.g., chaff corridors or self-protection jammers) but generally, airborne DEA/SP equipment is developed to provide platform self-protection. Examples of defensive airborne EA are: Radar Warning Receivers, Chaff, DE, Towed Decoys, Low observable technologies. (AFDP 3-85)

***airborne electromagnetic attack —*** The objective of airborne EA is to use offensive EA to mitigate an enemy's EMSO capability, therefore enabling joint force operations. (AFDP 3-85)

***airborne electromagnetic support —*** [Airborne] ES identifies, locates, and reports enemy threats and positions in near-real time (NRT) to C2 and warfighters to support decision making and employ effects. Enemy reactions are monitored to provide battlespace awareness to friendly forces and imminent threat warning (ITW). (AFDP 3-85)

***airborne offensive electromagnetic attack —*** Typically, offensive EA (off-board EA) is employed by air assets in a supporting role to operations, e.g., escort jamming for a strike package. However, offensive EA aircraft can be the supported asset when tasked to strike targets. In supporting joint forces, offensive airborne EA should focus on any exploitable domain EMS node or pathway. This includes enemy communications, enemy radars and ground based-space facilities, and missile warning radars. Examples of offensive airborne EA systems are: Electromagnetic jamming, Anti-Radiation Missiles, Air-launched decoys, Electromagnetic Intrusion, Meaconing, EMP, DE. (AFDP 3-85)

***all-domain —*** Pertaining to all the physical domains (land, maritime, air, and space) and cyberspace. (JP 1, Vol 1) (DoD Dictionary)

***anti-radiation missiles —*** A missile which homes passively on a radiation source. Also called ARM. See also guided missile. (JP 3-01) (DoD Dictionary)

***anti-satellite (ASAT) weapons —*** Weapons capable of destroying or degrading spacecraft and spacecraft components and/or denying or disrupting their capabilities. There are two basic types. Direct ascent systems are best visualized as being "surface-to-space missiles," while on-orbit ASAT systems are also possible. ASATs may cause structural damage by impacting the target. Even small projectiles can inflict substantial damage or destroy a satellite. More advanced ASAT weapons could employ proximity operations and robotic arms to seize target satellites or use stand-off capabilities such as EA and DE. (AFDP 3-14)

***battle damage assessment —*** The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of fires. Also called BDA. See also combat assessment. (JP 3-0)

***blue cyberspace —*** Denotes areas in cyberspace protected by: The United States and its mission partners. Other areas that the DoD may be ordered to protect. (DoDI O-3600.03) Note. Army doctrine refers to this as *friendly cyberspace*.

***chaff —*** Radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion purposes. (JP 3-85)

***communications contested environment —*** An environment where the adversary use of electronic attack restricts the freedom to operate, and communicate, impacting the transfer of information from one person or place to another via the electromagnetic spectrum or cyberspace, by restricting or denying the use of systems or services such as satellite spoofing and data link denial or degradation, to include communications/Global Positioning System jamming and spoofing and data link denial or degradation. (NTRP 1-03)

***communications intelligence —*** Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT. (JP 2-0) (DoD Dictionary)

***communications security —*** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. (JP 6-0) (DoD Dictionary)

***communications security monitoring —*** The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis to determine the degree of security being provided to those transmissions. (AR 525-24)

***computer network attack (CNA) —*** The division of computer network operations that uses computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-09)

***computer network exploitation (CNE) —*** Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. See FLTCYBERCOM (FCC): Fleet cyber command. (NTRP 1-03)

***congested electromagnetic spectrum —*** [Resulting] congestion as commercial users, adversaries, partners, and United States electromagnetic spectrum-enables systems saturate available bandwidth and constrain maneuver within the electromagnetic spectrum. (NTRP 1-03)

***contested cyberspace —*** Circumstances in which one or more adversaries attempt to change the outcome of a mission by denying, degrading, disrupting, manipulating, or destroying capabilities in cyberspace, or by altering the usage, production, or confidence in those capabilities. (AFDP 3-12)

***contested electromagnetic spectrum —*** The competition for bandwidth coupled with easy access to sophisticated technology increases the likelihood of an adversary intentionally obstructing freedom of maneuver within the electromagnetic spectrum to disrupt joint operations. (NTRP 1-03)

***countermeasures —*** That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. See also *electromagnetic warfare.* (JP 3-85) (DoD Dictionary)

***counterspace —*** A mission that integrates offensive and defensive operations to attain and maintain the desired control and protection in and through space. (AFDP 3-14) (Air Force Glossary)

***counterthreat operations —*** The Air Force Office of Special Investigations capability to find, fix, track, and neutralize enemy threats in order to create a sustained permissive environment for air, space, and cyberspace operations. Also called CTO. (AFTTP 310.3) (Air Force Glossary)

***cryptological analysis support element (CASE) —*** The cryptologic resource coordinator staff resident within the strike group. Led by the cryptologic resource coordinator and assistant cryptologic resource coordinator, the cryptological analysis support element assists the cryptologic resource coordinator with monitoring the strike group collection and reporting to include health and status of organic, theater, and national signals intelligence systems. (NTRP 1-03)

***cyber operations (space) —*** Knowledge to defend the global networks upon which military Spacepower is vitally dependent. Ability to employ cyber security and cyber defense of critical space networks and systems. Skill to employ future offensive capabilities. (Space Capstone Publication, Spacepower) (SDP 3-100)

***cyber-persona —*** The combined features comprising the digital representation of an actor or entity in cyberspace used for intelligence analysis and reporting and for planning operations related to that entity. (JP 3-12) (DoD Dictionary)

***cyber-persona layer —*** A view of cyberspace created by abstracting and combining data from the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace (cyber-persona). (AFDP 3-12)

***cyber tasking order —*** Tasking document used by the Air Force cyber component commander to task assigned Air Force cyber forces to perform specific actions at specific time frames in support of Air Force and joint requirements. Also called CTO. (AFDP 3-12) (Air Force Glossary)

***cybersecurity —*** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01) (DoD Dictionary)

***cybersecurity services —*** A service provided or subscribed to in order to protect the DoDIN. Cybersecurity services include capabilities to implement DoD Component activities addressing vulnerability assessment and analysis;

vulnerability management; malware protection; continuous monitoring; incident handling; insider threat process to identify and evaluate anomalous user activity; and warning intelligence and attack, sensing, and warning to protect the DoDIN. (AR 525-24)

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

***cyberspace attack —*** Actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) or manipulation effects in cyberspace and are considered a form of fires. (JP 3-12) (DoD Dictionary)

***cyberspace capability —*** A device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. (JP 3-12) (DoD Dictionary)

***cyberspace defense —*** Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. (JP 3-12)

***cyberspace domain —*** The interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum. (FM 3-0) (FM 1-02.1)

***cyberspace effects —*** [The result of] specific tactical-level actions or tasks that employ cyberspace capabilities. All cyberspace mission objectives are achieved by the combination of one or more of these actions, which are defined exclusively by the types of effects they create. (JP 3-12)

***cyberspace effects and enabling capabilities (CEEC) —*** Capabilities that include standalone cyberspace attack and cyberspace exploitation, including EMS-enabled, SO-enabled cyberspace attack/exploitation capabilities exercised to support the full spectrum of cyberspace operations, to create noticeable (either immediately or latent) denial effects (i.e., degradation, disruption, and destruction) in cyberspace or effects in cyberspace that contribute to effects in other domains. (DoDI O-3600.03)

***cyberspace effects operations —*** Cyberspace actions that create various direct effects in cyberspace (i.e., denial, degradation, disruption, or destruction) and manipulations that can manifest as denial actions in the physical domains (AFDP 3-12)

***cyberspace electromagnetic activities —*** The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations. (ADP 3-0) Also called CEMA. (FM 1-02.1)

***cyberspace exploitation —*** Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations. (JP 3-12) (DoD Dictionary)

***cyberspace incident —*** Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. (AR 525-24)

***cyberspace intelligence, surveillance, and reconnaissance (C-ISR) —*** A military intelligence action conducted by the JFC, authorized by an execute order (EXORD). Cyberspace ISR is normally conducted to gather intelligence which may be required to support planning or execution of cyberspace operations. (AFDP 3-12)

***cyberspace Layer Model —*** To assist in the planning and execution of CO, cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona. Each layer represents a different focus from which CO may be planned, conducted, and assessed. (JP 3-12)

***cyberspace operational resilience —*** The ability of U.S. and partner forces to prepare for, fight unencumbered in and through, and recover from cyberspace and EMS attacks or other events in a cyber-contested environment. (AR 525-24)

***cyberspace operations —*** The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO comprise the military, national intelligence, and ordinary business operations of DOD in and through cyberspace. (JP 3-12)

***cyberspace parity —*** A condition in which no force has control of cyberspace. This represents a situation in which both friendly and adversary forces may encounter significant cyberspace interference. Parity is not a standoff, nor does it imply an inability to maneuver. On the contrary, parity may be typified by fleeting, intensely contested operations at critical points to achieve a sufficient level of control. (AFDP 3-12)

***cyberspace security —*** Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (JP 3-12) Note. Joint doctrine uses the term “cyberspace security” to distinguish this tactical-level cyberspace action from the policy and programmatic term “cybersecurity” used in Department of Defense (DOD) and United States Government (USG) policy. To enable effective planning, execution, and assessment, doctrine distinguishes between cyberspace security and cyberspace defense actions, a distinction not

made in DOD and USG cybersecurity policy, where the term cybersecurity includes the ideas of both security and defense. Doctrine uses both “cyberspace security” and “cybersecurity,” depending upon the context. (JP 3-12)

***cyberspace superiority —*** The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference. (JP 3-12)

***cyberspace supremacy —*** A degree of cyberspace control that permits operations wherein the opposing force is incapable of effective interference. Interference may still exist but can be easily countered or has little or no effect on operations. (AFDP 3-12)

***cyberspace surveillance and reconnaissance (CS&R) —*** A cyberspace exploitation action conducted by the joint force commander, authorized by an execute order and conducted by a military cyber unit that has been given direct support authority by Commander, USCYBERCOM. Cyberspace surveillance and reconnaissance includes activities in cyberspace conducted to gather information required to support planning and execution of current and future offensive cyberspace operations. Cyberspace surveillance and reconnaissance focuses on tactical and operational information and on identifying and mapping threat cyberspace to support planning. (FM 3-12)

***cyberspace system operation —*** Actions taken within the Department of Defense information network to ensure it operates in support of its user’s mission, including all non-security actions to administer, configure, update, extend, maintain, or repair it. (JP 3-12) (DoD Dictionary)

***cyberspace threat hunting (CTH) —*** The process of proactively and iteratively searching through networks to detect malicious cyberspace activity, above and beyond already identified indicators of compromise promulgated by Joint Force Headquarters-Department of Defense Information Network of the intelligence community for use in boundary or host based security systems defenses, to identify and isolate advanced threats evading existing security solutions. (NTRP 1-03)

***cyberspace-enabled operations in the information environment —*** Operations in the information environment (OIE) [combine] cyberspace operations and other information activities and capabilities to create effects in support of joint operations throughout the operating environment. Cyberspace operations can be conducted independently or synchronized, integrated, and deconflicted with other information capabilities and activities for more effective OIE. (AFDP 3-12)

***cyberspace-enabled operations —*** Cyberspace actions [that] use cyberspace to enable other types of activities, which employ cyberspace capabilities to complete tasks but are not undertaken as part of one of the three CO missions: OCO, DCO, or DODIN operations. These uses include actions like operating a C2 or logistics system, sending an e-mail to support an information objective, using the Internet to complete an online training course, or developing a briefing. (JP 3-12)

***cyberspace-operational preparation of the environment (C-OPE) —*** consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. This mission includes identifying data, software, system / network configurations and identifiers, or physical structures connected to, or associated with, the network. (AFDP 3-12)

***cyberspace threat intelligence (CTI) —*** Timely, relevant, and actionable intelligence is imperative to the success of DCO missions and should be evaluated early in the mission planning process. CTI should shy away from singular or transitory indicators, and focus instead on adversary motivations, capabilities, and TTPs. (AFDP 3-12)

***defensive cyberspace operations —*** Missions to preserve the ability to utilize and protect blue cyberspace capabilities and data by defeating on-going or imminent malicious cyberspace activity. Also called DCO. (JP 3-12) (DoD Dictionary)

***defensive cyberspace operations hunt —*** A tactical mission task undertaken in friendly controlled or contested cyberspace to identify and characterize threat presence and activity on the network. Refer to TC 3-12.2.98 for more information about hunt operations. (JP 3-12)

***defensive cyberspace operations-internal defensive measures —*** A defensive cyberspace operations mission in which defense actions occur within the defended portion of cyberspace. Also called DCO-IDM. (JP 3-12) (DoD Dictionary)

***defensive cyberspace operations-response actions —*** A defensive cyberspace operations mission executed external to the defended network or portion of cyberspace without the permission of the owner of the affected system. Also called DCO-RA. (JP 3-12) (DoD Dictionary)

***defensive electromagnetic attack —*** The use of EA to protect against threats by denying enemy use of the EMS to target, guide, and/or trigger weapons. EA used for defensive purposes in support of force protection or self-protection is often mistaken as EP. Although defensive EA actions and EP protect personnel, facilities, capabilities, and equipment, EP protects from the effects of EA or EMI, while defensive EA is primarily used to protect against lethal attacks by denying enemy use of the EMS to target, guide, and/or trigger weapons. (JP 3-85)

***defensive electromagnetic attack —*** Uses the EMS to protect personnel, facilities, capabilities, and equipment. Examples include employing flares, chaff, low-observable technologies, towed decoys, DE, and IR countermeasures. (AFDP 3-85)

***defensive electromagnetic spectrum operations —*** EMSO [that] can provide protection from physical attack or defend friendly EMS systems from enemy offensive EMSO. (AFDP 3-85)

***Department of Defense information network —*** The information capabilities and associated processes owned or leased by the Department of Defense for collecting, processing, storing, disseminating, and managing information, whether interconnected or stand-alone. Also called DoDIN. (JP 6-0) (DoD Dictionary)

***Department of Defense information network operations —*** Operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network. Also called DoDIN operations. (JP 3-12) (DoD Dictionary)

***Department of Defense information network-Army —*** An Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide. (ATP 6-02.71) Also called DODIN-A. (FM 1-02.1)

***directed energy (DE) —*** An umbrella term covering technologies that produce concentrated EM energy and atomic or subatomic particles. DE examples include active denial technology, lasers, RF weapons, and DE antisatellite and HPM weapon systems. (JP 3-85)

***directed-energy device —*** A system using directed energy primarily for a purpose other than as a weapon. See also directed energy; directed-energy weapon. (JP 3-85) (DoD Dictionary)

***directed-energy warfare (DEW) —*** Military action involving the use of DE weapons, devices, and countermeasures to incapacitate; cause direct damage or destruction of enemy equipment, facilities, and/or personnel; or to determine, exploit, reduce, or prevent hostile use of the EMS through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the EMS. (JP 3-85)

***directed-energy weapon —*** A weapon or system that uses directed energy to incapacitate, damage, or destroy enemy equipment, facilities, and/or personnel. See also directed energy. (JP 3-85) (DoD Dictionary)

***direction finding —*** A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. Also called DF. (JP 3-85)

***directive authority for cyberspace operations —*** The authority to issue orders and directives to all Department of Defense components to execute global Department of Defense information network operations and defensive cyberspace operations internal defensive measures. Also called DACO. (JP 3-12)

***early warning —*** Early notification of the launch or approach of unknown weapons or weapons carriers. Also called EW. See also attack assessment. (JP 3-01) (DoD Dictionary)

***effects-based targeting —*** [An] approach to targeting [which] combines both lethal and nonlethal options to achieve a commander's desired effects. Information superiority is essential to the success of an effects-based approach. Information superiority cannot be obtained without timely effective intelligence. Understanding the adversary's objectives, intentions, and decision cycle reveals the means to produce effects against the enemy's critical vulnerability. Targeting effects are the cumulative results of actions taken to engage geographical areas, complexes, installations, forces, equipment, functions, perception, or information by lethal and nonlethal means. Targeting effects are either direct or indirect. (NTRP 1-03)

***electromagnetic attack —*** Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-85). Also called EA. (FM 1-02.1)

***electromagnetic attack control authority (EACA) —*** As a broader evolution of jamming control authority, EACA is the authority a commander has to issue orders to transmit (or cease transmission of) EM energy. (JP 3-85)

***electromagnetic battle management —*** The dynamic monitoring, assessing, planning, and directing of operations in the electromagnetic spectrum in support of the commander’s concept of the operation. Also called EMBM. (JP 3-85) (DoD Dictionary)

***electromagnetic battle management system —*** The facilities, equipment, software, communications, procedures, and personnel essential for a commander to plan, direct, monitor, and assess operations in the electromagnetic spectrum. (JP 3-85) (DoD Dictionary)

***electromagnetic compatibility (EMC) —*** The ability of systems, equipment, and devices that utilize the EMS to operate in the OE without suffering unacceptable degradation or causing unintentional degradation because of EM radiation or response. EMC involves the application of sound EMS management to maximize operational effectiveness. (JP 3-85)

***electromagnetic deception —*** The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy’s combat capability. (JP 1-02)

***electromagnetic environment —*** The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform

when performing its assigned mission in its intended operational environment. Also called EME. (JP 3-85) (DoD Dictionary)

***electromagnetic environmental effects —*** The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. (JP 3-85) Also called E3. (FM 1-02.1)

***electromagnetic hardening —*** Actions taken to protect personnel, facilities, and equipment by filtering, attenuating, grounding, bonding, blanking, and shielding against undesirable effects of EM energy. EM hardening is an EP activity against the effects of EA (e.g., laser, HPM, EMP). (JP 3-85)

***electromagnetic interference —*** Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. Also called EMI. (JP 3-85)

***electromagnetic intrusion —*** The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. (JP 3-85)

***electromagnetic jamming —*** The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability. (Approved for incorporation into the DOD Dictionary.) (JP 3-85)

***electromagnetic jamming (space) —*** An attack that interferes with the link segment of space systems by generating noise in the same frequency band and within the field-of-view of the antenna on the targeted spacecraft or terrestrial receiver. (SDP 3-100)

***electromagnetic maneuver warfare (EMW) —*** The Navy's warfighting approach to gain decisive military advantage in the electromagnetic spectrum and enable freedom of action across all Navy mission areas. Control of the electromagnetic spectrum is the decisive military advantage necessary to enable all domain access through the achievement of the following electromagnetic maneuver warfare objectives: battlespace awareness, assured command and control, maneuver, integrated fires. (NTRP 1-03)

***electromagnetic masking —*** The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-85)

***electromagnetic operational environment —*** The background electromagnetic environment and the friendly, neutral, and adversarial electromagnetic order of battle within the electromagnetic area of influence associated with a given operational area. Also called EMOE. (JP 6-01) (DoD Dictionary)

***electromagnetic probing —*** Intentional radiation designed to be introduced into the devices or systems of an adversary for the purpose of learning the functions and operational capabilities of the devices or systems. (JP 3-85)

***electromagnetic protection —*** Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-85) Also called EP. (FM 1-02.1)

***electromagnetic pulse (EMP) —*** A strong burst of electromagnetic radiation caused by a nuclear explosion, energy weapon, or by natural phenomenon, that may couple with electrical or electromagnetic systems to produce damaging current and voltage surges (JP 3-85).

***electromagnetic radiation hazards —***Transmitter or antenna installation that generates or increases electromagnetic radiation in the vicinity of ordnance, personnel, or fueling operations in excess of established safe levels. (JP 3-85)

***electromagnetic reconnaissance —*** The detection, location, identification, and evaluation of foreign electromagnetic radiations. See also *reconnaissance.* (JP 3-85)

***electromagnetic security —*** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications EM radiations (e.g., radar). (JP 3-85)

***electromagnetic spectrum (EMS) —*** A maneuver space consisting of all frequencies of EM radiation (oscillating electric and magnetic fields characterized by frequency and wavelength). The EMS is often organized by frequency bands, based on certain physical characteristics. The EMS includes radio waves, microwaves, infrared (IR) radiation, visible light, ultraviolet radiation, x-rays, and gamma rays. (JP 3-85)

***electromagnetic spectrum management —*** The operational, engineering, and administrative procedures to plan and coordinate operations within the electromagnetic operational environment. (JP 3-85) (DoD Dictionary)

***electromagnetic spectrum operations (EMSO) —*** Coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment. Also called EMSO. (JP 3-85)

***electromagnetic spectrum parity —*** The degree of control in which no force has control of the EMS. This represents a situation in which both friendly and enemy EMS operations may encounter significant interference by the opposing force. Parity is not a standoff, nor does it mean maneuver has halted. On the contrary, parity may be typified by fleeting, intensely contested battles at critical points during an operation with maximum effort exerted between combatants in their attempt to achieve some level of control. (AFDP 3-85)

***electromagnetic spectrum readiness (EMSR) —*** The ability of military forces to operate, fight, and meet the demands of assigned missions given the following: the electromagnetic operational environment with regard to the planned scheme of maneuver; the required operations in the electromagnetic spectrum and the amount of electromagnetic interference expected, the difference between electromagnetic spectrum assets required and those assigned; and the electromagnetic spectrum compatibility between assigned assets. Also called EMSR. (NTRP 1-03)

***electromagnetic spectrum superiority —*** That degree of control in the EMS that permits the conduct of operations at a given time and place without prohibitive interference, while affecting an enemy's ability to do the same. EMS superiority is achieved through JEMSO and is a critical enabler to superiority throughout the OE. (JP 3-85)

***electromagnetic spectrum supremacy —*** The degree of control that permits operations wherein the opposing force is incapable of conducting effective EMSO to friendly forces. EMS supremacy may be managed by location, system, frequency, and time, or it may be broad and enduring. (AFDP 3-85)

***electromagnetic support —*** Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Also called ES. (JP 3-85)

***electromagnetic vulnerability —*** The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of electromagnetic environmental effects. Also called EMV. (JP 3-85) (DoD Dictionary)

***electromagnetic warfare (EW) —*** Military actions involving the use of electromagnetic (EM) and directed energy (DE) to control the electromagnetic spectrum (EMS) or to attack the enemy. EW consists of three distinct divisions: EA, electromagnetic support (ES), and electromagnetic protection (EP). EW is a key function of joint electromagnetic spectrum operations (JEMSO) and critical to joint force operations and success in the dynamic electromagnetic operational environment (EMOE). (JP 3-85)

***electromagnetic warfare frequency deconfliction —*** Actions taken to integrate those frequencies used by electromagnetic warfare systems into the overall frequency deconfliction process. See also *electromagnetic warfare*. (JP 3-85) (DoD Dictionary)

***electromagnetic warfare reprogramming —*** The deliberate alteration or modification of electromagnetic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. (JP 3-85) (FM 1-02.1)

***electronic attack/electromagnetic (EA) —*** The division of EW involving the use of electromagnetic (EM) energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: actions taken to prevent or reduce an enemy's effective use of the EM spectrum, such as jamming and EM deception, and employment of weapons that use either EM or directed energy as their primary destructive mechanism (e.g., lasers, radio frequency weapons, particle beams). (JP 3-09)

***electronic deception —*** The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to a threat or to threat spectrum-dependent systems, thereby degrading or neutralizing the threat actor's capability. EW supports both strategic and tactical deception, using electromagnetic means and scaling appropriately for the desired effect. (FM 3-12)

***electronic exploitation (EE) —*** Refers to EMS systems capable of sensing the EMOE. Sensing systems support intelligence collection, SA, targeting, and warning. EMS sensors can be active (e.g., air-to air radars, IFF interrogators) or passive (e.g., radar warning receivers, passive radars, IR weapons seekers). These sensing missions are typically executed through signals intelligence (SIGINT) and ES operations. (JP 3-85)

***electronic intelligence —*** Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (JP 3-85)

***electronic order of battle —*** Details on the identification, location, and disposition of friendly and enemy electronic emitters and platforms in a particular area of operations. Also called EOB. (MCRP 1-10.2)

***electronic warfare integrated reprogramming —*** The systematic process designed to enable aircrew survivability and mission success while operating in an environment characterized by friendly, neutral, and hostile threat systems that use the electromagnetic (EM) spectrum. Electronic warfare integrated reprogramming provides a capability to characterize the EM emissions of hostile and other systems, analyze and model their impact on operations, and to incorporate these characteristics to enable rapid detection, accurate identification, and appropriate response within the EM spectrum. Also called EWIR (AFI 10-703) (Air Force Glossary)

***electro-optical (EO) —*** The science and technology of the generation, modulation, detection and measurement, or display of optical radiation by electrical means. (NTRP 1-03)

***electro-optical countermeasure (EOCM) —*** Action taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far infrared (1,000 micrometers). (NTRP 1-03)

***electro-optical-infrared countermeasure (EO-IR CM) —*** Any device or technique employing electro-optical-infrared (EO-IR) materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision-guided weapons and sensor systems. EO-IR CMs may use laser jammers, smokes/aerosols, signature suppressants, decoys, pyrotechnics/pyrophorics, high-energy lasers, or directed IR energy countermeasures. (JP 3-85)

***emission control —*** The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan. Also called EMCON. (JP 3-85)

***emission security —*** This portion of communications security designed to deny unauthorized persons information of value as a result of intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. See also communications security. (JP 6-0) (DoD Dictionary)

***expeditionary cyberspace operations —*** Cyberspace operations that require the deployment of cyberspace forces within the physical domains. (JP 3-12) (DoD Dictionary)

***fire support —*** Fires that directly support land, maritime, amphibious, space, cyberspace, and special operations forces to engage enemy forces, combat formations, and facilities in pursuit of tactical and operational objectives. See also fires. (JP 3-09) (DoD Dictionary)

***fire support team —*** A field artillery team provided for each maneuver company/troop and selected units to plan and coordinate all supporting fires available to the unit, including mortars, field artillery, naval surface fire support, and close air support integration. Also called FIST. See also close air support; field artillery; fire support; support. (JP 3-09.3) (DoD Dictionary)

***fires —*** The use of weapon systems or other actions to create specific lethal or nonlethal effects on a target. (JP 3-09) (DoD Dictionary)

***foreign instrumentation signals intelligence —*** A subcategory of signals intelligence, consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. Also called FISINT. See also signals intelligence. (JP 2-01) (DoD Dictionary)

***frequency deconfliction —*** A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. See also electromagnetic spectrum management; electromagnetic warfare. (JP 3-85) (DoD Dictionary)

***frequency management —*** The requesting, recording, deconfliction of and issuance of authorization to use frequencies (operate EMS dependent systems) coupled with monitoring and interference resolution processes (JP 6-0). (CJCSM 3320.01C)

***full-spectrum superiority —*** The cumulative effect of dominance in the air, land, maritime, and space domains, electromagnetic spectrum, and information environment (which includes cyberspace) that permits the conduct of joint operations without effective opposition or prohibitive interference. (JP 3-0) (DoD Dictionary)

***gray cyberspace —*** All cyberspace that does not meet the description of either “blue cyberspace” or “red cyberspace” is referred to as “gray cyberspace.” (DoDI O-3600.03) See also neutral cyberspace. (FM 3-12)

***guarded frequencies —*** Enemy frequencies that are currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the guarded frequency list changes as the enemy assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential gain against the loss of technical information. (JP 3-51) (MCRP 3-32D.1)

***high-altitude electromagnetic pulse (HEMP) —*** A high-altitude EMP can generate significant disruptive field strengths over a continental-size area, whereas a DE weapon can generate significant disruptive field strengths to a more localized area or a specific target. (JP 3-85)"

***host nation coordination —*** The coordination with nation states for authorization to operate EMS-dependent systems within national borders (includes use of systems that emanate across the border from other AOIs). Coordination is required when operating within foreign nations as well as the United States. (FM 3-12)

***hyperspectral imagery —*** Term used to describe the imagery derived from subdividing the electromagnetic spectrum into very narrow bandwidths allowing images useful in precise terrain or target analysis to be formed. Also called HSI. (JP 2-03) (DoD Dictionary)

***infrared signature —*** The sum of all heat sources (mechanical, electrical, and solar), such as engine exhaust, gear boxes, reflection from windows and windshields, reflective paint, and lights. (NTRP 1-03)

***imitative electromagnetic deception —*** The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. (JP 1-02) (MCRP 3-32D.1)

***inform and influence activities —*** The integration of designated information related capabilities in order to synchronize themes, messages, and actions with operations to inform the U.S. and global audiences, influence foreign audiences, and affect adversary and enemy decision-making. (AR 525-24)

***information operations —*** The integrated employment, during military operations, of information related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (AR 525-24)

***information operations red team —*** An independent, threat-based, and threat-simulated opposition force that uses passive, active, technical, and nontechnical capabilities on a formal, time-bound basis to expose and exploit the vulnerabilities of friendly forces from an IO threat perspective. (AR 525-24)

***information security —***The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, against the denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. (MCRP 3-32D.1)

***information superiority —*** Degradation of the enemy's C2 while allowing the joint forces to maximize friendly C2 capabilities. (AR 525-24)

***information warfare —*** The employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and preserve friendly freedom of action during cooperation, competition, and conflict. (AFDP 3-99) (Air Force Glossary)

***informational power —*** The ability to leverage information to shape the perceptions, attitudes, and other elements that drive desired behaviors and the course of events. This includes the ability to use information to affect the observations, perceptions, decisions, and behaviors of relevant actors; ability to protect and ensure the observations, perceptions, decisions, and behaviors of the Joint Force; and the ability to acquire, process, distribute, and employ data (information). This helps commanders and staff incorporate the concept of the preeminent nature of information into the design of all operations to maximize military power (see Joint Concept for Operating in the Information Environment). (AR 525-24)

***integrated tasking order —*** An order promulgated by a joint force commander that integrates effects using fires from all domains throughout the operational area. Also called ITO. (JP 3-60) (DoD Dictionary)

***intelligence —*** 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations conducting such activities. See also all-source intelligence; communications intelligence; critical intelligence; domestic intelligence; electronic intelligence; foreign instrumentation signals intelligence; general military intelligence; imagery intelligence; joint intelligence; measurement and signature intelligence; medical intelligence; national intelligence; open-source intelligence; scientific and technical intelligence; strategic intelligence; tactical intelligence; target intelligence; technical intelligence. (JP 2-0)

***investigative defensive cyberspace operations —*** DCO activities [that] identify, illuminate, and characterize threats that have breached Air Force networks and provide options for response. (AFDP 3-12)

***joint electromagnetic spectrum management operations —*** Those interrelated functions of frequency management, HN coordination, and JSIR that together enable the planning, management, and execution of operations within the EMOE during all phases of military operations. Also called JEMSMO. (CJCSM 3320.01C)"

***joint electromagnetic spectrum operations —*** Military actions undertaken by a joint force to exploit, attack, protect, and manage the EMOE. These actions include/impact all joint force transmissions and receptions of electromagnetic (EM) energy. JEMSO are offensively and defensively employed to achieve unity of effort and the commander's objectives. JEMSO integrate and synchronize electromagnetic warfare (EW), EMS management, and intelligence, as well as other mission areas, to achieve EMS superiority. (JP 3-85)

***joint restricted frequency list —*** A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the number of frequencies necessary for friendly forces to accomplish objectives. Also called JRFL. (JP 3-51) (MCRP 3-32D.1)

***joint spectrum interference resolution (JSIR) —*** Identifies, reports, analyzes, and mitigates or resolves incidents of electromagnetic interference (EMI). JSIR uses a continuous systematic process to report and diagnose the cause or source of EMI. For further information on JSIR, see CJCSI 3320.02, Joint Spectrum Interference Resolution, and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3320.02, Joint Spectrum Interference Resolution (JSIR) Procedures. (JP 3-85).

***key terrain-cyberspace —*** Any locality or area in cyberspace (logical, physical, or cyber-persona) whose seizure, retention, or disruption affords a marked advantage to any combatant. (NTRP 1-03)

***key terrain in cyberspace (KT-C) —*** Analogous to key terrain in a physical domain, in that access to or control of it affords any combatant a position of marked advantage (JP 3-12). In cyberspace, it may only be necessary to maintain a secure presence in a particular location, or in a particular process, for a limited period. KTCs often have a

virtual component identified in the logical network layer or the cyber-persona layer. Examples of KT-C include 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 DODIN connected assets. (AFDP 3-12)

***kinetic —*** Relating to actions designed to produce effects using the forces and energy of moving bodies and directed energy, including physical damage to, alteration of, or destruction of targets. Kinetic actions can have lethal or non-lethal effects. (AFDP 3-0).

***logical network layer —*** The logical network layer consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not necessarily tied to a specific physical link or node, but to their ability to be addressed logically and exchange or process data). (AFDP 3-12)

***low observability —*** Electromagnetic protection attributes [that increase the ability of EM systems] to operate in the physical domains by reducing the possibility of their detection and exploitation by enemies. Low observability and other signature reduction techniques also improve the effectiveness of electro-optical-infrared countermeasures (EO-IR CMs). (JP 3-85)

***malicious cyberspace activities —*** Activities, other than those authorized by or in accordance with US law, which seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident therein. (AFDP 3-12)

***manipulative electromagnetic deception —*** Seeks to eliminate, reveal, or convey misleading indicators of friendly intentions. Manipulative electromagnetic deception uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit will attack when it is actually planning to withdraw, the unit might transmit false plans and requests for ammunition. Units use manipulative electromagnetic deception to mislead the enemy to misdirect their electromagnetic attack and electromagnetic support assets, while interfering less with friendly communications. (FM 3-12)

***Marine air-ground task force —*** The Marine Corps' principal organization for missions across a range of military operations, composed of forces organized under a single commander capable of responding rapidly to a contingency anywhere in the world. Also called MAGTF. (MCRP 5-12C) (MCDP 1-0)

***Marine tactical electronic warfare squadron (VMAQ) —*** Provides EW support to the Marine Air-Ground Task Force (MAGTF) and other designated forces. The VMAQ conducts tactical jamming to prevent, delay, or disrupt the enemy's ability to use early warning, acquisition, fire or missile control, counterbattery, and battlefield surveillance radars. The VMAQ conducts electronic surveillance operations to maintain electronic orders of battle, including both selected emitter parameters and location of nonfriendly emitters. It also provides threat warnings for friendly aircraft, ships, and ground units. (MCRP 3-32D.1)

***meaconing —*** Consists of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings for aircraft or ground stations. (JP 3-85)

***meaconing, intrusion, jamming and interference (MIJI) —*** Any military actions in the electromagnetic spectrum described by meaconing, intrusion, jamming, or interference. (NTRP 1-03)

***measurement and signature intelligence —*** Information produced by quantitative and qualitative analysis of physical attributes of targets and events to detect, characterize, locate, and identify targets and events; and derived from specialized, technically derived measurements and signatures of physical phenomenon intrinsic to an object or event. Also called MASINT. See also intelligence; scientific and technical intelligence. (JP 2-0) (DoD Dictionary)

***mission assurance —*** Measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities. (AFDP 3-12) (Air Force Glossary)

***mission thread defense —*** In DOD usage, mission thread refers to a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities. Mission thread defense is a change from traditional point defenses in cyberspace that failed to account for mission, network, and data interdependencies. Defensive cyber forces conduct systems analysis (see chapter 1) to identify the critical capabilities and dependencies for a mission thread and plan appropriate defenses. Refer to TC 3-12.2.90 for more information about mission thread defense. (FM 3-12)

***mobile electronic warfare support system —*** A specially configured light armored vehicle resident in the radio battalions capable of conducting signal intercept with line of bearing and electronic attack operations. Also called MEWSS. (MCRP 1-10.2)

***multi–domain operations (MDO) —*** Operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives. (AR 525-24)

***navigation warfare —*** Actions that maintain friendly use of positioning, navigation, and timing information while denying the same to an adversary. Also called NAVWAR. (JP 3-14) (DoD Dictionary)

***non-kinetic —*** Relating to actions designed to produce effects without the direct use of the force or energy of moving objects and directed energy sources. Kinetic actions can have lethal or nonlethal results. (AFDP 3-0) (Air Force Glossary)

***obscuration —*** The employment of materials into the environment that degrade optical and/or electro-optical capabilities within select portions of the electromagnetic spectrum in order to deny acquisition by or deceive an enemy or adversary. (ATP 3-11.50) (FM 1-02.1)

***offensive counterspace —*** Operations undertaken to negate an adversary's use of space capabilities, reducing the effectiveness of adversary forces in all domains. Also called OCS. (AFDP 3-14). (Air Force Glossary)

***offensive cyberspace operations —*** Missions intended to project power in and through cyberspace. Also called OCO. (JP 3-12) (DoD Dictionary)

***offensive electromagnetic attack —*** Used to suppress a threat for a specified period. Examples such as EM jamming; meaconing and intrusion; expendable decoys; anti-radiation missiles; DE and high-energy weapons including lasers, radio-frequency weapons, high-power microwave, and EMP; EMS-enabled cyberspace attacks; and navigation warfare. (AFDP 3-85)

***offensive electromagnetic spectrum operations —*** Used to deceive, disrupt, degrade, or destroy the enemy’s ability to use the EMS. (AFDP 3-85)

***offensive space control (OSC) —*** Consist of offensive operations conducted for space negation, where negation involves measures to deceive, disrupt, deny, degrade, or destroy space systems or services. Adversaries, both state and non-state actors, will exploit the availability of space-based capabilities to support their operations. In keeping with the principles of joint operations, this makes it incumbent on the United States to deny adversaries the ability to utilize space capabilities and services. OSC actions targeting an enemy’s space-related capabilities and forces could employ reversible and/or nonreversible means. (JP 3-14)

***on-call target —*** Planned target upon which fires are determined using deliberate targeting and triggered, when detected or located, using dynamic targeting. See also dynamic targeting; on-call; operational area; target. (JP 3-60) (DoD Dictionary)

***overhead persistent infrared —*** Within geospatial intelligence, a capability that provides on-demand, persistent, global, and/or localized coverage of high- to low-intensity infrared events to detect energy radiation from various tactical to strategic objects. (JP 2-0) (DoD Dictionary)

***physical network layer —*** The physical network layer consists of the information technology (IT) devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components. The physical network also includes hardware and infrastructure (e.g., computing devices, storage devices, network devices, and network links [wired and wireless]). All physical components are owned by public or private entities capable of controlling or restricting access and require security measures to protect from physical damage or unauthorized access. (AFDP 3-12)

***physical security —*** That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. See also communications security; security. (JP 3-0) (DoD Dictionary)

***protected frequencies —*** Friendly, generally time-oriented, frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electromagnetic warfare operations are directed against hostile forces. See also electromagnetic warfare. (JP 3-85) (DoD Dictionary)

***protective defensive cyberspace operations —*** DCO activities [which] minimize risk to Air Force networks, systems, and data through threat-informed cyberspace security actions. (AFDP 3-12)

***radar warning receiver (RWR) —*** An onboard receiver providing information to the aircrew about radar energy striking the aircraft. (NTRP 1-03)

***radio battalion (RadBn) —*** To provide EW support, the Marine Corps has two types of EW units: RadBns and VMAQs. The mission of the RadBn is to provide COMSEC monitoring, tactical SIGINT, electronic warfare, and special intelligence communications support to the MAGTF. (MCRP 3-32D.1)

***rapid software reprogramming —*** Electromagnetic warfare software reprogramming activities requiring an expeditious update or creation, categorized as either urgent or emergency priority. (AR 525-24)

***red cyberspace —*** Refers to those portions of cyberspace owned or controlled by an adversary or an enemy. (DoDI O-3600.03)

***red team —*** An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (AR 525-24)

***response defensive cyberspace operations —*** DCO activities [that] are conducted by cyberspace operations forces, on or off DODIN systems in friendly- or adversary-controlled cyberspace terrain. (pp. 8) (AFDP 3-12)

***scheduled target —*** Planned target upon which fires or other actions are scheduled for prosecution at a specified time. See also target. (JP 3-60) (DoD Dictionary)

***scientific and technical intelligence —*** Foundational all-source intelligence that covers: a. foreign developments in basic and applied research and applied engineering techniques and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. Also called S&TI. See also intelligence; technical intelligence. (JP 2-0) (DoD Dictionary)

***service cyber component (SCC) —***The service cyber component commander plans, coordinates, integrates, synchronizes, directs, and conducts the network operations of the Department of Defense information networks; when directed, conducts cohesive unified action in cyberspace to secure freedom of action and deny the same to our adversaries. (NTRP 1-03)

***ship's signals exploitation space —*** A capability that provides real-time signals intelligence using organic and nonorganic resources in response to national, theater, and fleet cryptologic requirements. (NTRP 1-03)

***signals intelligence —*** 1. A category of intelligence comprising all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted, individually or in combination. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT. See also communications intelligence; electronic intelligence; foreign instrumentation signals intelligence; intelligence. (JP 2-0) (DoD Dictionary)

***signals intelligence/electronic attack planning/coordinating message (SIEPCM) —*** Used to plan and coordinate SIGINT collection and EA communications or noncommunications missions. It is also a vehicle for requesting cross-Service assets to satisfy tasks beyond a component Service's capabilities. (MCRP 3-32D.1)

***signals intelligence operational tasking authority —*** A military commander's authority to operationally direct and levy signals intelligence requirements on designated signals intelligence resources. See also *signals intelligence*. (JP 2-0)

***simulative electromagnetic deception —*** [Electromagnetic deception that] attempts to represent friendly, notional, or actual capabilities to mislead threat forces. (FM 3-12)

***space electromagnetic warfare —*** Knowledge of spectrum awareness, maneuver within the spectrum, and non-kinetic fires within the spectrum to deny adversary use of vital links. Skill to manipulate physical access to communication pathways and awareness of how those pathways contribute to adversary advantage. (Space Capstone Publication, Spacepower)

***special information operations —*** Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. Also called SIO. (JP 3-13) (MCRP 3-32D.1)

***spectrum-dependent (S-D) systems —*** All electronic systems, subsystems, devices, and/or equipment that depend on the use of the spectrum to properly accomplish their function(s) without regard to how they were acquired (full acquisition, rapid acquisition, Joint Concept Technology Demonstration, etc.) or procured (commercial off-the-shelf, government off-the-shelf, non-developmental items, etc.). (DoDI 4650.01)

***spectrum management operations —*** The interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. (FM 6-02) Also called SMO. (FM 1-02.1)

***spoofing —*** A form of electromagnetic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is the real signal it is trying to receive. (SDP 3-100)

***suppression of enemy air defenses —*** Activity that neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means. Also called SEAD. See also electromagnetic warfare. (JP 3-01) (DoD Dictionary)

***surveillance —*** 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) (DoD Dictionary)

***TABOO frequencies —*** Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces including international distress, safety, and controller frequencies. See also electromagnetic warfare. (JP 3-85) (DoD Dictionary)

***technical effects —*** One or more capabilities, activities, or programs planned, coordinated, or executed that utilize classified means to accomplish an objective or enable military operations. (FM 1-02.1) [Note: Encompasses all capabilities, activities, or programs that, when associated with authorities or specific targets, target audiences, or locations, are classified at a higher level than UNCLASSIFIED. This term enables staffs and commanders to describe single or multiple capabilities, activities, or programs delivering an effect to accomplish an objective in an UNCLASSIFIED or a lower classification venue than required by specific security classification guides. These

capabilities, activities, or programs include, but are not limited to: cyber-OPE, delayed and non-attribution MISO, deception in support of OPSEC, electronic attack, electronic warfare support, joint MILDEC, offensive counter intelligence operations, offensive cyberspace operations, offensive space operations, special access programs, and tactical deception. (FM 1-02.1)

***technical intelligence* —** Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an enemy's technological advantages. Also called TECHINT. See also exploitation; intelligence. (JP 2-0) (DoD Dictionary)

***threat cyberspace* —** Capabilities [that] jeopardize U.S. freedom of action in cyberspace and the electromagnetic spectrum. (FM 3-12) See also *red cyberspace*.

***threat warning* —** The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (JP 2-0) (DoD Dictionary)

***transmission security* —** That portion of communications security designed to protect communications from interception and exploitation by means other than cryptanalysis. See also communications security. (JP 6-0) (DoD Dictionary)

***VMAQ* —** See Marine Tactical electronic warfare squadron. (MCRP 3-32D.1)

***vulnerability assessment* —** A Department of Defense, command, or unit-level evaluation to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a physical or cyberspace threat. (JP 3-26) (DoD Dictionary)

***wartime reserve modes* —** Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to, or misunderstood by, opposing commanders before they are used but could be exploited or neutralized if known in advance. Also called WARMs. (JP 3-85) (DoD Dictionary)

# Appendix G – Consolidated List of References

*The following is a comprehensive compilation of joint and allied doctrinal publications that directly address cyberspace operations and electromagnetic warfare or are referenced by those publications. These publications collectively shaped our understanding of the subjects covered in this study and are presented here as an alphabetized by-title reference list. Please note that not all of the following publications are explicitly cited within the text of this study.*

[1] Office of the Principal Cyber Advisor to the Secretary of the Army, "120-Day Study of U.S. Army Electromagnetic Warfare, Cyberspace Operations, and Information Advantage Capabilities and Organizations (Draft)," U.S. Dept. of the Army, Washington, DC, USA, 2023.

[2] U.S. Army Cyber Center of Excellence, "Advanced Electromagnetic Countermeasure (ECMs) Assessment: Assessing Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) considerations for the ARCYBER (Army Cyber) STARBLAZOR Pilot" U.S. Dept. of the Army, Fort Eisenhower, GA, USA, 2021.

[3] *ADP 2-0*, *Intelligence*. Washington, DC, USA: U.S. Dept. of the Army, 2019. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18009-ADP_2-0-000-WEB-2.pdf

[4] *ADP 3-0*, *Operations*. Washington, DC, USA: U.S. Dept. of the Army, 2019. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf

[5] *ADP 3-13*, *Information*. Washington, DC, USA: U.S. Dept. of the Army, 2023. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39736-ADP_3-13-000-WEB-1.pdf

[6] *ADP 3-19*, *Fires*. Washington, DC, USA: U.S. Dept. of the Army, 2019. [Online]. Available: https://armypubs.army.mil/epubs/dr_pubs/dr_a/pdf/web/arn18615_adp%203-19%20final%20web.pdf

[7] *ADP 3-37*, *Protection*. Washington, DC, USA: U.S. Dept. of the Army, 2024. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN40011-ADP_3-37-000-WEB-1.pdf

[8] *ADP 3-90*, *Offense And Defense*. Washington, DC, USA: U.S. Dept. of the Army, 2019. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34828-ADP_3-90-000-WEB-1.pdf

[9] *AFDP 2-0*, *Intelligence*. Washington, DC, USA: U.S. Dept. of the Air Force, 2023. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_2-0/2-0-AFDP-INTELLIGENCE.pdf

[10] *AFDP 3-0*, *Operations and Planning*. Washington, DC, USA: U.S. Dept. of the Air Force, 2016. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-0/3-0-AFDP-OPERATIONS-PLANNING.pdf

[11] *AFDP 3-12*, *Cyberspace Operations*. Washington, DC, USA: U.S. Dept. of the Air Force, 2023. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

[12] *AFDP 3-13*, *Information in Air Force Operations*. Washington, DC, USA: U.S. Dept. of the Air Force, 2023. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-13/3-13-AFDP-INFO-OPS.pdf

[13] *AFDP 3-14*, *Counterspace Operations*. Washington, DC, USA: U.S. Dept. of the Air Force, 2018. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/AFDP-3-14-Counterspace-Ops.pdf

[14] *AFDP 3-60*, *Targeting*. Washington, DC, USA: U.S. Dept. of the Air Force, 2021. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf

[15] *AFDP 3-85*, *Electromagnetic Spectrum Operations*. Washington, DC, USA: U.S. Dept. of the Air Force, 2023. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf

[16] *Air Force Glossary*, *Air Force Doctrine*. Washington, DC, USA: U.S. Dept. of the Air Force, 2021. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_Air-Force-Glossary/AF-GLOSSARY.pdf

[17] *AJP-3.6*, *Allied Joint Doctrine for Electronic Warfare*. Brussels, Belgium: NATO, 2020. [Online]. Available: https://standards.globalspec.com/std/14362044/ajp-3-6

[18] *AJP-3.6.2*, *Allied Joint Doctrine for Land Operations (Draft)*. Brussels, Belgium: NATO, 2024. [Online]. Available: https://natolibguides.info/

[19] *AJP-3.20*, *Allied Joint Doctrine for Cyberspace Operations*. Brussels, Belgium: NATO, 2020. [Online]. Available: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

[20] *AR 5-12*, *Army Use Of The Electromagnetic Spectrum*. Washington, DC, USA: U.S. Dept. of the Army, 2020. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN37511-AR_5-12-001-WEB-3.pdf

[21] *Army Publishing Directorate*, *Army Regulation (AR) 525-24, U.S. Army Cyberspace And Electromagnetic Warfare Operations*. Washington, DC, USA: U.S. Dept. of the Army, 2023. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_d/ARN31149-AR_525-24-000-WEB-1.pdf

[22] *ATP 3-12.3*, *Electromagnetic Warfare Techniques*. Washington, DC, USA, 2023. [Online]. Available: https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1026337

[23] *CJCS Instruction 3160.01D*, *No-Strike and the Collateral Damage Estimation Methodology*. Washington, DC, USA: Joint Chiefs of Staff, 2021. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/CJCSJS%20Directives%20Limited/Forms/Instr_CJCSJS.aspx

[24] *CJCS Instruction 3210.01C*, *Joint Information Operations Proponent*. Washington, DC, USA: Joint Chiefs of Staff, 2014. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSI%203210.01C.pdf

[25] *CJCS Instruction 3210.04B*, *Joint Electromagnetic Warfare Reprogramming Policy*. Washington, DC, USA: Joint Chiefs of Staff, 2022. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSI%203210.04B.pdf

[26] *CJCS Instruction 3320.02F*, *Joint Spectrum Interference Resolution*. Washington, DC, USA: Joint Chiefs of Staff, 2013. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSI%203320.02F.pdf

[27] *CJCS Instruction 5810.01E*, *Implementation of the Department of Defense Law of War Program*. Washington, DC, USA: Joint Chiefs of Staff, 2023. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSI%205810.01E.pdf

[28] *CJCS Manual 3108.01A*, *Joint Fires Element*. Washington, DC, USA: Joint Chiefs of Staff, 2023. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSM%203108.01A.pdf

[29] *CJCS Manual 3130.03B*, *Planning and Execution Formats and Guidance*. Washington, DC, USA: Joint Chiefs of Staff, 2024. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/CJCSJS%20Directives%20Limited/CJCSM%203130.03B.pdf

[30] *CJCS Manual 3320.01C*, *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment*. Washington, DC, USA: Joint Chiefs of Staff, 2019. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSM%203320.01C.pdf

[31] *CJCS Manual 3320.02E*, *Joint Spectrum Interference Resolution (JSIR) Procedures*. Washington, DC, USA: Joint Chiefs of Staff, 2022. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSM%203320.02E.pdf

[32] *CJCS Manual 6510.01B*, *Cyber Incident Handling Program*. Washington, DC, USA: Joint Chiefs of Staff, 2012. [Online]. Available: https://jsportal.sp.pentagon.mil/sites/Matrix/DEL/JEL%20%20Unlimited/CJCSM%206510.01B.pdf

[33] *DoD Dictionary*, *Military and Associated Terms*. Washington, DC, USA: Department of Defense, 2024. [Online]. Available: https://jdeis.js.mil/jdeis/new_pubs/dictionary.pdf

[34] *DoD Directive 3020.4*, *Mission Assurance*. Washington, DC, USA: Department of Defense, 2016. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983

[35] *DoD Directive 3025.18*, *Defense Support of Civil Authorities*. Washington, DC, USA: Department of Defense, 2018. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302518p.pdf?ver=2019-02-05-090338-707

[36] *DoD Directive 3600.01*, *Information Operations (IO)*. Washington, DC, USA: Department of Defense, 2017. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf?ver=2019-08-12-094732-187

[37] *DoD Directive 3700.01*, *DoD Command and Control Enabling Capabilities*. Washington, DC, USA: Department of Defense, 2022. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/370001p.pdf?ver=O0nCZiX_-SU6Vy7TU6bi0w%3d%3d

[38] *DoD Directive 4650.05*, *Positioning, Navigation, and Timing*. Washington, DC, USA: Department of Defense, 2023. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/465005p.pdf?ver=eoeqO6z-xTmE0nzmh_LL4Q%3d%3d

[39] *DoD Directive 5143.01*, *Under Secretary of Defense for Intelligence and Security (USD(I&S))*. Washington, DC, USA: Department of Defense, 2020. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/514301p.pdf?ver=2019-07-01-092756-170

[40] *DoD Directive 8000.01*, *Management of the Department of Defense Information Enterprise (DOD IE)*. Washington, DC, USA: Department of Defense, 2017. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/800001p.pdf?ver=2019-06-06-110331-810

[41] *DoD Instruction 3222.03*, *DoD Electromagnetic Environmental Effects (E3) Program*. Washington, DC, USA: Department of Defense, 2017. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/322203p.pdf?ver=2019-02-26-101527-160

[42] *DoD Instruction 3607.02*, *Military Information Support Operations (MISO)*. Washington, DC, USA: Department of Defense, 2016. [Online]. Available: https://login.milsuite.mil/?goto=https%3A%2F%2Fwww.milsuite.mil%3A443%2Fbook%2Fservlet%2FJiveServlet%2FpreviewBody%2F1217519-102-1-2848172%2FO360702p.pdf

[43] *DoD Instruction 4630.09*, *Communications Waveform Management and Standardization*. Washington, DC, USA: Department of Defense, 2020. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/463009p.pdf?ver=_AodYK2mcqGmezDUQiIGhA%3d%3d

[44] *DoD Instruction 4650.01*, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*. Washington, DC, USA: Department of Defense, 2017. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/465001p.pdf?ver=2019-01-24-112300-743

[45] *DoD Instruction 5205.13*, *Cybersecurity Activities Support to DoD Information Network Operations*. Washington, DC, USA: Department of Defense, 2017. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853001p.pdf?ver=2019-02-26-101530-693

[46] *DoD Instruction 6055.11*, *Protecting Personnel from Electromagnetic Fields*. Washington, DC, USA: Department of Defense, 2021. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/605511p.pdf?ver=l44ncGJF4r_5w55oLmhe-g%3d%3d

[47] *DoD Instruction 8320.05*, *Electromagnetic Spectrum Data Sharing*. Washington, DC, USA: Department of Defense, 2017. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/832005p.pdf?ver=2019-01-24-135438-937

[48] *DoD Instruction 8330.01*, *Interoperability of Information Technology, Including National Security Systems*. Washington, DC, USA: Department of Defense, 2022. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/833001p.pdf?ver=c7Bds_aCFKSe7SK_MiYBIg%3d%3d

[49] *DoD Instruction 8500.01*, *Cybersecurity*. Washington, DC, USA: Department of Defense, 2019. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf?ver=2019-10-07-112048-860

[50] *DoD Instruction 8530.03*, *Cyber Incident Response*. Washington, DC, USA: Department of Defense, 2023. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853003p.PDF?ver=XPp9bgbmddCqR7gokbskWg%3d%3d

[51] *DoD Instruction 8560.01*, *Communications Security (COMSEC) Monitoring*. Washington, DC, USA: Department of Defense, 2018. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/856001p.pdf?ver=2018-08-22-082328-107

[52] *DoD Instruction 8585.01*, *DoD Cyber Red Teams*. Washington, DC, USA: Department of Defense, 2024. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858501p.pdf?ver=0J4GT4-ji4H0Dd7mOa173w%3d%3d

[53] *DoD Instruction O-3600.03*, *Test and Evaluation of Cyberspace Effects and Enabling Capabilities*. Washington, DC, USA: Department of Defense, 2022. [Online]. Available: https://login.milsuite.mil/?goto=https%3A%2F%2Fwww.milsuite.mil%3A443%2Fbook%2Fservlet%2FJiveServlet%2FpreviewBody%2F1217518-102-1-2848161%2FO360003p.pdf

[54] *DoD Strategy*, *Strategy for Operations in the Information Environment*. Washington, DC, USA: Department of Defense, 2023. [Online]. Available: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF

[55] D. J. Trump, *Executive Order 13800*, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Washington, DC, USA: White House, 2017. [Online]. Available: https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure#page-

[56] J. R. Biden Jr., *Executive Order 14028*, *Improving the Nation's Cybersecurity*. Washington, DC, USA: White House, 2021. [Online]. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity#page-

[57] *FM 1-02.1*, *Operational Terms*. Washington, DC, USA: U.S. Dept. of the Army, 2024. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN40321-FM_1-02.1-000-WEB-2.pdf

[58] *FM 2-0*, *Intelligence*. Washington, DC, USA: U.S. Dept. of the Army, 2023. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39259-FM_2-0-000-WEB-2.pdf

[59] *FM 3-0*, *Operations*. Washington, DC, USA: U.S. Dept. of the Army, 2022. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf

[60] *FM 3-12*, *Cyberspace Operations And Electromagnetic Warfare (Draft)*. Washington, DC, USA: U.S. Dept. of the Army, 2024. [Online]. Available: https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1022713

[61] *FM 6-02*, *Signal Support To Operations*. Washington, DC, USA: U.S. Dept. of the Army, 2013. [Online]. Available: https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1007816

[62] *JP 2-0*, *Joint Intelligence*. Washington, DC, USA: Joint Chiefs of Staff, 2022. [Online]. Available: (SIPR Only)

[63] *JP 3-0*, *Joint Campaigns and Operations*. Washington, DC, USA: Joint Chiefs of Staff, 2022. [Online]. Available: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

[64] *JP 3-01*, *Countering Air and Missile Threats*. Washington, DC, USA: Joint Chiefs of Staff, 2023. [Online]. Available: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

[65] *JP 3-05*, *Joint Doctrine for Special Operations*. Washington, DC, USA: Joint Chiefs of Staff, 2020. [Online]. Available: https://jdeis.js.mil/jdeis/new_pubs/jp3_05.pdf

[66] *JP 3-09*, *Joint Fire Support*. Washington, DC, USA: Joint Chiefs of Staff, 2019. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf?ver=2019-05-14-081632-887

[67] *JP 3-12*, *Joint Cyberspace Operations*. Washington, DC, USA: Joint Chiefs of Staff, 2022. [Online]. Available: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=791

[68] *JP 3-13.4*, *Military Deception*. Washington, DC, USA: Joint Chiefs of Staff, 2017. [Online]. Available: https://jdeis.js.mil/my.policy

[69] *JP 3-14*, *Joint Space Operations*. Washington, DC, USA: Joint Chiefs of Staff, 2023. [Online]. Available: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=832

[70] *JP 3-60*, *Joint Targeting*. Washington, DC, USA: Joint Chiefs of Staff, 2014. [Online]. Available: https://jdeis.js.mil/jdeis/new_pubs/jp3_60.pdf

[71] *JP 3-85*, *Joint Electromagnetic Spectrum Operations*. Washington, DC, USA: Joint Chiefs of Staff, 2020. [Online]. Available: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=704

[72] *JP 5-0*, *Multinational Operations*. Washington, DC, USA: Joint Chiefs of Staff, 2024. [Online]. Available: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=888

[73] *JP 6-0*, *Joint Communications*. Washington, DC, USA: Joint Chiefs of Staff, 2023. [Online]. Available: https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=845

[74] *LOCE*, *Littoral Operations in a Contested Environment (LOCE)*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2017. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/148/No/47bf2d8f-147e-4f8a-9183-f26b23a16a2b/false/LOCE%2C%20Littoral%20Operations%20in%20a%20Contested%20Environment%20(LOCE).pdf

[75] *MCDP 1*, *Warfighting*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 1997. [Online]. Available: https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/899837/mcdp-1/

[76] *MCDP 1-0 w/Ch 1-3*, *Marine Corps Operations*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2019. [Online]. Available: https://www.marines.mil/Portals/1/Publications/MCDP%201-0%20w%20Ch%201-3.pdf?ver=KugfXDOHFuRQmxSmTiUJwg%3d%3d

[77] *MCDP 1-4*, *Competing*. Washington, DC, USA: MCDP 1-4, 2020. [Online]. Available: https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/2449338/mcdp-1-4/

[78] *MCDP 8*, *Information*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2022. [Online]. Available: https://www.marines.mil/Portals/1/Publications/MCDP%208.pdf?ver=6gIvEcD0CUuPAgTSmyDNag%3d%3d

[79] *MCRP 1-02*, *Marine Corps Supplement to the DOD Dictionary of Military and Associated Terms*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2020. [Online]. Available: https://www.marines.mil/Portals/1/Publications/1-10.2%20(SECURED).pdf?ver=Io6qEzsWPanVv1LtWF96eA%3d%3d

[80] *MCRP 2-10A.5*, *Remote Sensor Operations*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2016. [Online]. Available: https://www.marines.mil/portals/1/Publications/MCRP%202-10A.5%20(Formerly%20MCRP%202-24B).pdf?ver=2016-06-23-110531-747

[81] *MCRP 2-10B.1*, *Intelligence Preparation of the Battlespace*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2023. [Online]. Available: https://www.marines.mil/Portals/1/Publications/MCRP%202-10B.1.pdf?ver=WZgANNGDKsmcphvgtPdt-Q%3d%3d

[82] *MCRP 3-32D.1*, *Electronic Warfare*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2018. [Online]. Available: https://www.marines.mil/portals/1/Publications/MCRP%203-32D.1%20gn.pdf?ver=2019-04-25-145246-263

[83] *MCWP 3-31*, *Marine Air-Ground Task Force Fires and Effects*. Washington, DC, USA: U.S. Marine Corps, Dept. of the Navy, 2024. [Online]. Available: https://www.marines.mil/Portals/1/Publications/MCWP%203-31%20(SECURED).pdf?ver=8-R_z1atKvJd2FRolggX6w%3d%3d

[84] *Navy Warfare Library*, *NWP 3-60 Maritime Targeting*. Washington, DC, USA: U.S. Dept. of the Navy, 2023. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/1282/No/cd49056e-1fe3-4c27-9ffb-0f19ee62334a/false/NWP%203-60%2C%20Maritime%20Targeting.pdf

[85] *NCIRP*, *National Cyber Incident Response Plan*. Washington, DC, USA: U.S. Department of Homeland Security, 2016. [Online]. Available: https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

[86] *NDP 1*, *Naval Warfare*. Washington, DC, USA: U.S. Dept. of the Navy, 2020. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/158/No/5b2c13d1-be4f-4a3d-b228-c2d15285c80b/false/NDP%201%2C%20Naval%20Warfare.pdf

[87] *NDS 2022*, *National Defense Strategy*. Washington, DC, USA: Department of Defense, 2022. [Online]. Available: https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf

[88] *NSS*, *National Security Strategy*. Washington, DC, USA: White House, 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[89] *NTP 4*, *Naval Communications*. Washington, DC, USA: U.S. Dept. of the Navy, 2008. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/161/No/f43bef77-85bd-402d-960d-bc7000d91a6e/false/NTP%204%2C%20Naval%20Communications.pdf

[90] *NTP 6(F)*, *Navy Electromagnetic Spectrum Guide*. Washington, DC, USA: U.S. Dept. of the Navy, 2018. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/162/No/0914d7a6-ff3c-4e0f-a25a-b77bed3acd19/false/NTP%206(F)%2C%20Navy%20Electromagnetic%20Spectrum%20(EMS)%20Guide.pdf

[91] *NTRP 1-03*, *Navy Supplement to the DOD Dictionary of Military and Associated Terms (Navy Dictionary)*. Washington, DC, USA: U.S. Dept. of the Navy, 2024. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/1359/No/651148ba-cad6-4b51-ab1d-e7c20229b86e/false/Navy%20Supplement%20to%20the%20DOD%20Dictionary%20of%20Military%20and%20Associated%20Terms.pdf

[92] *NTTP 3-12.1*, *Cyberspace Threat Hunting*. Washington, DC, USA: U.S. Dept. of the Navy, 2023. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/1336/No/bd838e3d-04a6-44a6-a324-b7053d785762/false/NTTP%203-12.1%2C%20Cyberspace%20Threat%20Hunting.pdf

[93] *NTTP 3-60.1*, *Multi-Service Tactics, Techniques, and Procedures for Dynamic Targeting*. Washington, DC, USA: U.S. Dept. of the Navy, 2023. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/1336/No/bd838e3d-04a6-44a6-a324-b7053d785762/false/NTTP%203-12.1%2C%20Cyberspace%20Threat%20Hunting.pdf

[94] *NWP 2*, *Fleet Intelligence*. Washington, DC, USA: U.S. Dept. of the Navy, 2022. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/286/No/02aeebfb-fd6f-4f47-a90e-5979494d4fdd/false/NWP%202-0%2C%20Naval%20Intelligence.pdf

[95] *NWP 3*, *Fleet Warfare*. Washington, DC, USA: U.S. Dept. of the Navy, 2021. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/288/No/1d333452-0c16-4880-9223-eb5402c57369/false/NWP%203%2C%20Fleet%20Warfare.pdf

[96] *NWP 3-01*, *Fleet Air and Missile Defense*. Washington, DC, USA: U.S. Dept. of the Navy, 2020. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/289/No/213081d3-1ae8-4700-9656-b00583efaab4/false/NWP%203-01%2C%20Fleet%20Air%20and%20Missile%20Defense.pdf

[97] *NWP 3-09*, *Fleet Fires*. Washington, DC, USA: U.S. Dept. of the Navy, 2024. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/1410/No/5347ed27-6a00-4a59-9f1d-843c209c5808/false/NWP%203-09%2C%20Fleet%20Fires.pdf

[98] *NWP 3-10*, *Naval Expeditionary Combat Forces*. Washington, DC, USA: U.S. Dept. of the Navy, 2020. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/298/No/7e5f811e-e147-47de-8e46-da9716c5d2be/false/NWP%203-10%2C%20Navy%20Expeditionary%20Combat%20Forces.pdf

[99] *NWP 3-12*, *Cyberspace Operations*. Washington, DC, USA: U.S. Dept. of the Navy, 2018. [Online]. Available: SIPR Only

[100] *NWP 3-13*, *Navy Information Operations*. Washington, DC, USA: U.S. Dept. of the Navy, 2014. [Online]. Available: https://doctrine.navy.mil/default.aspx#/pubs/approved/all/view/300/No/73994488-1079-41f1-a214-5fe7276e1524/false/NWP%203-13%2C%20Navy%20Information%20Operations.pdf

[101] B. H. Obama, *PPD-21*, *Presidential Policy Directive (PPD)-- Critical Infrastructure Security and Resilience*. Washington, DC, USA: White House, 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[102] B. H. Obama, *PPD-41*, *Presidential Policy Directive (PPD)-- United States Cyber Incident Coordination*. Washington, DC, USA: White House, 2016. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[103] W. J. Clinton, *PPD-63*, *Presidential Policy Directive (PPD)-- Critical Infrastructure Protection*. Washington, DC, USA: White House, 1998. [Online]. Available: https://clinton.presidentiallibraries.us/items/show/12762

[104] *SDP 2-0*, *Intelligence Doctrine for Space Forces*. Washington, DC, USA: U.S. Space Force, Dept. of the Air Force, 2023. [Online]. Available: https://www.starcom.spaceforce.mil/Portals/2/SDP%202-0%20Intelligence%20(19%20July%202023).pdf?ver=-G44px6uvwU3vIkE4R5jWw%3d%3d

[105] *SDP 3-0*, *Operations Doctrine for Space Forces*. Washington, DC, USA: U.S. Space Force, Dept. of the Air Force, 2023. [Online]. Available: https://www.starcom.spaceforce.mil/Portals/2/SDP%203-0%20Operations%20(19%20July%202023).pdf?ver=nHRhKpy49XVtcSVRaQRNNg%3d%3d

[106] *SDP 3-100*, *Space Domain Awareness Doctrine for Space Forces*. Washington, DC, USA: U.S. Space Force, Dept. of the Air Force, 2023. [Online]. Available: https://www.starcom.spaceforce.mil/Portals/2/SDP%203-100%20Space%20Domain%20Awareness%20(November%202023)_pdf_safe.pdf?ver=jcB9D6t8Pq-tzgBdoESmww%3D%3D

[107] *SDP 3-101*, *Targeting Doctrine for Space Forces*. Washington, DC, USA: U.S. Space Force, Dept. of the Air Force, 2024. [Online]. Available: https://my.spaceforce.mil/articles/sdp-3-101-targeting

[108] *Spacepower (SCP)*, *Space Capstone Publication (SCP) Spacepower*. Washington, DC, USA: U.S. Space Force, Dept. of the Air Force, 2020. [Online]. Available: https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf

[109] U. S. Department of State, *United States International Cyberspace & Digital Policy Strategy*, *United States International Cyberspace & Digital Policy Strategy*. Washington, DC, USA, 2024. [Online]. Available: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/