DEPARTMENT OF THE ARMY
UNITED STATES ARMY CYBER CENTER OF EXCELLENCE
Capabilities Development & Integration Directorate
Fort Gordon, Georgia, 30905-5735

U.S. Army

Defense of Cyberspace

Concept of Operations

Version 1.4

18 March 2019

THIS DOCUMENT SUPERSEDES ALL PREVIOUS VERSIONS
This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemption number 5 applies (internal advice, recommendations, and subjective evaluations that are reflected in records pertaining to the decision-making process of or among agencies).

Defense of Cyberspace
Concept of Operations

Table of Contents

Figures

Tables

(U) FOREWORD FROM THE CG, CYBER CENTER OF EXCELLENCE

The Army has learned much about establishing the defense in cyberspace over the last two years as it incorporated new doctrine, shaped or stood up new organizational structures, delivered advanced cyberspace operations training, created corresponding leadership and education forums, and equipped personnel within the Army's newest branch (17 series Military Occupation Specialties). The revised "Defense of Cyberspace Concept of Operations (CONOPS)" is the culmination of captured observations, insights, and lessons learned from various operations, training exercises, experimentation, evaluations, and assessments. Moreover, the revision of the CONOPS continues to demonstrate the continuing collaboration between the U.S. Army Cyber Center of Excellence (CCOE); as the capability developer; the U.S. Army Cyber Command (ARCYBER); to include the U.S. Army Network Enterprise Technology Command and Cyber Protection Brigade; and the U.S. Army Forces Command (FORSCOM), which provides expeditionary, regionally engaged, land forces to combatant commanders.

In collaboration with ARCYBER and FORSCOM, the CCOE has produced the Defense of Cyberspace CONOPS Version 1.4. The intent of the document is to further shape the Army's understanding of how it establishes the defense in cyberspace utilizing end-to-end capabilities consisting of defensive cyberspace operations, Department of Defense information network (DODIN) operations, offensive cyberspace operations, electronic warfare, intelligence, and other information related capabilities, similar to how the Army establishes the defense in the land domain. This CONOPS details the tactics, techniques, and procedures executed by applicable Army forces to prevent, shape, and win in friendly cyberspace. The concept will continue to guide future capability development by codifying cyberspace defense capabilities the Army needs to meet objectives. Additionally, the CONOPS will be used to influence science and technology, rapid technological advancement, and other evolving efforts across government, industry, and academia related to this area in order to drive evolution and change.

This CONOPS recognizes that cyberspace defense capabilities employed at critical areas of the DODIN will be essential to defeating enemies and adversaries who will challenge U.S. advantages. The Army's contribution must be comprised of unique, organic and supporting capabilities for commanders. These capabilities will enable cyberspace defenders to implement functions meant to secure, recon, maneuver, mitigate, engage, and clear against enemy activity. To do this, it is critical the Army continues to move at a speed commensurate with the dynamic nature of cyberspace, both for the operational and the institutional Army. Ultimately, this document is meant to signify the framework for the integration and innovation the Army requires for the cyberspace defense, ensuring the Army can always dominate in a complex environment.

JOHN B. MORRISON JR.
Major General, U.S. Army
Commanding

Executive Summary

(U//FOUO) This concept of operations (CONOPS) describes an operational framework for establishing the defense in cyberspace. The intent of this CONOPS is to answer the military problem: "How does the Army operationally integrate cyberspace defenders at all echelons and equip them with the required capabilities in order to establish the defense in cyberspace, similar to how it establishes the defense in the land domain"? For over a decade, the Army has possessed multiple cybersecurity solutions meant to protect and defend networks, information systems, and data against common, known threats. These solutions have enabled the Army to fulfill its United States Code (USC) Title 44 (Federal Information Security Act) responsibilities. Most recently, the Army has begun to deliver defensive cyberspace operations (DCO) capabilities to cyber warfighters (e.g. Cyber Protection Teams), which are operationalized based on mission and threat to meet USC Title 10 responsibilities.

(U//FOUO) The Army continues to acquire defensive cyberspace capabilities that offer an integrated approach for planning, securing, conducting reconnaissance/counter-reconnaissance, maneuvering and engaging, and clearing enemy activity through counter-mobility operations. More specifically, emerging cyberspace defense capabilities allow the Army to better identify and protect key and mission relevant terrain in cyberspace, actively predict and discover the existence of advanced threats and vulnerabilities within that terrain, and outmaneuver and engage adversaries – possibly beyond the perimeter of friendly networks when authorized.

(U//FOUO) As part of an integrated approach, related cyberspace defense people, processes, and technologies will be employed across global, regional, and local (base/post/camp/station (to include deployed tactical networks)) levels to achieve a defense in breadth. Key to this approach is the integration of DCO, Department of Defense information network operations, offensive cyberspace operations, electronic warfare, intelligence, and other information related capabilities. Comprehensive integration of each ensures Army forces can understand cyberspace threats and related tactics, techniques, and procedures; support and be supported by organic and expeditionary elements; and possess the ability to deny the adversary access to friendly cyberspace. Because of this necessary integration, consideration was made to ensure continued alignment with the Joint Information Environment CONOPS, Cyber Mission Force Concept of Employment, Unified Network Operations CONOPS, Army Operating Concept, and multiple Army Warfighting Functional Concepts.

(U//FOUO) The Army will continually develop capabilities commensurate with the dynamic nature of cyberspace and evolving threats to achieve freedom of action in all domains through the conduct of unified land and cyberspace operations. Subsequently, this CONOPS will remain a living document that strives to keep pace with cyber-related national, joint, and Army strategies, concepts, and doctrine, organizational, training, materiel, leadership and education, personnel, and facility and policy change decisions. In the end, the realization of an integrated cyberspace defense ensures future Army forces can prevent, shape, and win in both the land and cyberspace domains.

1. (U) INTRODUCTION

1.1 (U) Purpose

(U//FOUO) TRADOC Regulation 71-20-3 describes a concept of operations (CONOPS) as a "statement in broad outline… designed to give an overall picture and a useful visualization of how future operations will be conducted." This CONOPS describes how future operations will establish the defense in cyberspace similar to how the Army establishes the defense in the land domain. The CONOPS additionally details how cyberspace defenders will plan for the defense, maneuver to a designated network and set up battle positions, conduct surveillance and reconnaissance on decisive terrain, find the presence of cyber threats and vulnerabilities, engage and mitigate the impacts of those threats to achieve mission assurance, and eradicate them when directed. Lastly, the CONOPS provides vignettes to illustrate how cyberspace defensive actions, when integrated with intelligence, Department of Defense information network (DODIN) operations, offensive cyberspace operations (OCO), electronic warfare (EW), intelligence, and other information related capabilities (IRC), enables mission assurance.

(U//FOUO) This CONOPS leverages the Joint Information Environment CONOPS, Cyber Mission Force Concept of Employment, Unified Network Operations CONOPS, multiple capability needs analyses, the Army Operating Concept, and all Army Warfighting Functional Concepts to support the need for establishing the cyberspace defense at all echelons. Moreover, the CONOPS strives to answer the appropriate learning demands in accordance with (IAW) the Army Warfighting Challenge (AWFC) #7 (Conduct Space and Cyber Electromagnetic Operations and Maintain Communications). AWFC #7 highlights the need to assure uninterrupted access to critical communications and information links to include satellite communications (SATCOM); position, navigation, and timing (PNT); intelligence; surveillance; and reconnaissance (ISR) across a multi-domain architecture when operating in a contested, congested, and competitive environment. The learning demands (LD) associated with AWFC #7 influence and are influenced by essential elements of analysis (EEA). While this CONOPS does not focus on all LDs, the following LDs and EEAs are addressed.

- LD 7.2 What is the optimal way for the Army to organize the activities associated with Cyberspace Operations to maximize cyber capabilities across the Army Warfighting Functions while minimizing required resources?
  - EEA 7.2.1 In 2030, what is the correct skill-set for the CEMA element?
  - EEA 7.2.2 In 2030, what is the appropriate composition/echelon for the CEMA element?
- LD 7.3 What is the optimal way to employ cyber capabilities with the elements of traditional combat power to support unified land operations (ULO) and deliver the effects required by commanders at all echelons?
  - EEA 7.3.3 What echelon and with what activities should a Cyber Mission Force provide support with OCO effects?
  - EEA 7.3.4 What denial effects can be conducted within contested cyberspace to support ULO?

- EEA 7.3.5 What conditions must be attained for cyber effects (OCO, DCO, DODIN) to be most beneficial to the tactical commander at echelon?
- EEA 7.3.6 What doctrine, organizational structure, training, materiel, leadership & education, personnel, facilities, and policy (DOTMLPF-P) changes are required to employ Cyber Mission Forces?

- LD 7.8 How does the Army develop and maintain situational understanding across the range of military operations to win in a complex world?

- EEA 7.8.2 How must the Army synchronize all available sensors to answer intelligence requirements throughout area of operations without redundancy and seamlessly at all echelons?
- EEA 7.8.3 How does the Army process and exploit information at the point of collection to inform/support the lowest echelon of mission command for all domains in the future operational environments (cyberspace, subterranean, mega-cities, etc.)?
- EEA 7.8.4 How does the Army improve situational awareness amongst Coalition Forces (CF), Special Operations Forces (SOF) and Joint, Interagency, Intergovernmental, Multinational (JIIM) organizations and units throughout the operating environment, across the range of military operations?
- EEA 7.8.5 How does the Army Total Force through knowledge management and the integration of relevant information achieve a comprehensive Common Operational Picture for situational understanding in all conditions and at all echelons?
- EEA 7.8.6 How does the Army achieve situational understanding to plan, prepare, execute and assess operations at all echelons under degraded network conditions?

(U//FOUO) This CONOPS provides context for cyberspace defense (Chapter 2), states the military problem (Chapter 3), describes the associated concept of operation and presents a doctrinal hierarchy (Chapter 4), and highlights the solutions required (Chapter 5). The CONOPS includes two vignettes that illustrate the application of cyberspace defense actions in support of corps and below commanders (Appendix B), as well as Army business operations (Appendix C). Also included are a list of recommended Army universal tasks related to the cyberspace defense (Appendix D), glossary and terms (Appendix E), and a description of how to perform Intelligence Preparation of the Battlefield to support the cyberspace defense. This CONOPS establishes a foundation on which to build; it provides a common lexicon to guide further operational and institutional efforts. Lastly, it strives to influence science and technology, evaluations and assessments, rapid technological advancement, and other evolving efforts across government, industry, and academia in order to drive continued evolution and change.

1.2 (U) Scope

(U//FOUO) This CONOPS codifies how the Army; while executing unified land and cyberspace operations; will integrate capabilities in order to preserve the use of data, networks, net-centric capabilities, and other designated systems. The timeframe for the CONOPS spans from the present to 2025. It takes into consideration Force 2025 and beyond. Moreover, the CONOPS is influenced by ongoing DOTMLPF-P efforts to address requirements for cyberspace support at the corps and below. The CONOPS focuses on the collective ability of organic and expeditionary elements at the strategic, operational, and tactical levels. Since relationships between the Army

and mission partners are also important, this CONOPS highlights, where applicable, specific concerns cyberspace defenders need to factor when integrating operations with coalition forces or providing defense support to host nation/civil authorities.

2. (U) CONTEXT FOR CYBERSPACE DEFENSE

(U) This chapter establishes the context for the cyberspace defense, influenced by Army doctrine, strategic plans and studies, the operational environment (OE), and research and analysis contained in Army and joint cyberspace capabilities needs analyses.

2.1 (U) Doctrine

(U//FOUO) Joint and Army doctrine provide clear and strong context for cyberspace defense. First by establishing the importance of the defense and framing it in the context of cyberspace. Second, joint and Army doctrine establish the requirement for the Army to conduct cyberspace operations, and then state the need to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.

(U//FOUO) Joint doctrine addresses the importance of cyberspace operations to achieve mission assurance. JP 3-12(R), Cyberspace Operations, states cyberspace defense is an action requiring the employment of various capabilities to create specific effects, categorized by intent, for the purpose of securing, operating, and defending the DODIN. For the Army, specific focus is placed on the defense of the DODIN-Army (DODIN-A). Cyberspace defense includes activities such as protection, detection, characterization, countering, and mitigation. These actions are usually created or controlled by the entity that owns, operates, or provides support to the DODIN, except in cases where these actions would impact the operations of networks outside the responsibility of the respective owner.

(U//FOUO) Army Doctrine Publication (ADP) 3-0, Unified Land Operations, first introduced the integrating function of cyber-electromagnetic activities (CEMA) as one of four primary staff tasks.[1] CEMA were later defined in Army Doctrine Reference Publication (ADRP) 3-0 as "activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system."[2] Most recently, FM 3-12 (Cyber and Electronic Warfare Operations); approved in April 2017; describes how the Army plans, integrates, and synchronizes cyberspace operations through CEMA as a continual and unified effort. The continuous planning, integration, and synchronization of cyberspace and EW operations, enabled by spectrum management operations, can produce singular, reinforcing, and complementary effects.

(U//FOUO) Army Doctrine Reference Publication (ADRP) 3-90, Offense and Defense, and Army Doctrine Publication (ADP) 3-90, Offense and Defense, describe tactics for the defense in the land domain. They are easily transferrable and applicable to the cyberspace domain. Army forces conduct cyberspace defensive tasks as part of major operations and joint campaigns, while

[1] Army Doctrine Publication (ADP) 3-0, Unified Land Operations, November 2016.
[2] Army Doctrine Reference Publication (ADRP) 3-0, Unified Land Operations, November 2016.

simultaneously conducting DODIN operations and requesting the delivery of OCO effects as part of decisive actions. In the defense, commanders and other leaders must choose how, when, and where to employ limited assets (weapons systems, obstacles, ISR, etc.) to retain decisive terrain, regain the initiative, or deny a vital area to the enemy. Commanders ultimately strive to identify, or fix the enemy as a prelude to the offense. As a supporting publication to ADP 3-90, FM 3-90-2 (Reconnaissance, Security, and Tactical Enabling Tasks) stresses the importance of conducting reconnaissance on key terrain as part of the defense by stating, "The security force aggressively and continuously seeks the enemy and reconnoiters key terrain. It conducts active area or zone reconnaissance to detect enemy movement or enemy preparations for action and to learn as much as possible about the terrain. The ultimate goal is to determine the enemy's course of action (COA) and assist the main body in countering it. Moving security forces perform zone, area, or route reconnaissance along with using observation posts to detect enemy movements and preparations".[3]

(U//FOUO) ADP 2-0, Intelligence, creates the context for the cyberspace defense through intelligence operations. Intelligence supports the commander's defensive tasks with Intelligence Preparation of the Battlefield products to identify probable threat objectives and various approaches; patterns of threat operations; and the threat's ability to counterattack. Intelligence supports the commander's use of information collection assets to visualize the terrain [in cyberspace], determine cyberspace threat strengths and dispositions, and confirm or deny threat COAs. Intelligence organizations residing within conventional Army units will leverage reach-back combined with an organic information collection effort to inform cyberspace defenders at their level. Defending forces then decide how to array assets in an economy-of-force role to shape the battlefield.[4] Maneuver commanders know what this means in other domains – the Army must then explain how the terms terrain, obstacles, weapons platforms, and other warfighting language applies to cyberspace operations. The concepts are the same, but the means of achieving objectives can be very different.

(U//FOUO) FM 6-02, Signal Support to Operations, further sets the context for the cyberspace defense by highlighting the need to leverage Network Operations (NetOps) [DODIN operations] and SMO to establish a secure and defensible network. FM 6-02 states, "[DODIN operations] create and preserve information assurance [cybersecurity] on the Department of Defense information networks. These include proactive technical functions such as configuration control, system patching, cybersecurity (formally information assurance (IA)) measures and user training, physical security, secure architecture design, operation of host-based security systems and firewalls, and encryption of data at rest. Many DODIN operations activities are regularly scheduled events and the aggregate effect establishes the security framework on which all missions ultimately depend."[5]

2.2 (U) Operational Environment

(U//FOUO) Persistent conflict continues to evolve within the cyberspace domain. A variety of opponents will continually contest multiple aspects of the OE with differing synchronous and

[3] Field Manual (FM) 3-90-2, Reconnaissance, Security, and Tactical Enabling Tasks, March 2013.
[4] Army Doctrine Publication (ADP) 2-0, Intelligence, 31 August 2012.
[5] Field Manual (FM) 6-02, Signal Support to Operations, 22 January 2014.

asynchronous capabilities across the range of conflict, from major combat to stability operations. To appreciate the role and capabilities of cyberspace defense, it is important to understand the OE, the variables that influence the OE, and the ways in which the OE may affect operations in cyberspace.

2.2.1 (U) Cyberspace

(U//FOUO) IAW JP 3-12(R), dated 5 February 2013, cyberspace is defined as "…the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". In the past, the OE contained components of what is now included in cyberspace (such as routers, fiber optic cables, and servers). But those components were merely regarded as devices to complete the mission. Today, the integration of the IT within our facilities, vehicles, weapons, and Soldiers, and the ever-increasing reliance on IT has led to the realization that this collection of systems and networks must be treated as a domain.

(U//FOUO) Recognizing and fully understanding cyberspace as a domain is the first step in describing operations in cyberspace. Similar to the land domain, cyberspace must be defended and an effects-based approach to operations must be applied in order to gain a certain level of control. As in other domains, control parameters are affected by the characteristics of the environment.

(U//FOUO) Cyberspace has characteristics that differ from land, air, maritime, and space. These characteristics affect how the Army operates and defends networks, information systems (to include weapon systems), and data. Effective attributes of cyberspace, unlike the other domains are man-made and integrated with the private sector (which the Army does not own or have direct control of). The fact that cyberspace is man-made implies malleability – which is a key aspect of developing scheme of maneuver for operations. JP 3-12(R) models cyberspace as having separate layers (physical, logical, and cyber-persona), and the dominance of each has vastly different meaning:

- The physical layer component is comprised of network transport (wired, wireless, cabled links, electromagnetic spectrum (EMS) links, satellite, and optical) and communications infrastructure (wires, cables, radio frequency, routers, switches, servers, and computers). However, the physical layer uses logical constructs as the primary method of confidentiality, integrity, and availability (e.g., virtual private networks that tunnel through cyberspace). It is the first point of reference for determining jurisdiction and application of authorities.

- The logical layer consists of those elements of the network that are related to one another in a way that is abstract from the physical layer (e.g. the form or relationships are not tied to an individual, specific path, or node). A simple example is any web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator. The logical layer includes various routing and switching protocols, operating systems, network services, and host applications.

- The cyber-persona layer represents yet a higher level of abstraction. It uses rules applied in the logical layer to develop a digital representation of an individual or identity. The cyber-persona layer consists of the people actually on the network. It may relate directly to an actual person or entity, incorporating some data, e-mail and internet protocol (IP) address(es), web pages, phone numbers, etc. However, one individual may have multiple cyber-persona, which can vary in the degree to which they are factually accurate. Reversely, a single cyber-persona can have multiple users. As a result, this makes attribution in cyberspace difficult.

(U//FOUO) Connections between various layers of cyberspace generate a portion of the information environment (IE). The IE is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. It is broken down into the physical, informational, and cognitive dimensions; and each layer is associated with a specific dimension:

- The physical dimension is composed of command and control (C2) systems and supporting infrastructure that enable individuals and organizations to conduct operations. It is the dimension where physical platforms and the networks that connect them reside. The physical dimension includes; but is not limited to; fiber optic cables, computers, and networking devices.

- The informational dimension is the place where information is collected, processed, stored, disseminated, and protected. Information is disseminated via virtual routes over physical networks and stored within virtual file systems either on the local hard drive or in the cloud. Ultimately, actions in this dimension affect the content and flow of data.

- The cognitive dimension encompasses the minds of the person or persons who transmit, receive, and respond to or act on information. In this dimension people think, perceive, visualize, understand, and decide.

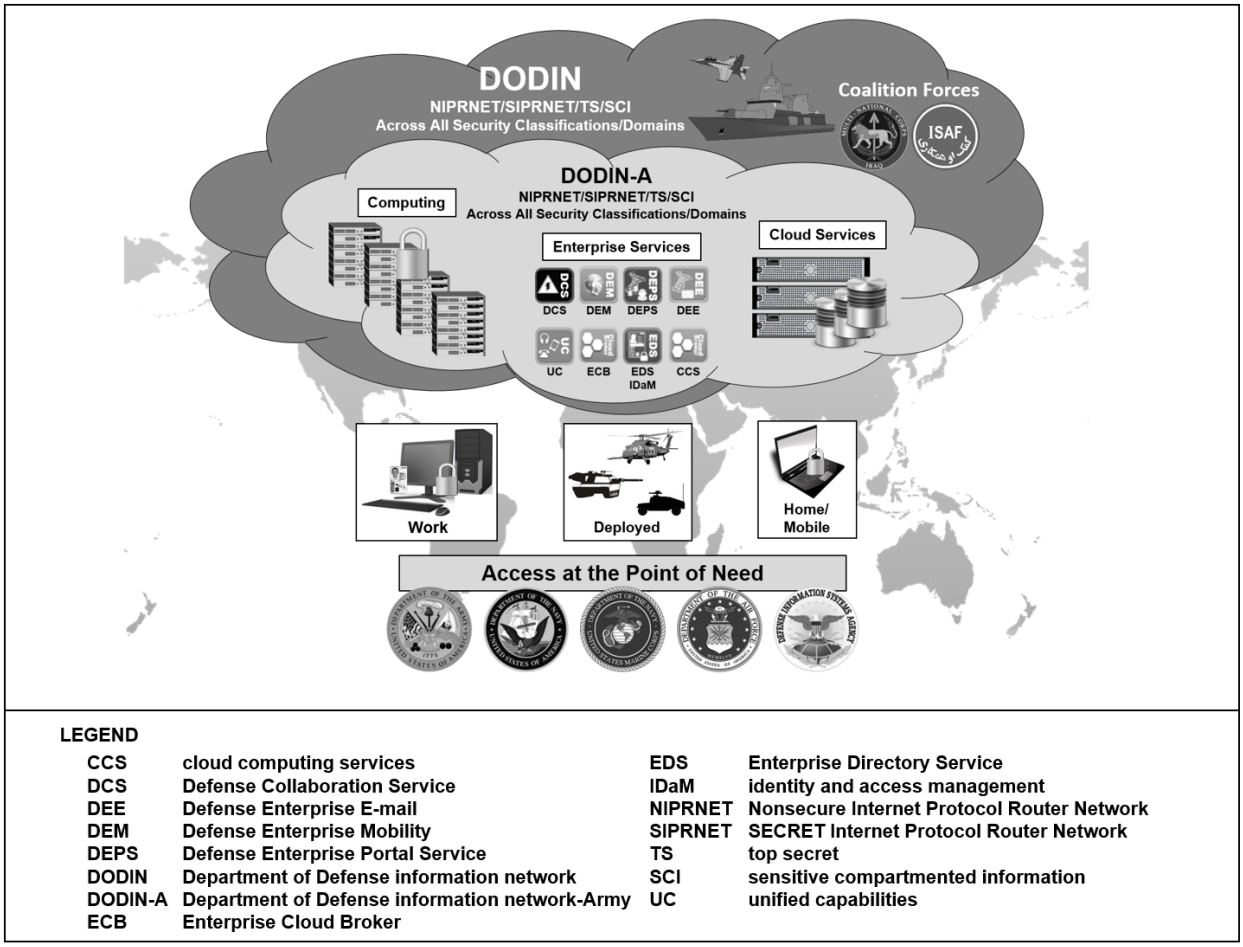
2.2.1.1 (U) Friendly (Blue) Cyberspace

2.2.1.1.1 (U) Department of Defense Information Networks

(U//FOUO) JP 3-12(R) defines the DODIN as:

... The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

(U//FOUO) Figure 1 depicts the DODIN-A as a subset of the DODIN. The DODIN-A is the Army's critical warfighting platform, which enables mission command, fires, intelligence, and other warfighting functions. It provides commanders, staffs, Soldiers, and civilians access to the right information at the right time. It offers connectivity while individuals are at home station, a temporary duty location, or in a deployed environment. These segments enable operating and generating forces to access centralized resources from any location during all operational phases.



LEGEND			
CCS	cloud computing services	EDS	Enterprise Directory Service
DCS	Defense Collaboration Service	IDaM	identity and access management
DEE	Defense Enterprise E-mail	NIPRNET	Nonsecure Internet Protocol Router Network
DEM	Defense Enterprise Mobility	SIPRNET	SECRET Internet Protocol Router Network
DEPS	Defense Enterprise Portal Service	TS	top secret
DODIN	Department of Defense information network	SCI	sensitive compartmented information
DODIN-A	Department of Defense information network-Army	UC	unified capabilities
ECB	Enterprise Cloud Broker		

Figure 1. (U//FOUO) DODIN-A Operational View

2.2.1.1.2 (U) Net-Enabled Warfighting Platforms

(U) The Army must recognize the fact most of its weapons systems (e.g. Patriot Missile System, M1A2 Abrams Tank, etc.) are network-enabled. Warfighting networks ensure platforms, sensors, weapons, and systems can seamlessly exchange warfighting data and information via machine-to-machine interfaces. Such advanced capabilities involve tactical targeting network technology that integrates with airborne platforms to increase the capability to track and engage targets in dense threat environments. Advanced tactical data link waveforms that track capacity and enhance other performance characteristics assured PNT for Ground Positioning Systems and aggregation of data providing system C2. Loss of communications to and from these systems render them combat ineffective or can even result in aircraft or munitions veering off course – with the potential for loss of life.

2.2.1.1.3 (U) Mission Partners Environments

Army forces conduct operations as part of a joint, interdependent force. In addition, they routinely work with multinational forces and interagency, intergovernmental, and non-

governmental partners as part of unified action. As such, the Army must consider how it will defend friendly cyberspace when integrating with these mission partner environment.

- **Joint Considerations.** Army forces conduct operations as part of a joint, interdependent force. In addition, they routinely work with multinational forces and interagency, intergovernmental, and non-governmental partners as part of unified action. Operations that involve the use of cyberspace have joint implications. Each Service component implements some level of cyberspace defense that contributes to an integrated whole, synchronized by a joint force headquarters aligned to a combatant command (COCOM). Army units may also work as subordinate elements of a joint task force.

- **Interagency and Intergovernmental Considerations.** The Army must consider the unique capabilities, structures, and priorities of interagency and intergovernmental partners when establishing the cyberspace defense. Successful execution of the defense with mission partners requires a shared understanding and common objectives. Interagency and intergovernmental partners often have network architectures, data classification standards, and governance processes that can vary greatly from the Army. This will generally require liaison elements to be in place before operations, as it will likely be too late and ineffective to establish these elements after the-fact. Cyberspace defenders must ensure interagency and intergovernmental planners clearly understand Army cyberspace defense capabilities, requirements, operational limitations, liaisons, and legal considerations.

- **Multi-National and Coalition Considerations.** Just as with interagency and intergovernmental partners, the Army may be required to establish the cyberspace defense in conjunction with multi-national coalition partners. Differences in national standards and laws pertaining to sovereignty in cyberspace may affect the willingness or legality of a country's participation. Some partners may refuse to participate, while others will enable or undertake their own cyberspace defense separate from the Army's. Cyberspace provides essential communications between multinational forces in mutual support during operations. Cyberspace defense issues may be compounded by interoperability constraints. Hardware and software incompatibilities and disparities in standards, cybersecurity solutions, and policies may cause gaps in the defense that require additional efforts to fix.

- **Non-Governmental Considerations.** Commanders ensure adherence to cyberspace defense principles when conducting cyberspace operations with non-governmental organizations. Integration with non-governmental organizations may be necessary for foreign humanitarian assistance, peace operations, and civil support operations. Incorporation of these organizations into the overall network requires a balance between the need of the non-governmental organization to share data and collaborate with Army forces. Many non-governmental organizations may be hesitant to provide access or integrate their network with the DODIN to prevent compromising their status as independent entities.

- **Host Nation Considerations.** Each nation has sovereignty over its cyberspace components within its geographic area. A nation's portion of cyberspace includes television stations, radio stations, financial networks, government networks, etc. Defending these networks requires coordination and negotiation through formal diplomatic communication channels. This

coordination ensures supportability for operations and establishes approved and pre-coordinated cyberspace availability and assured access. Additionally, coordination allows for the development of an interoperable cyberspace defense capability. Considerations for coordination with adjacent countries, particularly those countries where our forces stage, train, or operate. Likewise, coordinated protective measures, and countermeasures are essential to avoid any potential cyberspace fratricide.

- **Private Industry Considerations.** Private industry plays a significant role in cyberspace. The Army relies on its connectivity with its defense industrial base partners and the private industry for many of its non-warfighting day-to-day functions for support and sustainment. Examples include electronic databases and interfaces for medical services, accounting and finance services, personnel records, equipment maintenance, and logistics functions. Global transport and logistics require data exchange between military and private networks. The Army relies on shipping companies, transportation grid providers, and suppliers as a part of the global transportation system. The security and reliability of private industry networks directly affects Army operations.

2.2.1.1.4 (U) Supervisory Control and Data Acquisition/Industrial Control Systems

(U) Supervisory control and data acquisition (SCADA) is a control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management. SCADA systems (for which HQDA G-3/5/7 terms “Operational Technology”) incorporate the use of other peripheral devices such as programmable logic and discrete controllers to interface with industrial control systems (ICS). Industrial control systems manage the delivery of electricity, water, fuel, and other vital services necessary for day-to-day operations on most Army installations, not to mention delivery of these services to the rest of the populace.

(U) Any denial, disruption, or degradation of industrial controls systems hampers the force projection power of Army forces to anywhere in the world. Without power, logistics and transportation specialist cannot coordinate the delivery of ammunition or parts. Denial, disruption, or degradation of fuel or water to the nation would cause mass chaos similar to what was experienced during the aftermath of Hurricane Katrina. The ability for nation-state adversaries to impact the functionality of SCADA/ICS becomes a deterrent for the U.S. to flex elements of national power in support of policies or strategic goals. Subsequently, SCADA/ICS must be considered when establishing the overall cyberspace defense.

2.2.1.2 (U) Neutral (Gray) Cyberspace

(U//FOUO) Neutral cyberspace is that which is not in the direct control of friendly or adversary forces. The cyberspace connections (wired or wireless) across publically accessible networks are sometimes viewed as a gray space; however, some entity installed, operates, and manages all portions of cyberspace. Because someone built each node and connection, gray networks should not be viewed as an unconstrained global commons. It is more like a man-made information highway occupied by private citizens, host nations, industry, and academia, along with innumerable social networks, collaborative and educational forums, peer-to-peer services, and

numerous criminal, state, and non-state threat actors. Unfortunately, many Army and DOD network routes ride over this information highway for which the Army has limited to no authorities to operate within this space during the absence of control. Since private industry is the primary catalyst for commercial assets and global supply chains, the Army has become increasingly reliant on providers for which the Army has no direct influence to mitigate risk effectively. The Army must work with federal, state, and local partners; along with the academic and private sectors; to meet the challenge of conducting operations in cyberspace.

2.2.1.3 (U) Adversary (Red) Cyberspace

(U//FOUO) Adversary cyberspace is that portion of the cyberspace domain for which cyberspace threats have continuous access to operate in order to conduct cyberspace operations without the fear of repercussion. Unfortunately, red cyberspace is often protected by being separated from worldwide connections. Also, adversary activity in cyberspace is more times than not non-attributable. This is mainly due to the logical and anonymous nature of networks and the physical nature of computer code and commands. While it is possible to capture and quarantine an intruder's implanted code or tool, it is difficult or impossible to physically capture an intruder in cyberspace. They do not need to be in the same building or same country in order to be in targeted computers, and "cyber forensic footprints" are challenging to backtrack or attribute to legal standards of certainty. In the past, only a handful of adversaries had the ability to conduct OCO against friendly forces; but today, a wide range of actors utilize advanced technologies that represent an inexpensive way to pose a significant threat to the Army. The application of low-cost cyberspace capabilities used by the adversary can result in disproportionate effects against Army forces that have become dependent on cyberspace and its ability to enhance ULO. Potential adversaries see the use of cyberspace as a much cheaper, clandestine, and quicker method to achieve their objectives in comparison to more traditional or non-technical measures.

2.2.2 (U) Cyberspace Threats

(U//FOUO) A cyberspace threat is any circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a system resulting in a loss of confidentiality, integrity, or availability (see Army Regulation 25-2 (Cybersecurity/Information Assurance) for the definition of these terms). As defined here, cyberspace threats not only involve an action but also require actors (threat agents) to execute that action in order to exploit cyber weaknesses and generate denial effects that disrupt, degrade, destroy, and manipulate friendly use of information.

2.2.2.1 (U) Cyberspace Threat Agent Categories

(U//FOUO) Several primary threat agent categories, methodologies, and intents exist (*the following is not an all-inclusive list of documented categories and sub-elements of those categories*):

- **Hackers.** Develop/use damaging code to break into private networks with the intent of exfiltrating, modifying, or deleting critical data.

- **Organized Crime.** Exploits online activity, hires hackers, and bribes insiders in order to achieve monetary gain.

- **Terrorists.** Hack or exploit networks to acquire information for planning physical or cyberspace attacks on command and control systems.

- **Nation-States.** Use offensive cyberspace capabilities for widespread impact from the performance of denial, degradation, disruption, destruction, manipulation, and data exfiltration. Nation States may also employ and/or recruit hackers, organized crime, terrorists, and insiders to conduct activities that hold targets at risk, creating a more dispersed and diversified cyberspace threat which further complicates DCO and intelligence requirements.

- **Insider Threats.** Willfully or naively violate policy and procedures by not complying with the user agreement (opening the network up to social engineering and malware-like attacks); or insiders maliciously abuse their access privileges and exfiltrate data from friendly networks because they are disgruntled or disagree with the operations of the organization.

2.2.2.2 (U) Cyberspace Threat Capabilities

(U//FOUO) Threat actions against the Army networks are meant to deny, degrade, disrupt, destroy, control, or otherwise adversely affect friendly forces ability to use cyberspace in support of objectives. Because networks consist of many different segments across traditional domains, with many different means of communicating and differing levels of interconnectivity and isolation, a wide continuum of capabilities are available to the threat in order to conduct offensive operations in the Army's portion of the DODIN (to include U.S. Army Corps of Engineers (ACE), Defense Research and Engineering Network (DREN), and tactical network space). These capabilities target any portion of friendly networks ranging from particular physical nodes and links to the actual data resident in those nodes and links.

(U//FOUO) Effective offensive operations holistically address the EMS, communications networks, information services, and associated physical infrastructure. Offensive operations include cyberspace attacks, electronic attacks (jamming of the EMS), physical attack against infrastructure and electronics; as well as exploitation type activities against friendly networks or the EMS.

- **Cyberspace Attack.** Cyberspace attack is a cyberspace action that creates various direct effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial, that is hidden or that manifests in the physical domains These specific actions are:

- **Electronic Attack (EA).** An EA is a subdivision of electronic warfare where actions are taken to prevent or reduce the adversary's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception. EA uses electromagnetic energy, directed energy, and anti-radiation weapons to attack radio frequency capabilities tied to personnel, facilities or

equipment with the intent of degrading, neutralizing, or destroying the adversary's combat capability.

- **Physical Attack.** While not a cyberspace operation, a physical attack uses measures to physically destroy or otherwise adversely affect a target. Because networks in cyberspace can be isolated, the ability to *kinetically* attack a network node may still be required. Physical attack can create effects within and outside cyberspace to help control the domain. Regardless of the degree of isolation, the adversary may determine a direct physical attack is the best option depending on the situation, the desired effect, and availability and suitability of other capabilities or options.

- **Cyberspace Surveillance and Reconnaissance.** The adversary must continuously gather intelligence within the Army's portion of the DODIN in order to effectively execute offensive operations. Successful intelligence gathering requires access to friendly activities and networks. Cyberspace Surveillance and Reconnaissance (S&R) and electronic warfare support are two types of intelligence operations performed within cyberspace. Cyberspace S&R reveals information resident on or in transit through a system. Adversarial intelligence operations can reveal vital information about Army networks.

(U//FOUO) Adversary offensive operations in cyberspace can cause effects to communications, mission command, and the execution of other warfighting functions (such as fires). The adversary's ability to access cyberspace can result in a change to the information residing on Army systems. This change can influence future friendly actions and/or lead to reduced confidence in the information provided; subsequently degrading situational understanding.

2.2.2.3 (U) Advanced Persistent or Sophisticated Threat

(U//FOUO) While the majority of cyberspace operations are conducted against the common, known cyberspace threat, the primary focus for cyberspace defenders conducting DCO must be the Advanced Persistent Threat (APT) or sophisticated cyberspace threat. An APT or sophisticated cyberspace threat conducts OCO, gains access to a target network, and operates undetected (sometimes for a long period). To maintain access without discovery, the attacker must continuously rewrite code and employ sophisticated evasion techniques. A goal of an APT or sophisticated cyberspace threat is to conduct a raid to exfiltrate data, recon the network and systems to determine key cyber terrain, and/or manipulate/destroy data.

2.3 (U) Elements of the Cyberspace Defense

(U) The establishment of the cyberspace defense requires the integration of cyberspace capabilities, EW, Intelligence, and other IRCs. Each have unique inter-relationships, which enables the synchronized, real-time execution of decisive actions meant to retain key terrain or deny a vital area to the enemy; attrit or fix the enemy as a prelude to other actions, surprise the enemy, and increase the enemy's vulnerability by forcing it to expose more of its assets. The relationship builds on traditional approaches to defending Army networks and systems to address the APT.

(U) It is important to note, the establishment of the "cyberspace defense" is an action, on par with conducting cyberspace ISR, cyberspace attack, and cyberspace operational preparation of the environment (OPE), which requires the employment of various capabilities to create specific effects in cyberspace. Specific effects include; but are not limited to; block, contain, fix, isolate, and neutralize. Cyberspace defense actions are normally performed to secure, operate, and defend the DODIN. Cyberspace defense actions are either dynamic or static. They consist of direct tasks to plan, secure, recon, maneuver against, and counter the effectiveness of an advanced cyberspace threat either attacking or preparing to attack friendly, net-enabled capabilities. This type of defense includes the dynamic employment/redeployment of cyberspace warfighting capabilities. A dynamic cyberspace defense facilitates the near-real time ability to find, fix, and finish the enemy within an area of operations. Static actions are measures, other than dynamic, taken to minimize the effectiveness of all cyberspace threats within an area of responsibility against friendly, net-enabled capabilities. These measures include perimeter protection, access control, attack sensing and warnings, and redundancy within a network. Passive cyberspace defense improves survivability by reducing the risk of common/known cyberspace threats and vulnerabilities impacting the day-to-day operation of the network.

2.3.1 (U) Cyberspace Defense Objectives

(U//FOUO) The primary goal of the cyberspace defense is to gain/ensure freedom of action in and through the domain, while denying the adversary the same. The employment of defensive capabilities creates specific effects in cyberspace through actions that allow commanders to achieve the following objectives:

- **Deter, Destroy, and/or Defeat Enemy Offensive Cyberspace Operations.** The primary purpose of establishing the cyberspace defense is to deter, destroy, and/or defeat enemy OCO. Successful defenses fix on the enemy and create opportunities to seize the initiative. Cyberspace defensive actions will deter potential aggressors if they believe an attempt to break friendly cyberspace defenses is futile or too costly. If the enemy does decide to conduct OCO, the cyberspace defense should be strong enough to prevent the enemy from realizing its intentions, while retaining operational freedom for friendly forces. Ultimately, the goal is to temporarily or permanently diminish the enemy's will to fight.

- **Gain Time.** Commanders employ defensive measures to gain time and complete the specified mission. Delaying actions trade space for time to improve defenses, expose enemy cyber forces to attack, and prepare response actions. Such measures succeed by slowing or halting an attack while allowing friendly reserves enough time to reinforce the defense and attrit or fix the enemy as a possible prelude to offensive actions. This is an overlooked aspect of operationalizing the domain – if the Army has a critical mission, it should be able to defend critical assets for the duration of the mission.

- **Economy of Force.** Cyberspace defense using organic and expeditionary/augmentation capabilities is also meant to achieve economy of force. Astute employment of cyberspace assets focused on data flows and decisive points allows commanders and other leaders to minimize resources used defensively. This will enable concentration of cyber power for other operations.

- **Control KT-C.** The intent of the defense is to retain decisive terrain or deny a vital area to the enemy. Such defenses are necessary to prevent enemy forces from doing the opposite. Control of KT-C can sway the outcome of a mission depending on which side owns it.

- **Protect MRT-C and Infrastructure.** Defense of vital cyberspace assets supports ULO and allows Army forces to achieve mission assurance. Units will defend areas of Army cyberspace that enable it to conduct its mission and provide indirect support to other operations. MRT-C can change with the phases of an operation – establishing the cyberspace defense is not a one-time event, but rather a dynamic, maneuver-enabled operation.

- **Develop Intelligence.** As with the offense, the defense may develop and gather intelligence that is required to conduct current or future operations. Cyberspace defensive actions support active cyberspace ISR that focuses on tactical and operational intelligence and seeks to map friendly and adversary cyberspace to support military planning. The more successful the defensive measures, the more Army forces learn about the enemy. A particular phase or task within a defense may be conducted to satisfy the Commanders Critical Information Requirements (CCIR) about the enemy's objective and main effort.

2.3.2 (U) Cyberspace Defense Principles

(U) Five principles apply to the cyberspace defense: full dimension, layered, redundant, integrated, and enduring. These principles are not a checklist and may not apply the same way in every situation, but they provide cyberspace defenders a context for implementing efforts, developing strategies, and allocating resources. The following briefly describes each principle:

- **Full Dimension.** The cyberspace defense is not a linear activity; it is continuous and asymmetrical. Efforts and activities must consider and account for cyberspace threats in all directions, at all times, and in all environments. Subsequently, to realize the principle of full dimension, cyberspace defense activities and capabilities must be integrated with OCO and intelligence to expand efforts through blue, red, and gray cyberspace. Cyberspace defense planning, coordination, and implementation occur anywhere the defense of information and information systems are required. Situational awareness supports this principle and leads to the proper response.

- **Layered (Defense-in-Depth).** Cyberspace defensive capabilities must be layered to provide strength and depth to the overall network (defense-in-depth). This also serves to reduce the destructive effect of a threat through the dissipation of energy or the culmination of force. Defense-in-depth may also provide time to focus identification, assessment, target acquisition, or response efforts and actions.

- **Redundant.** Redundancy ensures that specific activities, systems, efforts, or capabilities critical for the success of the overall cyberspace defense effort have a secondary or auxiliary purpose of equal or greater capability. Redundant capabilities are not duplicative, as they emphasize the overlapping of capabilities utilizing different means so there are no seams in the defensive posture. Redundancy may not be achieved in all defensive measures, resulting in the need to identify the critical point of failure or critical path associated with each major cyberspace

defensive action, system, effort, and capability to ensure redundancy is applied. Defensive efforts are often redundant and overlapping anywhere vulnerability, weakness, or failure is identified or expected.

- **Integrated.** The cyberspace defense is integrated with all other cyberspace operations (e.g. OCO and DODIN operations), EW, intelligence, and IRC activities, systems, efforts, and capabilities to provide strength and structure to the overall effort. Integration must occur vertically and horizontally across organizations and network tiers in all phases of operations. Cyberspace defense integration should complement the conduct of warfighting functions in the domain without significantly inhibiting other operations in and through cyberspace.

- **Enduring.** Cyberspace defense has an enduring quality that differentiates it from the conduct of DCO or specific security activities. Cyberspace defense has a persistent character that serves one dominant purpose – the preservation of the defended assets and capabilities. The enduring character of the cyberspace defense may affect freedom of action and resource allocation.

(U) The inherent strengths of the cyberspace defense include the defender's ability to access friendly networks, information systems, and data before the attack and use the available time to prepare. Commanders and other leaders choose to defend net-enabled capabilities to create conditions for mission success. A feature of the defense is a striving to regain the initiative from an attacking enemy. Defending forces integrate the following elements to help accomplish that task.

2.3.3 (U) Cyberspace Terrain Terms of Reference

(U) A critical element of the cyberspace defense is the ability to allocate virtual terrain by establishing areas of responsibility, areas of operation, and other specific locations within the domain. This is done through effective terrain analysis meant to collect, analyze, evaluate, and interpret characteristics on the features of the terrain, combined with other relevant factors, to predict the effect of the virtual terrain on unified land and cyberspace operations. To ensure understanding across the Army (and potentially beyond), this CONOPS provides several terms of reference related to friendly cyberspace terrain.

(U) Although cyberspace cannot be delineated geographically, the terms "area of responsibility" and "area of operations" (AO) still apply. It is important to note, while areas of responsibility for a network may not contain virtual AOs, a virtual AO cannot be established without a commander or other leader possessing the authority (responsibility) to plan and conduct DODIN operations. An AO in friendly cyberspace is defined by a commander or other leader; and it comprises all the critical net-enabled components necessary to accomplish a mission and secure cyberspace capabilities. Within a virtual AO resides key terrain in cyberspace, mission relevant terrain in cyberspace, critical assets, defended assets, battle positions, main battle areas, security areas, avenues of approach, and named areas of interest.

2.3.3.1 Observation, Avenues of Approach, Key Terrain, Obstacles, and Cover and Concealment

(U) The military aspects of virtual terrain are influenced by observation, avenues of approach, key terrain, obstacles, and cover and concealment (OAKOC). Defenders assigned an AO are responsible for terrain management within its boundaries. A higher headquarters may dictate that another element position itself within a subordinate element's AO, but the commander assigned the AO retains final approval authority for the exact placement. This ensures the unit commander controlling the AO knows what units are in that AO, and what missions they have been given. This allows defenders to deconflict operations, control movement, and prevent virtual fratricide. Military aspects of OAKOC are described as follows:

- **(U) Observation and Avenues of Approach.** Observation is achieved by setting the conditions in friendly cyberspace that permits defenders to see the friendly, adversary, and neutral aspects of the environment. Observation is conducted from virtual observation posts in order to direct and adjust actions, as well as execute appropriate communications. The primary observation post should cover the adversary's most likely avenue of approach into a virtual AO. An avenue of approach in cyberspace is a virtual route (physical, logical, and social) for which an attacking force of a given skill uses to achieve objectives or gain access to key terrain in its path.

- **(U//FOUO) Key Terrain in Cyberspace, Mission Relevant Terrain in Cyberspace, and Defended Assets.** The recognition of cyberspace as a domain for military operations drives the need to determine what constitutes key terrain in cyberspace (KT-C). For the purpose of this CONOPS, KT-C is any locality, or area, for which seizure, retention, or control affords a marked advantage to a combatant. KT-C consists of those physical, logical, and cyberspace persona elements of the network that enable mission essential functions. These might include major lines of communications; key access points for the defense, observation and launch points for the offense; or opportunities to create bottlenecks. In cyberspace, key terrain involves network links and nodes (or even individual administrator accounts) that are essential to a particular friendly or adversary capability. While the Army as a whole may consider elements across friendly (blue), neutral (gray), and adversary (red) as KT-C, references to it in this CONOPS specifically apply to friendly cyberspace assets and capabilities that allow the Army to conduct net-enabled operations; and therefore, must be defended in depth.

(U//FOUO) Even though cyberspace has many unique characteristics, the general concepts of "terrain" hold true. In a defense-in-breadth strategy, cyberspace terrain includes physical and logical infrastructure and mission data. The process of identifying key and mission relevant terrain in cyberspace (MRT-C) focuses on the technical environment (e.g. types of transport, types of operating systems, types of information services), relationships between physical and cyberspace elements, and linking missions and mission dependencies with the technical environment, as well as with the physical, logical, and cyber-persona layers. Identifying KT-C is extremely dynamic in nature. Determining it requires a continual process based on mission, enemy, terrain, troops and support available, time available, and civil considerations (METT-TC). During continued engagements in the cyberspace domain, KT-C will change rapidly as the enemy changes its tactics, techniques, and procedures (TTP) and objectives. In order to identify KT-C in friendly cyberspace, a complete understanding of the operating environment is required. This may be aided by mapping MRT-C for critical assets and capabilities.

- **Obstacles.** Obstacles in friendly cyberspace are any physical, logical, or persona obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in time and capability on the opposing force. When planning obstacles, cyberspace defenders consider not only current operations but also future operations. Defenders should design obstacles for current operations so they do not hinder future operations. Any network operator or cyberspace defender authorized to employ obstacles can designate certain obstacles to shape the environment as high-priority reserve obstacles. Cyberspace defenders integrate reinforcing obstacles with existing obstacles to improve the restrictive nature of the virtual terrain to halt or slow enemy movement, canalize enemy movement into engagement areas, and protect critical assets. At all possible, obstacles should be concealed from enemy observation. Improvement to the defensive is continuous. Given time and resources, the defending force constructs additional obstacles. Defenders at each level must coordinate to determine which entity is responsible for establishing and securing each obstacle. When determining what obstacles to employ defenders should ask; what controls, blocks, distracts, or impediments (physical or logical) make it difficult for an enemy to gain access? What obstacles can be removed in support of friendly forces? What obstacles can be added in support of deterring adversaries? How quickly can obstacles be deployed or mitigated in the operating environment.

- **Cover and Concealment.** Cover and concealment in friendly cyberspace are those measures necessary to give protection to a critical asset, plan, or operation from the enemy intelligence and surveillance efforts. Ultimately, cover and concealment is a security task to protect MRT-C by execution countermeasures to gain time while also observing and reporting information and preventing enemy observation of and attack against mission critical systems. When considering cover and concealment, defenders should determine if critical terrain elements are protect from attack. They should ask if the adversary can visualize the environment in part or completely. Additionally, defenders should think about what measures exist to limit cover and concealment in adversary contested terrain, or improve cover and concealment to gain a tactical advantage for friendly forces. Lastly, cyberspace defenders should gain a sense of how quickly they can make modifications to cover and concealment when required.

2.3.3.2 Battle Positions in Cyberspace

(U) A battle position in cyberspace is a defensive location oriented on likely adversary avenues of approach. The battle position outlines the location and general orientation of the defending forces. Cyberspace defenders select positions based on the virtual terrain (e.g. network routes, critical assets, and cybersecurity measures), adversary capabilities, and friendly capabilities. Battle positions in cyberspace are established when there is a need to retain a greater degree of control over net-enabled capabilities supporting a specific mission than what traditional measures can provide within the overall area of operations. Multiple battle positions may be established within a single network enclave. A commander or other leader should specify mission and engagement criteria to supporting cyberspace defenders. Those designated to perform DODIN operations (to include cybersecurity) typically operate outside a battle position. As within the land domain, there are five kinds of battle positions in cyberspace: primary, alternate, supplementary, subsequent, and strong point. On behalf of commanders and other leaders, cyberspace defenders determine the primary battle position. The primary position is the

position that covers the adversary's most likely avenue of approach into the AO. It is the best position from which to accomplish defend, such as an engagement area to prevent enemy penetration. An alternate position is a cyberspace defensive position designated for use when the primary position becomes combat ineffective for executive enabling tasks. It covers the same area as the primary position. These positions increase the survivability of critical assets by allowing cyberspace defenders to engage the enemy from multiple positions. A supplementary position is a cyberspace defensive position located within an AO that provides the best sectors of defensive terrain along an avenue of approach that is not the primary avenue where the adversary is expected to attack. For example, a potential network route into a unit's virtual AO from within the friendly network boundary requires establishing supplementary positions to allow cyberspace defenders to address potential social engineering attacks. A subsequent position is a position cyberspace defenders expect to move to during the course of the operation. Through the execution of wargaming, an organization should determine subsequent positions based on enemy reactions to the defense. A strong point is a heavily fortified battle position tied to reinforcing obstacles to create an anchor for the cyberspace defense or to deny the enemy decisive or key terrain. Cyberspace defenders position strong points on key or decisive terrain. The element providing overwatch prepares the position for its warfighting infrastructure, platforms, and tools/payloads. Establishing a strong point requires sufficient time and resources. Moreover, it requires significant support from network and system administrators organic to the organization.

2.3.3.3 Engagement Areas

(U) An engagement area (EA) in friendly cyberspace is where cyberspace defenders contain and destroy an enemy force with the massed effects of all available capabilities. An EA usually indicates the decisive point. Cyberspace defenders shape the characteristics of the EA by having relatively unobstructed access to the terrain and applicable capabilities. Cyberspace defenders cover designated EA along each enemy avenue of approach into an AO. EA are also used to designate known or suspected enemy locations. Once selected, cyberspace defenders are arrayed in positions to concentrate overwhelming effects into these areas. The commander routinely subdivides EA into smaller EAs for subordinates using one or more target reference points or by prominent terrain features. Engagement criteria are established that to specify those circumstances for initiating engagement with an enemy force. They may be restrictive or permissive. For example, cyberspace defenders could be told to hold off initiating mitigation measures until certain portions of the unit's mission were complete.

2.3.3.4 Main Battle Area

The main battle area (MBA) is the area where a unit deploys the bulk of its combat power and conducts decisive operations to defeat an attacking enemy. The defenders' major advantage is the ability to select the virtual area on which the battle takes place. Defenders are positioned in mutually supporting positions in breadth to quickly block or canalize cyber threats into prepared EAs, defeating the enemy's attack by concentrating the effects of overwhelming combat power. The inherent vulnerabilities of the position determines the distribution of capabilities in relation to both depth and breadth. In addition, defending forces employ fortifications and obstacles to improve an AO's defensive strength. In some situations, the MBA also includes the criteria in which the defending force creates an opportunity to deliver a decisive counterattack to defeat or

destroy the enemy. Unlike the MBA in the land domain that extends from the forward edge of the battle area to a rear boundary, the MBA in the cyberspace domain does not have "front" or "rear". Subsequently, a MBA may be considered "unabridged" (e.g. a set of Internet Protocol address in a subnet) or "disbanded" (e.g. several hosts spread across several subnets). This complicates the assignment of teams or elements of teams to specific terrain. In all cases, leaders should not split roles and responsibilities across an avenue of approach or KT-C.

2.3.3.5 Landing Zone

(U) A virtual landing zone in friendly cyberspace is part of an operational area in which augmentation forces access the defended network from reach-back to establish a presence and emplace capabilities for follow-on actions. As in the land domain, landing zones must be protected from adversary observation and attack. This may limit the positioning of capabilities to areas where greater access control measures can be applied.

2.3.3.6 Named Area of Interest

(U) A named area of interest (NAI) in friendly cyberspace is a virtual area where information that will satisfy a specific information requirement can be collected. NAIs are usually selected to determine adversary courses of action. Given the physical, logical, and social nature of the cyberspace domain, NAIs may actually be a physical location, a certain piece of hardware or software, an IP address, or a person. It is possible to redesignate a NAI as a targeted area of interest or a target area of interest (TAI) on confirmation of enemy activity within the area, allowing a commander to mass the effects of combat power on that area.

2.3.3.7 Battle Handover

(U) The battle handover line is a designated phase line in friendly cyberspace where responsibility transitions from the supported unit force to the supporting unit and vice versa. The supported commander of the two forces establishes the battle handover line after consulting with the supporting commander. The supported commander determines the characteristics of the line. Unlike the physical domains, the battle handover line in cyberspace is not a location. Rather it is a set of triggers or criteria that must be met in order to initiate transition of operations. The supported commander identifies the line where elements of the supporting unit can be effectively placed to provide additional combat power. The area between the battle handover line and the supported force belongs to the supported commander. The supported commander may also employ security forces and obstacles in the area.

2.3.3.8 Security Area

(U) Commanders use security operations to confuse the enemy about the location of the commander's main battle positions, prevent enemy observation of preparations and positions, and keep the enemy from delivering effects on mission relevant terrain. Commanders also try to force the attacking enemy to act prematurely. They can offset the attacker's inherent advantage of initiative regarding the time, place, plan, direction, strength, and composition of the attack by forcing the enemy to attack blind into prepared defenses. Commanders counter adversary

cyberspace reconnaissance activities through both active and passive measures. The commander must not permit adversary reconnaissance and surveillance assets to determine the precise location and strength of critical and defended assets. First, the defending force conducts reconnaissance to gain and maintain contact with the enemy. Second, each echelon normally establishes a security area around its main battle positions. The security area in friendly cyberspace is that virtual area that begins at the perimeter of the friendly network and extends as much across the network as cybersecurity forces can cover. Forces in the security area furnish information on the enemy and delay, deceive, and disrupt the enemy and conduct counter-reconnaissance. All units conduct aggressive security operations within their virtual AO, to seek out and repel enemy reconnaissance and cyberspace attacks.

2.3.3.9 Line of Departure

(U) The line of departure (LD) in friendly cyberspace is a phase line crossed at a prescribed time by forces initiating an operation. The purpose of the LD is to coordinate the advance of supporting forces, so that its elements generate effects at the time desired. The LD also marks where the unit transitions from movement to maneuver. Friendly forces should control the LD. The commander and staff analyze the cyberspace terrain before designating a LD. Different units have different movement rates on leaving their assembly area based on their inherent mobility characteristics and the designated terrain. The commander considers these different characteristics when establishing the LD to prevent these differences from affecting the synchronization of the operation. In many cases the LD is also the line of contact because the unit in contact is conducting the defensive actions from its current positions.

2.3.3.10 Cordon and Search

(U) Cordon and search is a technique of conducting a movement to contact that involves isolating a named area of interest and searching suspected virtual locations within that area to discover indicators of compromise. Cordon and search operations take place throughout the range of cyberspace defense activities. Defenders conducting a cordon and search organize their units into sub-elements. Cordon and search is normally conducted by a mission element. Each sub-element must be large enough to establish both an inner and an outer cordon around the search area. In that regards, cordon and search operations are similar to encirclement operations in the land domain.

2.3.4 (U) Integration of Defensive Cyberspace Operations

(U//FOUO) JP 3-12(R) explicitly describes DCO as “CO intended to defend DOD or other friendly cyberspace. Specifically, they are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems”. Types of DCO consist of:

- **DCO-Internal Defensive Measures (DCO-IDM).** DCO-IDM are defensive measures conducted within the Army’s portion of the DODIN. They include actively pursuing advanced internal threats within a friendly network, as well as the internal responses to these threats. Internal defensive measures respond to unauthorized activity or alerts/threat information within

the Army enterprise, and leverage intelligence, Counterintelligence (CI), Law Enforcement (LE) and other military capabilities as required.

- **DCO Response Actions (DCO-RA).** DCO-RA are those deliberate, authorized defensive actions which are taken external to the DODIN to defeat ongoing or imminent threats to defend DOD cyberspace capabilities or other designated systems. DCO-RA must be authorized IAW the standing rules of engagement (ROE) and any applicable supplemental ROEs and may rise to the level of use of force. In some cases, countermeasures are all that is required, but as in the physical domains, the effects of countermeasures are limited and will typically only degrade, not defeat, an enemy's activities. Countermeasures are a 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. In cyberspace, countermeasures are intended to identify the source of a threat and use non-intrusive techniques to stop or mitigate offensive activity in cyberspace. Countermeasures in cyberspace should not destroy or significantly impede the operations or functionality of the network they are being employed to support/protect. Any authorized use of countermeasures must comply with U.S. domestic law, international law, and applicable ROE.

2.3.5 (U) Integration of Department of Defense Information Network Operations

(U//FOUO) DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain Army communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. These include proactive actions, which address the entire Army information enterprise, including configuration control and patching, cybersecurity measures, user training, physical security and secure architecture design, operation of host-based security systems and firewalls, and encryption of data.

(U//FOUO) DODIN operations deliver protection capabilities, as defined doctrinally, that are network-focused and threat agnostic, while DCO capabilities are mission-focused and threat specific. Figure 2 illustrates integrated operations in which DODIN operations look at the "big picture" and DCO conducts operations of a more concentrated scope. Often individuals attempt to articulate where DODIN operations start or stop and DCO end or begin. No line of demarcation exists between the two, similar to the absence of a demarcation line between warfighting and humanitarian activities in a country that contains both combatants and refugees. There is a continual supported and supporting relationship between the two operations; with the determination of which one is supported and which one is supporting based on intent, focus, laws, and policies.

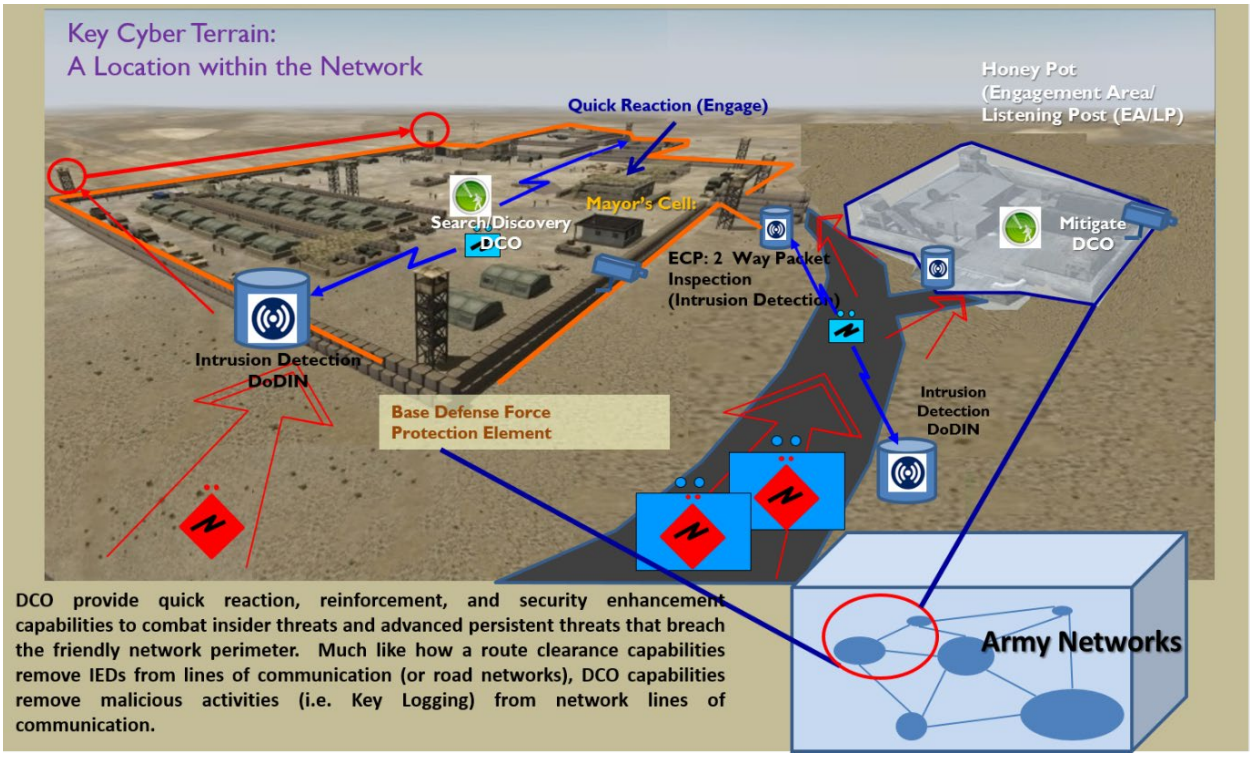


Figure 2. (U//FOUO) DCO and DODIN operations Integration

(U//FOUO) DCO-IDM integrates with the *secure* function of DODIN operations and reinforce protection measures according to terrain and/or adversary. While many of the functions of cybersecurity support DCO, cybersecurity measures are implemented IAW Title 44 United States Code (USC) to protect the enterprise as a whole against vulnerabilities for which general threats seek to exploit. DCO are meant to provide quick reaction, security enhancement, and reinforcement by focusing on specific missions, KT-C, MRT-C, and threats aligned with a commander's Title 10 USC responsibilities.

2.3.5 (U) Integration of Offensive Cyberspace Operations (OCO)

(U//FOUO) OCO are cyberspace operations intended to project power by the application of force in and through cyberspace. OCO is associated with cyberspace attacks that create various direct denial effects in cyberspace (i.e., fix, destroy, or suppress) and manipulation that leads to denial that is hidden or that manifests in the physical domains.

(U//FOUO) The integration of DCO and OCO primarily encompasses the use of S&R or OPE, and may set the conditions for defensive counter–fires or pre-emptive actions intended to identify the source of a threat and use non-intrusive techniques external to friendly networks to stop or mitigate offensive cyberspace activity. Some adversary actions can trigger DCO-RA necessary to defend networks, when authorized, by creating effects outside of the DODIN. DCO-RA can be utilized to tip and cue OCO and influence the process of selecting and prioritizing targets and matching the appropriate capabilities and effects to them, considering operational requirements. Reversely, OCO and be used to tip and cue DCO (both IDM and RA) to plan, prepare, and execute the defense against a confirmed threat preparing for a cyber attack.

2.3.6 (U) Integration of Electronic Warfare

(U//FOUO) In the context converged EW and CO capabilities, the EMS is the singular common maneuver space within which desired effects can propagate to influence operations in other domains. Convergence of EW and CO may best be described as the synchronized delivery of integrated effects through the EMS. The integrative nature of EW and CO requires a fused relationship between cyberspace defenders, Spectrum Managers, EW operators, and Intelligence Specialist across the full Range of Military Operations.

(U//FOUO) EW consists of electronic attack, electronic warfare support, and electronic protection (EP). From a defensive perspective, EP and DCO are mutually supporting actions to preserve the use of both net-enabled and EW capabilities. EP refers to actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, or adversary use of the EMS, as well as naturally occurring phenomena that degrade, neutralize, or destroy friendly combat capability.

(U//FOUO) EP facilitates the defense in cyberspace through electromagnetic (EM) hardening that filters, attenuates, grounds, bonds, blanks, and shields against undesirable EM effects; EM interference resolution that systematically diagnoses the cause or source of the interference; EMS control; and electronics security that consists of measures designed to deny unauthorized persons information of value. Cyberspace defense activities facilitate freedom of action in the EMS by offering capabilities that reprogram wireless network systems in response to validated changes in equipment, tactics, or the electromagnetic environment. Cyberspace defense activities can additionally deceive the adversary by deliberately radiating, re-radiating, altering, suppressing, absorbing, denying, enhancing, or reflecting EM energy from wireless systems in a manner intended to convey misleading information to an adversary; and countermeasures consisting of devices and techniques, threats, and TTPs that employ wireless technology to impair the effectiveness of adversary activity.

2.3.7 (U) Intelligence Support to the Cyberspace Defense

(U//FOUO) Intelligence drives operations through an increased understanding of the OE and the associated threat. Cyberspace defenders need constant access to civilian threat reports (commercial, DHS, and FBI), along with military and open source intelligence products for cyberspace operations. Intelligence products provide accurate, relevant and timely information and knowledge on adversary capabilities for potential use within the Army's portion of the DODIN and the associated intentions resulting from collection, processing, exploitation, dissemination, analysis, evaluation, and interpretation. Just as in other domains, intelligence support is required to address CCIRs. Assets are prioritized and tasked according to an intelligence collection plan that is synchronized with the other warfighting functions. The Intelligence Warfighting Function is to provide the Commander and Staff predictive analysis to "know the adversary" and make informed decisions. Intelligence provides indications and warnings and guides decisions on how, when, and where to engage enemy cyberspace forces to achieve the commander's objectives.

(U//FOUO) Ongoing cyberspace defense activities within Army networks requires assessment utilizing each one of the segments of the intelligence process, including evaluation and feedback. Intelligence support to the cyberspace defense must be nearly instantaneous, and cyberspace defenders need to be cleared to access threat data at the highest levels. A large part of intelligence support to the defense of cyberspace is processing and analyzing threat actions against specific friendly targets or target areas within Army networks. In addition to requiring access to intelligence products, commanders, other leaders, and/or staffs must leverage the Intelligence Community's systematic surveillance within cyberspace by visual, aural, electronic or other means. Surveillance can provide an understanding of adversary initiatives and detect changes in activities.

(U) The fundamental intent of integrating intelligence with other capabilities to establish the cyberspace defense is for cyberspace defenders to find indicators of compromise. An indicator is any piece of information that objectively describes an intrusion. Indicators can be subdivided into three types:

- **Atomic.** Atomic indicators are those which cannot be broken down into smaller parts and retain their meaning in the context of an intrusion. Typical examples here are IP addresses, mac addresses, email addresses, and vulnerability identifiers.

- **Computed.** Computed indicators are those which are derived from data involved in an incident. Common computed indicators include hash values and regular expressions.

- **Behavioral.** Behavioral indicators are collections of computed and atomic indicators, often subject to qualification by quantity and possibly combinatorial logic. An example would be a statement such as "the intruder would initially use a backdoor which generated network traffic matching [regular expression] at the rate of [some frequency] to [some IP address], and then replace it with one matching the Merkle-Damgard5 (MD5) hash [value] once access was established."

(U) Analysts seek to reveal indicators through analysis and collaboration. Once discovered, analysts learn more about indicator characteristics and utilize them when attempting to match other activity over a period of time. This activity, when investigated, will often lead to additional indicators. The overall process results in the development of an indicator life cycle. Tracking the derivation of a given indicator from its predecessors can be time-consuming and problematic if sufficient tracking is not in place, thus it is imperative that indicators subject to these processes are valid and applicable to the problem set in question. If attention is not given, analysts may find themselves applying these techniques to threat actors for which they were not designed, or to benign activity altogether.

(U) Intelligence and information sharing with allies and multinational partners is important during multinational operations. Special attention and awareness is important when sharing information due to specific and varying classification sharing policies. When synchronizing cyberspace and EW operations with multinational partners, Army units must ensure adherence to foreign disclosure and cybersecurity procedures. Security restrictions may prevent full disclosure of some cyberspace and electromagnetic capabilities or planning, which may severely limit

synchronization efforts. Effective synchronization requires access to systems and information at the lowest appropriate security classification level. Commanders are responsible for establishing procedures for foreign disclosure of intelligence information. (See AR 380-10 for more information on foreign disclosure.).

2.3.8 (U) Integration of Other Information Related Capabilities

(U//FOUO) Cyberspace operations capabilities make up a subset of IRCs. It is important to address the relationship between the cyberspace defense and other IRCs. Cyberspace defenders are concerned with using cyberspace capabilities to retain freedom of movement in the domain, which may allow for the creation of other effects that support operations across the physical domains. IRCs include tools, techniques, and activities using data, information, or knowledge that are leveraged to create effects operationally desirable within the physical, informational, and cognitive dimensions of the IE. IRCs are used in concert with other lines of operation, to inform and influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting friendly information, data, and networks. Thus, the cyberspace defense is an enabler to other IRCs, such as military information support operations (MISO) or Public Affairs (PA), by assuring the integrity and availability of the message. Conversely, other IRCs (e.g. MISO, PA, and Military Deception) can be employed to lessen the level of cyberspace defense required by helping to deter cyberspace threat aggression and/or mislead the threat regarding Army operations or infrastructure.

2.4 (U) Support to Host Nations/Civil Authorities

(U//FOUO) While the establishment of the cyberspace defense is generally focused on the DODIN, which includes all networks owned or leased by the Army and DOD, the Army relies on many other networks to include private sector networks in support of ULO. Responsibility for these non-Army networks, and systems falls to the network owners which include host nations and civil authorities. All Army networks are known targets for adversaries of the United States. Protection of non-Army networks and systems is also a priority, as threats may move laterally through networks and via files shared across networks. The Army cannot guarantee the level of security of non-Army networks or the robustness of network security standards. In order to make informed risk decision, commanders, other leaders, and/or staffs must know if their data will traverse private infrastructure (to include infrastructure that may be operated by foreign partners). A mission risk analysis should account for this uncertainty. Mission analysis can then support appropriate decisions (such as encryption). It is essential cyberspace defenders coordinate with non-Army network owners to better secure and defend those networks. This will require the Army to liaise with UAP, host nation agencies, and local governments.

2.5 (U) Current Situation (Organization Roles and Responsibilities)

(U//FOUO) Roles and responsibilities must create unity of effort, synchronize capabilities and resources, and facilitate information sharing in the execution of missions and functions. U.S. Army Cyber Command (ARCYBER) supports the execution of CO missions and functions assigned to the Commander, U.S. Cyber Command (CDRUSCYBERCOM), the Commander, Joint Forces Headquarters for DODIN operations, and designated Geographical Combatant

Commanders (GCC). The Commander, ARCYBER exercises operational control of Army CMFs, as delegated by CDRUSSTRATCOM and CDRUSCYBERCOM. With regard to assigned missions, the ARCYBER Commanding General exercises command and control of subordinate Army forces, other subordinate commands or organizations, and personnel as delegated in assignment orders by a combatant commander or sub-unified commander.

2.5.1 (U) Joint Organizations

2.5.1.1 (U) USCYBERCOM

(U//FOUO) CDRUSCYBERCOM directs the day-to-day global security, operations, and defense of the DODIN. Subsequently, USCYBERCOM provides overall guidance and assigns tasks to subordinate commands, as well as Service Cyber Commands. Additionally, USCYBERCOM controls the Cyber National Mission Force (CNMF), which is responsible for the defense of the nation against cyberspace attack. USCYBERCOM also controls the JFHQ-DODIN, which directs DCO-IDM and DODIN operations to achieve defense-in-depth. The USCYBERCOM Joint Operations Center (JOC) synchronizes and deconflicts full-spectrum cyberspace operations within the DOD, and coordinates with other US government and allied agencies to prevent cyberspace fratricide and ensure unity of effort across operations in the cyberspace domain. Cyberspace defense actions are integrated and synchronized by the supported commander into their CONOPS, detailed plans and orders, and specific defensive operations. The GCC is generally the supported commander for first order DCO effects within the assigned area of responsibility (AOR). Similarly, CDRUSCYBERCOM is generally the supported commander at the global or trans-regional (across AOR boundaries) level. C2 of DCO executed outside of the DODIN may require pre-determined and preauthorized actions based on threat information (attained through S&R or OPE), along with particular conditions and triggers. Commanders and planners should understand these actions are conducted by the CNMF and must coordinate with the USCYBERCOM and the supporting teams.

2.5.1.2 (U) JFHQ-DODIN

(U//FOUO) Joint Force Headquarters DODIN (JFHQ-DODIN) is the lead JFHQ under USCYBERCOM for coordination and deconfliction of DODIN operations (sustainment and protection) as well as DCO-IDM conducted in friendly-controlled terrain. JFHQ-DODIN works with the Service Cyber Commands (e.g. ARCYBER) and the Combatant Commanders to assign responsibilities for defense of terrain across the Joint network through the Mission Area and Resource Synchronization process. For JFHQ-DODIN, the DODIN is a joint operational area (JOA) defined by USCYBERCOM in which JFHQ-DODIN conducts cyberspace operations to accomplish specific missions. Applying the JOA construct to the DODIN is particularly useful because it offers scope to JFHQ-DODIN's mission and it ensures the areas between the Services boundaries of the DODIN are covered.

2.5.1.3 (U) Defense Information Systems Agency (DISA)

(U//FOUO) DISA, a Combat Support Agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information

infrastructure in direct support to Joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations. DISA synchronizes net-centric solutions across the DODIN in concert with other Services, agencies, Joint Chiefs of Staff, DOD CIO, Joint Staff J6, USCYBERCOM, military services, intelligence community, and the National Guard, to deliver responsive, protected and efficient full-spectrum warfighting support that assures global decision superiority and continuity of operations. DISA coordinates integrated and uniform net-centric global network operations (to include cybersecurity) solutions leveraging the Joint Regional Security Stacks providing full spectrum capabilities to ensure developed products satisfy network operations requirements.

2.5.1.4 (U) ARCYBER Controlled Joint Forces Headquarter-Cyber (JFHQ-C)

(U//FOUO) The JFHQ-C command post, which is a subordinate element to ARCYBER, is primarily responsible for CO in support of CENTCOM, NORTHCOM and AFRICOM. JFHQ-C is similar to a Tactical Action Center (TAC) for ARCYBER. JFHQ-C, along with the Army Cyber Operations and Integration Center (ACOIC), work together, similar to other units with a Tactical Operations Center (TOC) and TAC. JFHQ-C synchronizes Army cyberspace defenders involved in operations, exercises, and theater security cooperation activities in selected combatant command AORs. Moreover, JFHQ-C can provide GCCs with indications and warnings, gain access to cyberspace threat reports, and analyze raw data to identify vulnerabilities. As an operational headquarters with responsibilities across much of the world, the JFHQ-C normal battle rhythm conforms to mission requirements, which are coordinated with supported headquarters. The Joint Operations Center, as part of JFHQ-C, is organized to conduct cyberspace operations 24 hours per day, seven days per week, year-round.

2.5.2 (U) Army Organizations (Strategic)

2.5.2.1 (U) Army Cyber Command (ARCYBER)

(U//FOUO) ARCYBER is the Army Service Component Command (ASCC) to USCYBERCOM for the conduct of cyberspace operations in support of Joint requirements. ARCYBER executes all Service related DODIN operations (to include cybersecurity activities), DCO, and OCO IAW its USC Title 10/40/44 responsibilities. Decisive to these roles and responsibilities is ARCYBER's synchronization of cyberspace operations, IO, and EW. As an ASCC to USCYBERCOM, ARCYBER roles and tasks consist of the following:

- Exercise mission command over all Army forces assigned to USCYBERCOM to include ADCON, shared ADCON, and operational control (OPCON) of designated forces as directed
- Man, train, equip, and sustain assigned Army cyberspace forces
- Provide support to Army cyberspace forces conducting and/or supporting cyberspace operations
- Exercise OPCON of Army cyberspace forces as delegated by the combatant command

- Exercise OPCON of non-Army cyberspace forces as directed
- When directed serve as a Joint Force Functional Component Command or Joint Task Force
- Establish favorable conditions in support of conflict resolution for Combatant Commands and Army objectives
- Provide security cooperation support to Army and USCYBERCOM engagement plans
- Support the conduct of bilateral or multilateral agreements
- Serve as primary interface for USCYBERCOM with HQDA, ASCCs, Army commands (ACOM), direct reporting units (DRU), and other Combatant Commands as specified
- Execute lead service responsibility as assigned by USCYBERCOM
- Conduct DOD executive agent tasks as required/directed

(U//FOUO) The ACOIC was established as the Army strategic and operational Command Center for executing mission command of assigned and operationally controlled cyberspace forces, maintaining situational awareness of cyberspace activities and operations, enabling lateral communication across both internal and external entities, and providing strategic level analysis that builds situational understanding to enable critical decision-making. Through the ACOIC, the ARCYBER Commanding General (CG) achieves unity of command and effort, creating synergy across the full spectrum of cyberspace operations. The ACOIC is a cross-functional organization comprised of two units, the G-23 - Current Operations Intelligence; and the G-33 - Current Operations (CUOPS). The G-23 supports all-source intelligence needs for defensive operations in cyberspace. The G-33 is the CUOPS center which provides mission command of attached, aligned, and subordinate cyberspace forces. The G-33 is accountable for the operation and defense of the DODIN-A, as well as the execution of offensive and defensive missions to support Army and Joint objectives in cyberspace. Additionally, the ACOIC supports decision-making by the President, the Secretary of Defense, the Combatant Commanders, CDRUSCYBERCOM, the Chief of Staff of the Army, the ARCYBER CG, and the commanders of other supported commands and agencies. Roles and responsibilities of the ACOIC include:

- Provide near-real time, all-source intelligence analysis and reporting
- Create situational awareness of cyberspace threats to the DODIN-A
- Create situational awareness of the security, resiliency, and reliability of the Army's cyberspace infrastructure
- Conduct strategic analysis on situational awareness to produce understanding, or the understanding of the implications and consequences of situational awareness information
- Direct the Army's actions to respond to or mitigate disruptions and degradations to the Army's cyberspace infrastructure, including Platform Information Technologies and Control Systems
- Actively engage the military and private sectors, as well as international partners, to prepare for, prevent, and respond to catastrophic incidents that could degrade their ability to make decisions
- Establish standards and processes that enable unity of effort across Army cyberspace operations

2.5.2.2 (U) Regional Cyber Center (RCC)

(U//FOUO) The RCC was established as the ARCYBER operational command center for executing mission command of assigned and operationally controlled cyberspace forces; maintaining situational awareness of cyberspace operations, actions, and activities for senior leaders; enabling lateral communication across both internal and external entities; and providing strategic level analysis (e.g. building situational understanding). RCCs are under the operational control (OPCON) of ARCYBER and receive daily operational guidance, tasking, and mission control via the ACOIC. Through the ACOIC, the Commander, ARCYBER achieves unity of command and effort, creating synergy across the execution of cyberspace operations. The RCCs continuously conduct DODIN operations and provide DCO-IDM on the Army's portion of the DODIN in order to ensure Army and Joint Forces' freedom of action in cyberspace while denying the same to adversaries.

2.5.2.3 (U) Cybersecurity Service Providers (CSSP)

CSSPs (formerly known as Computer Network Defense Service Providers) conduct and deliver cybersecurity services for the Army. All DOD Component networks and systems must align to a certified CSSP. There are three levels of CSSP. DISA serves as a Tier I CSSP. ARCYBER serves as the Tier II CSSP for the Army's portion of the DODIN. ARCYBER has delegated a portion of its Tier II CSSP responsibilities to the RCCs. The U.S. Army Research Laboratory (ARL) serves as the Tier II CSSP for the Defense Research and Engineering Network and Secure Defense Research and Engineering Network. ARL also provides a fee for CSSP service model for cleared defense contractors connecting to the DODIN. ARL (for Army assets) exist as a Tier III CSSP. ARCYBER uses a layered approach to provide cybersecurity services to the Army. The first level of defense resides at the Network Enterprise Centers (NEC), which are supported by the RCCs. NECs fulfill the role a Tier III CSSP. The RCCs and NECs are the primary responders to cyberspace incidents and execute CJCSM 6510 incident response actions on a daily basis. The Network Enterprise Technology Command (NETCOM) provides technical and engineering solutions to the RCCs for cybersecurity services and compliance. CSSP personnel are trained and equipped to defeat known threat vectors and operate the majority of the Army's sensor grid in cyberspace. They operate the Army's primary cybersecurity systems at the logical-network layer, and provide some oversight at the cyberspace persona layer. CSSPs have limited capability to support cybersecurity training for units and possess limited forensics capability. Tier III CSSPs report to the ACOIC for overall situational awareness, and receive priorities, although functional command CSSPs retain significant autonomy in how those priorities are carried out.

2.5.2.4 (U) Network Enterprise Center (NEC)

(U//FOUO) The appropriate Signal Command (Theater) and corresponding Signal Brigade operationally and administratively control the NECs. NECs provide overall operations for the data and voice networks and are the designated information manager and IT manager on their respective post, camp, or station (or within an assigned geographical area). NECs plan and budget for appropriate network and information systems hardware and software technology upgrades or replacements in order to meet supported commands' validated requirements. NECs work with external organizations to ensure the proper operation of installation-level components of DOD or Army-level networks and information systems. NECs are responsible for establishing

and managing the post, camp, or station cybersecurity program on behalf of the local commander and in accordance with direction from the Signal Command (Theater) and RCC. Lastly, NECs provide the RCC with an understanding of mission impact based on cyberspace incidents.

2.5.2.5 (U) Cyber Protection Brigade/Cyber Protection Teams

(U//FOUO) The U.S. Cyber Protection Brigade defends key terrain against specified threats to deliver effects that ensure freedom of action in and through cyberspace and to deny the same to our adversaries. Consequently, USACPB mans, trains, equips, directs, and deploys Army Cyber Protection Teams (CPTs). CPTs act as the primary maneuver units for conducting DCO in cyberspace against APTs and sophisticated cyberspace threats. CPTs conduct defensive maneuver on U.S. Army networks and Mission Partner Environments (MPE)) to hunt APTs, clear APT presence, harden (networks), and assess (future APT risk and operational impact to the DODIN-A) the cyberspace environment to defend key terrain.

(U//FOUO) The CPTs perform mission analysis and terrain analysis (across the three layers – physical, logical, and cyberspace persona) on designated networks, systems, and data. When not actively engaged against enemy forces, CPTs can guide terrain owners in development of improved defensive positions to be manned by organic security forces, or to be temporarily manned as required by CPT personnel until battle handover to other entities. CPTs coordinate with both the terrain owner (mission commander) and the supporting cyberspace defenders when conducting operations. Whenever practical, CPTs coordinate with the necessary elements before conducting on-net operations, but in time-sensitive scenarios may be directed by the ACOIC to begin execution of mission immediately, and inform an organization as time comes available. In these cases, the ACOIC provides initial notification to the supporting organization.

2.5.2.6 Vulnerability Assessment Teams

(U//FOUO) Analysis of vulnerabilities will be conducted through penetration testing, which is the most preferred method, and security engineering analysis, which involves extrapolations of results from known security assessment databases. Teams that conduct vulnerability assessments consist of CPTs, Blue Vulnerability Assessment Teams (BVAT), Red Vulnerability Assessment Teams (RVAT), the U.S. Army Cyber OPFOR, and Command Cyber Readiness Inspection (CCRI) Teams.

(U//FOUO) Both BVATs and RVATs are assigned to 1st Information Operations Command. BVATs assess the network defense posture by reviewing an organization's SOPs, Plans, and policies, and checks for compliance. Through passive observation, interviews, and open source research, BVATs make a determination of the unit's posture, and provide training and guidance where needed. Upon completion of the assessment, an assessment of the organization's cyberspace defense posture is given to the commander.

(U//FOUO) RVATs emulate adversaries' cyberspace operations against an organization. RVATs conduct open source research, dumpster diving, social engineering and surreptitious penetration

testing against a designated network. As with the BVAT, RVATs, provide commanders with an understanding of the network defense posture upon completion of the assessment.

(U//FOUO) ARCYBER provides exercise planners, cyber observer/controllers - trainers (OC-Ts), and staff augmentation to the training units to incorporate Cyber Electromagnetic Activities (CEMA) into the exercise. OC-Ts observe the staff and provide feedback into the integration of CEMA principles and doctrine into operations. The U.S. Army Cyber OPFOR closely coordinates with the Land OPFOR and the irregular forces to conduct CEMA against the training units. The Cyber OPFOR operates under an approved ROE to ensure that exercise training objectives are met.

(U//FOUO) CCRI Teams coordinate with a unit's cybersecurity personnel and visit unit, post, and other organization facilities with Secret Internet Protocol Router Network (SIPRNET) presence. The team validates current accreditations, evaluates enclave and network security as well as all areas of traditional security, performs network-based vulnerability scans; and assesses compliance with DOD cybersecurity policies. A major tool for the assessment is the Cybersecurity/ Information Security Checklist and Information Assurance Incident Response Checklist. This reference provides guidance on what users are expected to do during physical security checks and cybersecurity incidents.

2.5.3 (U) Army Organizations (Corps and Below)

(U//FOUO) Corps and below commanders are directly responsible for the installation, operation, maintenance, and security of wired and wireless communications networks and network-enabled information services. The evolution of net-enabled operations and emerging requirements to conduct certain CO actions down to the tactical edge led to the establishment of the Cyber Electromagnetic Workgroup and the realignment of the G/S-6 to create an Information Assurance/Computer Network Defense (IA/CND) Cell as part of corps, division, brigade combat team (BCT), and multi-functional support brigade (MFSB) staffs.

2.5.3.1 (U) Cyber Electromagnetic Working Group

(U//FOUO) The Cyber Electromagnetic (CEM) Working Group is accountable for integrating CEMA and related actions into the concept of operations and schemes or concepts of support. CEM Working Groups do not add additional structure to an existing organization. The CEM Working Group is a collaborative staff meeting led by the Electronic Warfare Officer to analyze, coordinate, and provide recommendations for a particular purpose, event, or function. The CEM Working Group is responsible for coordinating horizontally and vertically to support ULO and it primarily deconflicts the request and delivery of cyber-related effects through the planning and targeting processes. Staff representation within the CEM Working Group includes the G-2 (S-2), G-6 (S-6), G-7 Information Operations Officer (S-7), G-9 (S-9), Fire Support Officer, Space Support Element, Judge Advocate General representative (or appropriate legal advisor), and a Joint Terminal Attack Controller when assigned. The CEM Working Group has a few differences in personnel structure at the corps, division, BCT, and MFSB (to potentially include Space and Special Technical Operations (STO) personnel).

(U//FOUO) Cyberspace defense-related responsibilities within the CEM Working Group consist of the following tasks:

- Integrate information on adversary, allied, neutral, or other specified cyberspace areas into the cyberspace common operating picture in order to contribute to the situational understanding of cyberspace and the electromagnetic spectrum
- Receive and request intelligence information from the G-2 (S-2) in reference to potential threats and associated threat TTPs used against mission command networks and systems
- Plan, integrate, and synchronize cyberspace defense actions into the unit's operations processes and scheme of maneuver
- Report information on unauthorized network activity to be integrated with other indications and warning of adversary activities
- Present a timely and accurate estimate of technical impacts resulting from cyberspace threat activity and determine detrimental effects to the unit's mission
- Plan, coordinate, and synchronize pre-approved response actions (such as tailored response actions (TRA)) to cyberspace threat activity and assesses risk to networks and information systems
- Plan, request, and coordinate the implementation of cyberspace defense actions and countermeasures provided by entities external to the unit
- Participate in the after action reviews of an incident to determine the effectiveness and efficiency of incident handling
- Assist in the prioritization of CEM effects and targets
- Deconflict cyberspace defense activities with ULO, including vulnerability assessments
- Support development of techniques, tactics, and procedures for capabilities within CEMA
- Assess cyberspace defensive requirements for CEMA
- Provide current assessment of cyberspace defense resources available to the unit

2.5.3.2 (U) G/S-6 IA/CND (Cybersecurity) Cells

(U//FOUO) Corps, division, BCT, and MFSB G/S-6s act as the principal staff officers for all matters concerning network operations (to include cybersecurity) within the area of operations. To facilitate cyberspace defense at the operational and tactical level, G/S-6 IA/CND Cells apply cybersecurity capabilities and processes to identify risks and then protect against, detect, mitigate, and recover from threats and vulnerabilities to the network and mission critical systems. The goal is to ensure the confidentiality, integrity, and availability of information, as well as authenticate and achieve non-repudiation for associated users. G/S-6 IA/CND Cells perform the following functions concurrently and continuously to address dynamic cybersecurity risks:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The Identify function provides understanding of the mission, the resources that support critical functions, and the related cybersecurity risks. It additionally must determine and map how networked devices are connected in relation to the conduct of a mission. This leads to determining avenues of approach and potential vulnerabilities. Moreover, it allows an organization to focus and prioritize efforts, consistent with risk management strategies and mission needs.

- **Protect** – Develop and implement the appropriate safeguards (such as secure network design, perimeter devices, and data management) to ensure delivery of critical services. The Protect function supports the ability to prevent or limit the impact of potential cybersecurity events.

- **Detect** – Develop and implement the appropriate activities to monitor and sense the occurrence of cybersecurity events. The Detect function may involve the employment of sensors as in other domain and it enables timely alerts of possible incidents generated by known threats.

- **Mitigate** – Develop and implement the appropriate activities to take action regarding detected cybersecurity events. The Mitigate function supports the ability to contain the impact of potential cybersecurity events while enabling defenders to learn and evolve to improve security measures.

- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to cybersecurity events. The Recover function supports timely recovery to normal operations and reduces the overall impact from events.

2.5.3.3 (U) Local Administrators

(U//FOUO) Local administrators are responsible for day-to-day touch-labor maintenance of networks and information systems, and often have privileged access available to conduct routine DODIN operations, such as configuration management or user management. Local administrators play a key role in establishing the cyberspace defense by hardening networks and systems before, during, and after an event based on threat information and lessons learned.

2.5.3.4 (U) Local Users

(U//FOUO) Local end users are responsible for protecting their own accounts at the persona-layer of cyberspace. This includes training and awareness of persona-layer attacks (such as phishing or social engineering), as well as permitting routine patching to take place. End users are rarely involved in coordinating the establishment of the cyberspace defense, but their actions are critical to sustaining an adequate defensive posture. Just like every Soldier is a rifleman, every Soldier is a defender of cyberspace. When something is wrong, awkward, or different, it is the local user that serves as a sensor and provides the first line of security against a compromise.

2.7 (U) Assumptions, Benefits, and Challenges

(U) The cyberspace defense has benefits for the Army's ability to gain and maintain advantages in the domain and to effectively integrate cyberspace operations into conventional warfare. Cyberspace defense also faces many challenges. This CONOPS addresses both in the context of assumptions about the future OE.

2.7.1 (U) Assumptions

(U//FOUO) In order to achieve full implementation of this concept, the following assumptions are made about the Army, the adversary, and the future OE.

- The Army will continue to invest resources in order to gain and maintain a competitive advantage in cyberspace
- The Army will be challenged by a growing number of threats using advanced cyberspace TTPs and capabilities
- The DOD will implement a standardized C2 framework and unified platform that are responsive to both global and regional needs.[6]
- The Army will fully implement the Joint Information Environment, with corresponding multiprotocol label switching and Joint Regional Security Stacks
- The Army will not be able to defend the entire DODIN-A at all times
- Commanders and other leaders at all levels will continue to plan for, request, and coordinate cyberspace defense effects into operations
- The Army will continually struggle to man corps and below units with the full complement of cyberspace defenders (255S and 25D)
- Additional capacity will be generated to provide cyberspace support to corps and below units
- Acquisition frameworks and funding will be established, updated, and streamlined based on changing threat TTPs, networks, and MRT-C to make the delivery of cyberspace defense capabilities more agile and flexible

2.7.2 (U) Benefits

(U) The changing nature of cyberspace threats has made active cyberspace defense increasingly important for both the DOD and Army. Passive cyberspace defense alone cannot prevent the exploitation of vulnerabilities, or deny access to advanced threats. Passive capabilities do provide some benefits in this environment and they are a necessary component of a well-designed defense. Basic cybersecurity practices, such as patching, can help reduce the number of low-level attacks cyberspace defenders need to address, but these measures no longer counter ever increasing and sophisticated threats.

(U) Cyberspace defense capabilities will provide commanders and other leaders with the ability to conduct, integrate, and synchronize defensive actions in real-time, utilizing capabilities to protect against, discover, mitigate, and engage threats and vulnerabilities. These capabilities will build on traditional approaches to defending networks and systems, supplementing best practices with new operating concepts. Cyberspace defense actions will be executed in real-time leveraging already existing sensors, data stores, and intelligence to detect and stop malicious activity before it can affect mission assurance.

2.7.3 (U) Challenges

[6] Joint Cyberspace Concept, 01 October 2015.

(U) There are challenges associated with the establishment of a defense in cyberspace. These challenges extend beyond the integration of new technologies and the inculcation of the use of that technology across the force. Legacy concepts and paradigms, inherent flaws to the development of network capabilities, the scale of cyberspace, increasing complexity of threats, the convolution of technology that exceeds user level knowledge, and the use of EMS to access domain resources create obstacles to achieving the desired end state.

(U//FOUO) Legacy concepts and paradigms dating back more than a decade resulted in the development of strategic and tactical networks as two different entities that hamper interoperability. Moreover, the tactical network is additionally sliced into upper, mid, and lower tactical internets. The Army in many respects still considers networks as a service vs. the network as a warfighting domain. It continues to focus on network operations vs. operations in the network. The Army is more influenced by standards and best business practices vs. intelligence and situational understanding. Many of the people, processes, and technologies that exist today were established to plug operational holes and gain additional capacity. The result has been a patchwork of solutions that lack the integration, coordination, and synchronization needed to be effective.

(U//FOUO) Even with the attempt to move to a single information environment, the size and complexity of the Army's network will continue to grow at an exponential rate. With this growth, cyberspace threats will rapidly proliferate; empowered by the low cost of entry to operate in the cyberspace domain. A single entity in cyberspace can create disproportionate effects against an Army dependent on net-enabled capabilities. Sensing these effects will be challenging due to the size, scale, and speed of data. Many S&R and maneuver activities within cyberspace are similar in theory to activities in other domains; but the volume, velocity, and variety of data are unique. A maneuver commander conducting ULO might get 20 reports an hour from a good battalion scout platoon, while a commander overseeing the conduct of cyberspace operations can receive over one million reports an hour from a multitude of cyberspace sensors.

(U//FOUO) Cyberspace and the EMS have a profound synergy both technically and operationally. EMS links and wireless infrastructure are components of the physical network layer of cyberspace.[7] Cyberspace operations therefore involve the use of the EMS and wireless communication technologies and systems that enable Soldiers, units, and unmanned vehicles to operate effectively. This makes the EMS a primary asset that must be protected and defended. That is why the Army must determine how EW assets, in addition to their traditional roles, can be considered and employed in support of the defense in cyberspace.

(U//FOUO) Lastly, authority for actions undertaken by the Army is derived from the U.S. Constitution and Federal law. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace. Key statutory authorities that apply to the Army include Title 10, USC, Armed Forces; Title 18, USC, Crime and Criminal Procedure; Title 32, USC, National Guard; Title 40, USC, Public Buildings, Property, and Works; Title 44, USC, Public Printing and Document; and Title 50, USC, War and

[7] Joint Publication (JP) 3-12(R), Cyberspace Operations, 5 February 2013.

National Defense. The establishment of the cyberspace defense may involve directives stemming from two or more of these authorities. Consequently, coordination, synchronization, and deconfliction must be performed across multiple organizations. In these types of situations, operations must be approved and the review and approval process may be lengthy, unless governed under an existing EXORD.

3. (U) MILITARY PROBLEM

"It [cyberspace] is now part of virtually everything we in the U.S. military do in all domains of the battle space and each of our lines of effort…There is hardly any meaningful distinction to be made now between events in cyberspace and events in the physical world, as they are so tightly linked."

ADM Michael S. Rogers
Commander, USCYBERCOM

(U//FOUO) The Army currently has limited ability to effectively establish the cyberspace defense against an APT or sophisticated cyberspace threat (in a similar manner to how it establishes the defense in the land domain) in order to maintain freedom of action in and through the domain as a critical part of ULO and unified actions. With the rapid change of cyberspace and quick development of DCO capability integrating capability to provide a complete Army solution for defending friendly cyberspace proves challenging. Thus, how does the Army operationally integrate elements existing at the strategic, operational, and tactical levels while equipping and training them with the required technologies in order to establish the cyberspace defense?

(U//FOUO) There are numerous Army initiatives aimed at mitigating existing cyberspace defense gaps. While all of these initiatives provide interim solutions to specific problems, the solutions fail to provide enduring and fully integrated capabilities. Moreover, these solutions independently compete for limited resources, provide either redundant or insufficient attributes, and are not applicable across the full spectrum of operations and mission variables. Establishing an overarching concept of operations for the cyberspace defense, which describes the operational integration of multiple capabilities, will provide the construct to evaluate not only obvious capability gaps, but enable the identification of gaps prevalent at integration and synchronization points (e.g. what gaps are the result of needing to request and integrate CPTs into operations so as to counter the impact of an on-going incident?).

4. (U) CONCEPT OF OPERATIONS

(U//FOUO) Cyberspace is a global domain consisting of networks used by friendly forces, the adversary, and neutral entities such as civilian populations and host nation governments. Figure 3 visually represents the concept of operations for the cyberspace defense; and it is meant to illustrate the complexity of the defense internal to the Army's portion of the DODIN.

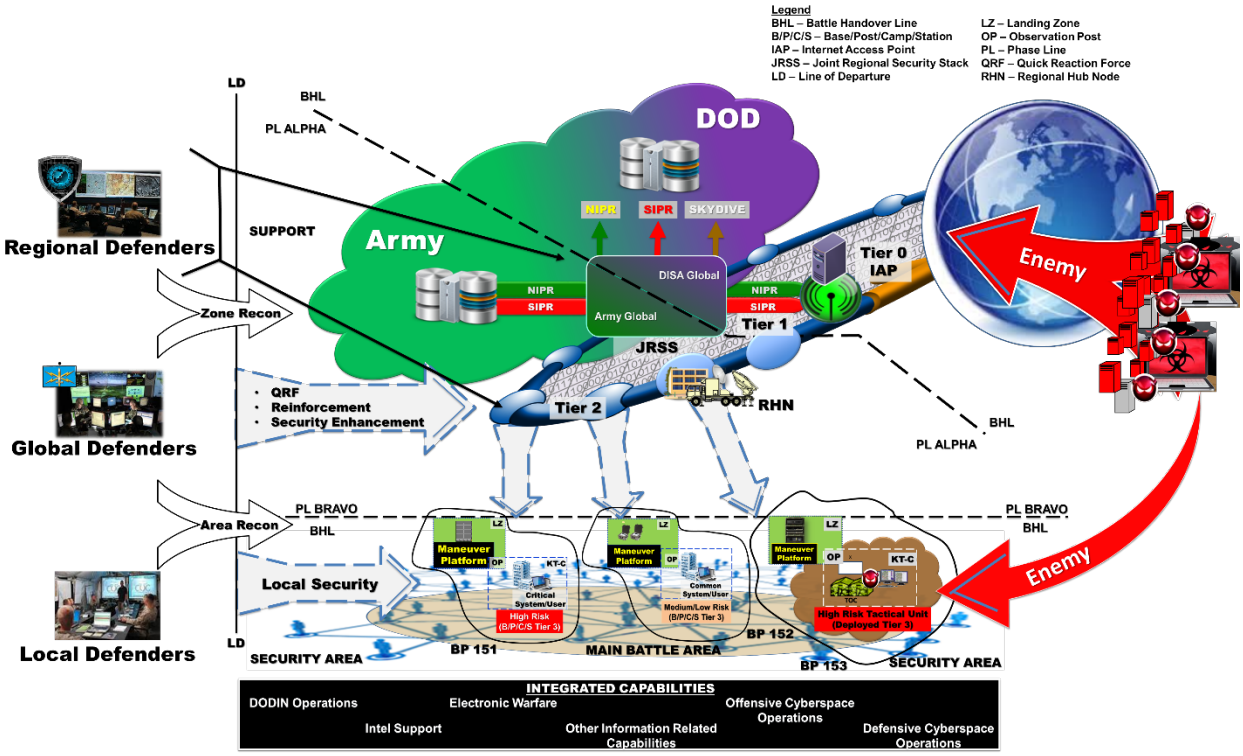


Figure 3. (U//FOUO) Defense of Cyberspace Concept of Operations

(U//FOUO) Establishing the cyberspace defense across blue, gray, and red cyberspace requires a multifaceted integration of global (e.g. CPTs), regional (e.g. RCCs), and local (e.g. those within the NECs or G/S-6 Sections) cyberspace defenders.

1. The adversary will attempt to penetrate or circumvent Internet Access Points (IAP) to the DODIN. The concept of operations for the cyberspace defense must address how the Army interrupts the adversary at the beginning of the cyber kill chain. A kill chain is a systematic process to target and engage an enemy to create desired effects. The Army's targeting doctrine defines the steps of this process as finding enemy targets suitable for engagement; fixing their location; tracking and observing; targeting with suitable weapons or assets to create desired effects; engaging the enemy; assessing the effects generated. This is an integrated, end-to-end approach described as a "chain" because any one deficiency will interrupt the entire process. Expanding on this process, a kill chain can be applied to intrusions. The essence of an intrusion is that the aggressor must develop an exploit to breach a trusted boundary, establish a presence inside a trusted environment; and from that presence, take actions towards their objectives, be they moving laterally inside a network or violating the confidentiality, integrity, or availability of a system in that network. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. With respect to cyberspace attacks or cyberspace surveillance and reconnaissance, the definitions for these kill chain phases are as follows:

- **Reconnaissance.** Research, identification, and selection of targets, often represented as crawling or fingerprinting. Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.

- **Weaponization.** Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool. Increasingly, application data files serve as the weaponized deliverable.

- **Delivery.** Transmission of the weapon to the targeted environment. The three prevalent delivery vectors for weaponized payloads by APT actors are email attachments, websites, and removable media.

- **Exploitation.** After the weapon is delivered to the targeted host, exploitation triggers malicious code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

- **Installation.** Installation of a remote access trojan or backdoor on the target system allows the adversary to maintain persistence inside the environment.

- **Command and Control (C2)**. Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have “hands on the keyboard" access inside the target environment.

- **Actions on Objectives.** Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Objectives can consist of data exfiltration, which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability; and passive observation of the network and systems. Additionally, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

2. Within the kill chain process, local cyberspace defenders at a base, post, camp, station (B/P/C/S), or tactical site implement local cybersecurity measures across the entirety of the security area in order to protect networks, information systems, and data. The organization utilizes passive cyberspace defense capabilities (e.g. host based security system, firewalls, and intrusion detection/prevention system) and strives to detect threats so as to quickly mitigate incidents. Commanders or other leaders provide essential elements of friendly information and CCIRs. Individuals overlay the CCIRs onto the supporting network to identify high value targets (e.g. MRT-C) and supporting KT-C required to conduct the mission, resulting in the production of a Critical Asset List (CAL) that determines named areas of interest. This task may include modifying network configurations, adding sensors to over-watch otherwise neglected areas, or re-tasking existing sensors. Based on the specific threats, vulnerabilities (physical, logical, and social), and the resources available; the CAL is reduced to a smaller Defended Asset List (DAL). This is analogous to developing an engagement area. Supported by DODIN operations, EW, intel, and other IRCs, local cyberspace defenders plan and prepare for adversary attacks and apply additional cyberspace security measures to achieve survivability. The unit again modifies network configurations, emplaces sensors, or tasks sensors to shape the engagement area according to particular mission objectives.

3. Regional cyberspace defenders support local defenders and generate a regional view from the delivery of cybersecurity services. Regional defenders provide area security and screening for KT-C and protect MRT-C by ensuring early and accurate warning of adversary operations. This allows for time and maneuver space within which personnel at B/P/C/S and tactical sites can react to the enemy and develop the situation that enables the effective use of the defending force. Security services are provided through fixed (e.g. Installation Campus Area Network) or deployable network infrastructure. When the situation dictates, regional cyberspace defenders conduct incident management in accordance with established tailored response actions.

4. Individuals within Army and DOD global operations centers work together at the strategic level to plan, integrate, coordinate, and synchronize actions across regional and global defenders to preserve the use of network access points and define the global picture. These organizations are able to monitor gray space for potential future incidents. Global and regional defenders collaborate at echelon and across subnet boundaries according to a scheme of maneuver that is clearly understood. Commanders or other leaders provide intent to facilitate decentralized execution.

5. On order, local and/or regional cyberspace defenders conduct a battle handover with global defenders, which are tasked and deployed either remotely or locally from an assembly area into a landing zone (LZ) to support a unit with synchronized, real-time, mission-focused capabilities. Upon arrival, global cyberspace defenders establish a battle position and set-up an observation post (OP) to conduct area reconnaissance. The primary objectives of global defenders are to discover indicators of compromise, gain and maintain contact with enemy, determine the threat's objectives and methods, attempt to achieve attribution, and in some cases, hand off the incident to offensive cyberspace forces. Global cyberspace defenders utilize a maneuver platform with supporting tools that allows it to act as a quick reaction force – employing defeat mechanisms through rapid generation and/or modification of modular platforms and tools that isolate, interdict, contain, block, defeat, disrupt, fix, neutralize, or destroy advanced or sophisticated cyberspace threats and vulnerabilities. Global defenders can also be designated to act as a security enhancement force that assists a unit in hardening (readying) MRT-C and provides augmentation to protect those assets in order to ensure their operational availability. Lastly, global defenders can be leveraged to provide reinforcement to cyberspace defenders at B/P/C/S or tactical sites conducting incident response and handling.

6. External to friendly networks, global offensive mission team execute deliberate, authorized defensive actions (DCO-RA/OCO) to shape or defeat ongoing or imminent threats and defend Army cyberspace capabilities and other designated systems out in front of the network boundary.

7. Activities in cyberspace by a sophisticated adversary are difficult to detect. Unlike adversary actions in the physical domains, which may be detected by the presence of equipment or specific activity, adversary actions in cyberspace are not easily distinguishable from legitimate activity. Intel/CI/LE capabilities for understanding, detecting, and attributing activities in cyberspace are critical to the effectiveness of defenders at all levels. Equally important, rapid assessment of operations in and through cyberspace using intel/CI/LE capabilities that offer the

ability to share information across classification boundaries facilitates necessary agile adaptation of tactics, defensive measures, and other available response options.

8. Global support personnel deploy to conduct objective penetration testing, risk analysis, and vulnerability assessments for the supported organizations. These support capabilities assist in determining a unit's defense posture and operational readiness – resulting in the hardening of systems and the validation of local cyberspace defender's knowledge, skills, and abilities.

9. At every echelon, and during all phases of operations within cyberspace, defensive missions are planned, integrated, coordinated, and synchronized with higher-level elements and processes.

10. Lastly, the enemy attempts to hide in the noise of data, requiring sophisticated approaches for detection. For behavioral analysis and pattern development, cyberspace analytics plays a key role in establishing, transforming, and maintaining the defense. Enterprise-wide data sources feed a big data platform in order for cyberspace analysts to actively search for and discover APT and sophisticated cyberspace threat activities over time. Discovery of these activities supports the development of cyberspace situational understanding.

4.1 (U) Scheme of Maneuver

(U//FOUO) A scheme of maneuver describes how arrayed forces will accomplish the objectives and actions for the cyberspace defense. This portion provides the central expression of the CONOPS and shapes the design and dissemination of supporting solutions.

(U//FOUO) Defense in cyberspace requires an array of cyberspace defenders and capabilities to be dispersed – locally, regionally, and globally. The degree of dispersal or concentration adopted by defending forces is both a function of the enemy's capabilities and the friendly forces' capability to concentrate overwhelming cyber power at decisive points.

4.1.1 (U) Local

(U) Local cyberspace defenders are defined as those individuals responsible to conduct cyberspace defense activities within a specific area of responsibility. Local cyberspace defenders include personnel organic to an organization in support of the local commander or leader. Typically, local cyberspace defender positions at a B/P/C/S are filled with civilian personnel (Career Program 34). Local cyberspace defense positions within the tactical force consist of military occupational specialty (MOS) 255S (Information Protection Technician), 25D (Cyber Network Defense Specialist), and/or other MOS with appropriate knowledge, skills, and abilities.

(U//FOUO) Local cyberspace defenders are first and foremost responsible for establishing a secure and defensible network. Their primary role at B/P/C/S and tactical sites is to plan, prepare for, and implement technical and non-technical cybersecurity measures. These measures are based on policy, directives, and best business practices to protect end user devices and preserve data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. The goal is to conceal and deny information to the threat, protect it from

unauthorized modification, and prevent unauthorized destruction. Cybersecurity measures include proactive actions such as access controls, application security, secure configuration control and patching, communications security, user training, physical security, secure architecture engineering, and the operation of host-based security systems and firewalls. Local cybersecurity prevents a unit from being surprised and is an important part of maintaining the initiative. The requirement for maintaining local security against common, known cyberspace threats is an inherent part of all operations and missions**.**

(U//FOUO) When mission dictates, local cyberspace defenders establish a perimeter defense around MRT-C that must be retained within the overall network security area to accomplish a specific mission (to include business related missions). This action usually consists of fortifying (hardening) the virtual terrain, emplacing observation posts (e.g. sensors) at likely points of entry, and conducting area reconnaissance. A perimeter defense creates a secure inner area for which additional or advanced organic and requested augmentation cyberspace assets can be focused.

(U//FOUO) In the attempt to apply similar ULO symbology to cyberspace, Figure 4 shows that within the perimeter; local cyberspace defenders aggressively recon for vulnerabilities and perform system and service hardening to eliminate as many security risks from MRT-C as possible. This is typically done by removing or disabling all non-essential applications, ports, protocols, services, and utilities from information systems. While these functions may offer useful features to users, they can present vulnerabilities that put a mission at risk.

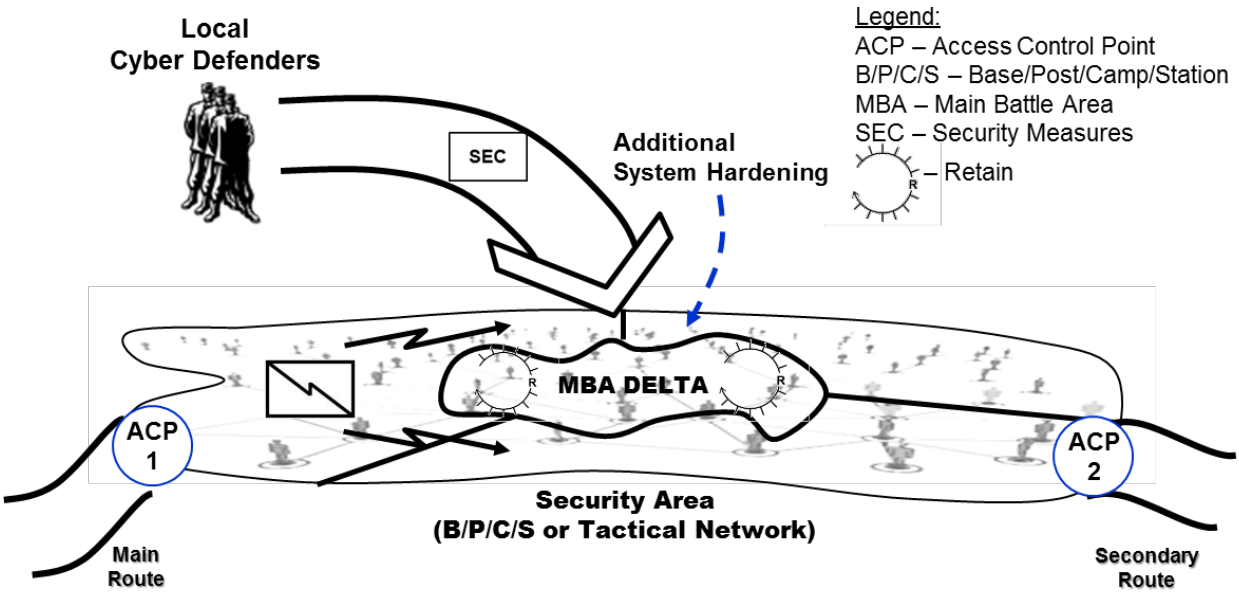


Figure 4. (U) Establish Mission Relevant Terrain in Cyberspace

(U//FOUO) Local cyberspace defenders conduct continuous monitoring activities at the network access control points (ACP) to become aware of vulnerability alerts or detect anomalous activity within their networks. Local cyberspace defenders understand their assigned assets; and thus, they are best postured to determine the impact of any mitigation actions. When under attack,

local cyberspace defenders more often than not will only be able to contain the effects using measures such as quarantines (isolation). Local cyberspace defenders stop or hold the threat until it can be destroyed (eradicated) by organic assets or until supporting augmentation/expeditionary cyberspace defenders can move in to support.

(U//FOUO) Local cyberspace defenders, through the appropriate office or staff element, request, coordinate, integrate, and synchronize activities and effects with cyberspace defenders at the regional and global levels for the purposes of situational awareness, assessments, readiness, and support.

4.1.2 (U) Regional

(U//FOUO) For commanders and leaders at B/P/C/S and tactical sites, regional cyberspace defenders provide area cyberspace defense and security in order to cover, guard, and/or screen an organization's overall network, KT-C, and MRT-C. Using another analogy, regional cyberspace defenders provide a base cluster like-defense. They focus on the protected B/P/C/S and tactical sites, along with the ACPs and network routes to those specific areas within their region. Regional cyberspace defenders use technical assets to provide advance, early warning of enemy offensive operations. Area cyberspace defense and security offers economy-of-force measures designed to ensure the continued conduct of DODIN operations. As shown in Figure 5, all area cyberspace defense and security operations take advantage of the local security measures performed by all units regardless of their location within friendly cyberspace. Sometimes area security forces must retain readiness over long periods of time without contact with the enemy. This occurs most often during area security operations, when the enemy force knows it's overmatched. In this case, the adversary normally tries to avoid engaging friendly forces unless it is on favorable terms. These favorable terms include the use of malware or specialized exploits. Forces conducting area security should not develop a false sense of security, even if the enemy appears to have ceased operations in the secured area. Regional cyberspace defenders must assume that the adversary is observing friendly operations and is seeking routines, weak points, and lax security for the opportunity to strike with minimum risk. This requires for regional cyberspace defenders to maintain vigilance and discipline to preclude that opportunity from developing.

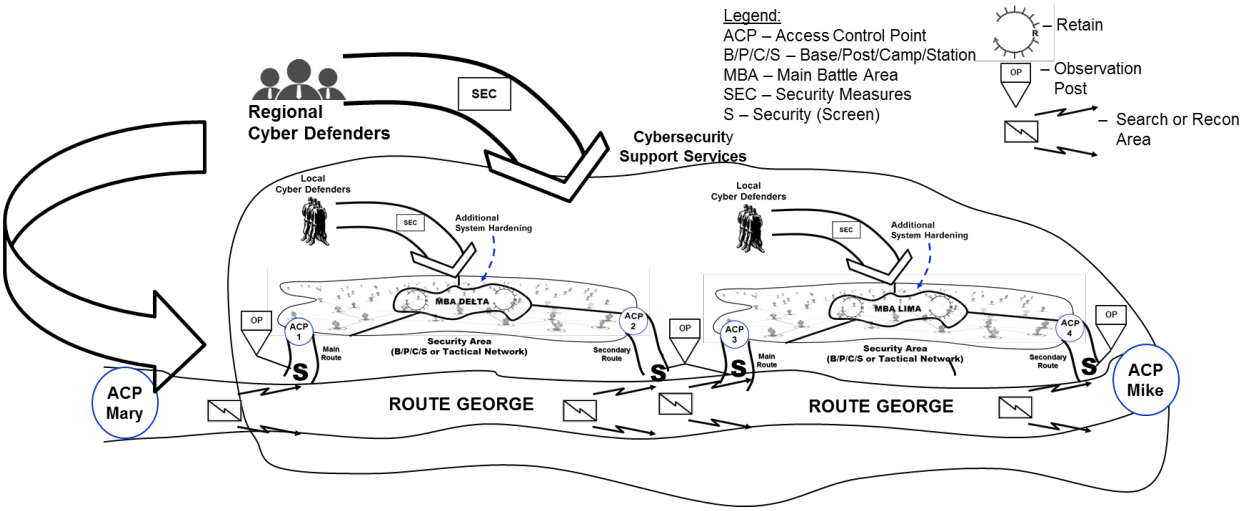


Figure 5. (U//FOUO) Area Cyberspace Defense and Security

(U//FOUO) Regional cyberspace defenders are responsible for synchronizing the defense of the Army's portion of the DODIN within their respective area of operations. Regional cyberspace defenders provide cybersecurity services that establish baseline protection, network monitoring and threat detection, incident analysis and response, and generalize mitigation and remediation of incidents. Like local cyberspace defenders, regional cyberspace defenders are informed by intelligence elements and they recommend defensive measures to network operators in order to deny adversaries freedom of maneuver within the network. Additionally, similar to local cyberspace defenders, regional defenders, through the appropriate office or staff element; request, coordinate, integrate, and synchronize activities with cyberspace defenders at other levels for the purposes of situational awareness, assessments, readiness, support, and changes in the cybersecurity baseline across the network.

4.1.3 (U) Global

4.1.3.1 (U) Quick Reaction, Reinforcement, and Security Enhancement Forces

(U//FOUO) Globally, cyberspace defense are tasked organize based on a mission element and a support element to offers commanders and leaders quick response, reinforcement, and security enhancement capabilities. Globally arrayed cyberspace defenders focus on four major lines of operations: Defend the Nation, Protect the DODIN, CCMD Support, and Service Support, with emphasis on performing DCO-IDM. This force possesses a unique skill set that differs from local or regional cyberspace defenders and enables the execution of specialized missions. As Figure 6 highlights, the timeline for global defenders is cyclical as individuals conduct reconnaissance; planning; reception, staging, onward movement, and integration (RSOI); execution; redeployment; and refit. Reconnaissance through RSOI can occur within hours to months. Execution requires weeks to months; and redeployment and refit periods will vary. Of course the timeline is difficult to predict once the mission commences.

Figure 6. (U//FOUO) Global Defender Mission Timeline

(U//FOUO) Mission elements are focused on moving forces virtually to a position of advantage over the enemy. Within the elements, personnel align to command and control (C2), network subject matter expert (SME), host SME, and master gunner positions. The support element integrates with the mission elements with complementary and reinforcing capabilities for reconnaissance and counter-mobility. Global defender capabilities are intended to provide transformational defensive effects in cyberspace from the strategic level to the tactical edge. Specialized capabilities consist of the following:

- **Mission Protection.** Global cyberspace defenders provide mission protection capabilities to assist supported organizations in identifying KT-C and MRT-C. Cyberspace defenders conduct a comprehensive analysis of a supported commander's or other leader's mission and determine cyberspace dependencies. Global cyberspace defenders additionally perform a mission impact analysis to evaluate risks and develop courses of action for managing those risks to achieve mission assurance. Mission protection capabilities serve to build and sustain an understanding and awareness (utilizing solutions such as a common operating picture) of the supported commander's or other leader's mission critical, net-enabled assets.

- **Discovery and Counter-Infiltration.** Global cyberspace defenders use discovery and counter-infiltration capabilities to detect, illuminate, and remove unknown malicious activity from specified AO. Discovery and counter-infiltration capabilities, moreover, enable cyberspace defenders to conduct real-time reconnaissance within for critical systems during specific mission

execution. The intent is to search for, discover, and characterize advanced adversary tradecraft that evades routine security measures.

(U//FOUO) Missions for global cyberspace defenders are primarily generated based on a request from local or regional cyberspace defenders. As depicted in Figure 7, employment of global cyberspace defenders can be done physically or remotely (denoted by "**R**" in the unit icon) from an assembly area (AA). Physical (onsite) employment offers close access and a better tie-in to the supported organizations OPTEMPO. Physical employment requires regional and local cyberspace defenders to coordinate the authorizations and network access/permissions necessary to support. It additionally requires regional and local cyberspace defenders to make available information about the network topology, MRT-C, and other key information well before augmentation forces conduct mission. Remote access offers a quicker response in comparison with on-site support, and should always be the first method implemented. However, remote access may not always be technically feasible. Moreover, it may prevent a comprehensive assessment of security measures and the defense posture.

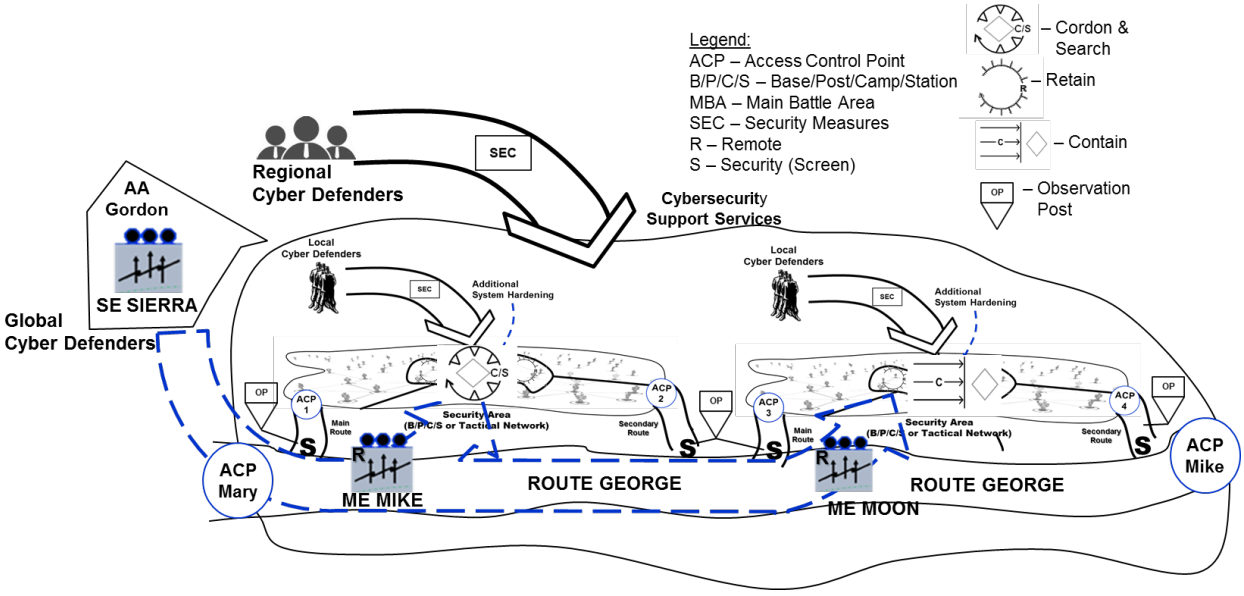


Figure 7. (U) Employment of Global Cyberspace Defenders

(U//FOUO) Global cyberspace defenders that operate outside friendly networks use specialized target/actor knowledge to plan protection and reconnaissance within their assigned area of operation. Defenders operating outside friendly networks conduct digital network exploitation in order to report potential cyberspace threats and manage the development of countermeasures and mitigation strategies (e.g. counterattacks). A unique aspect of global cyberspace defenders is the ability to see from where data emanates – they can observe the access points (chokepoints) where traffic flows between friendly and gray space.

4.1.3.2 (U) Global Support Forces

(U//FOUO) Global DCO support forces provide commanders and other leaders with independent assessments that offer critical reviews and alternative perspectives – challenging prevailing

notions, rigorously testing current TTPs, and countering presumptions in order to enhance operational readiness. Specialized capabilities consist of the following:

- **Cyberspace Threat Emulation.** Global cyberspace defenders use capabilities to assess an organization's security by emulating specific TTPs used by known adversaries to identify unmitigated vulnerabilities through simulated exploitation attacks on Army net-enabled capabilities. Global cyberspace defenders differ from traditional penetration testing or red teams in that they will closely resemble adversary OCO in their processes and execution instead of conducting generic auditing of security measures.

- **Cyber Readiness.** Global cyberspace support forces focus capabilities on providing in-depth reviews of mission-supporting cyberspace assets ensuring compliance with DOD and Army policies and regulations. Through targeted inspections, global support personnel review the effectiveness of current security policies, recommended changes, and provide insight into the inspected organizations operational readiness.

- **Cyber Support.** Global cyberspace support forces use capabilities to provide an organization assistance with enhancing its cybersecurity and cyberspace defense posture by identifying and correcting deficiencies in security and defensive operations, policies, and procedures with the end-state being improved and self-sustaining protection. Global support forces work closely with local, organic network defenders at an organization to plan, train, and deploy mitigations for cyberspace vulnerabilities.

(U//FOUO) Global cyberspace support forces are requested by the network/system owner; and based on a defined scenario; support elements become knowledgeable of the target system(s), match their approach to the environment, gather appropriate tools to assess the defense posture of the network/system, and train to execute the assessment. Global support forces then deploy to execute, documenting the vulnerabilities and suggesting countermeasures. They work closely with network/system owners, demonstrating how exploits were run, and how owners can protect their MRT-C. Global support forces provide an accurate assessment on which network/system owners can make coherent risk management decisions concerning their information systems, networks, and supporting infrastructure.

4.2 (U) Cyberspace Defense Doctrinal Hierarchy

(U) Figure 8 outlines the Army's cyberspace defense doctrinal taxonomy consisting of tasks associated with defending Army and other networks as a decisive action for cyberspace operations; along with tactical enabling and mission tasks. Different units involved in the defense may be conducting different types and subordinate forms of the defense, and often transition rapidly from one element or subordinate task to another. Cyberspace defenders rapidly shift emphasis to continually keep the enemy off balance, while positioning available resources for maximum effectiveness. Army cyberspace defenders conduct tactical enabling tasks to assist with the planning, preparation, and execution of the cyberspace defense. Tactical enabling tasks are more shaping in nature and used to reduce risk during a mission. Tactical mission tasks describe actions by friendly forces or effects on enemy forces that have specific military definitions addressed in this CONOPS.

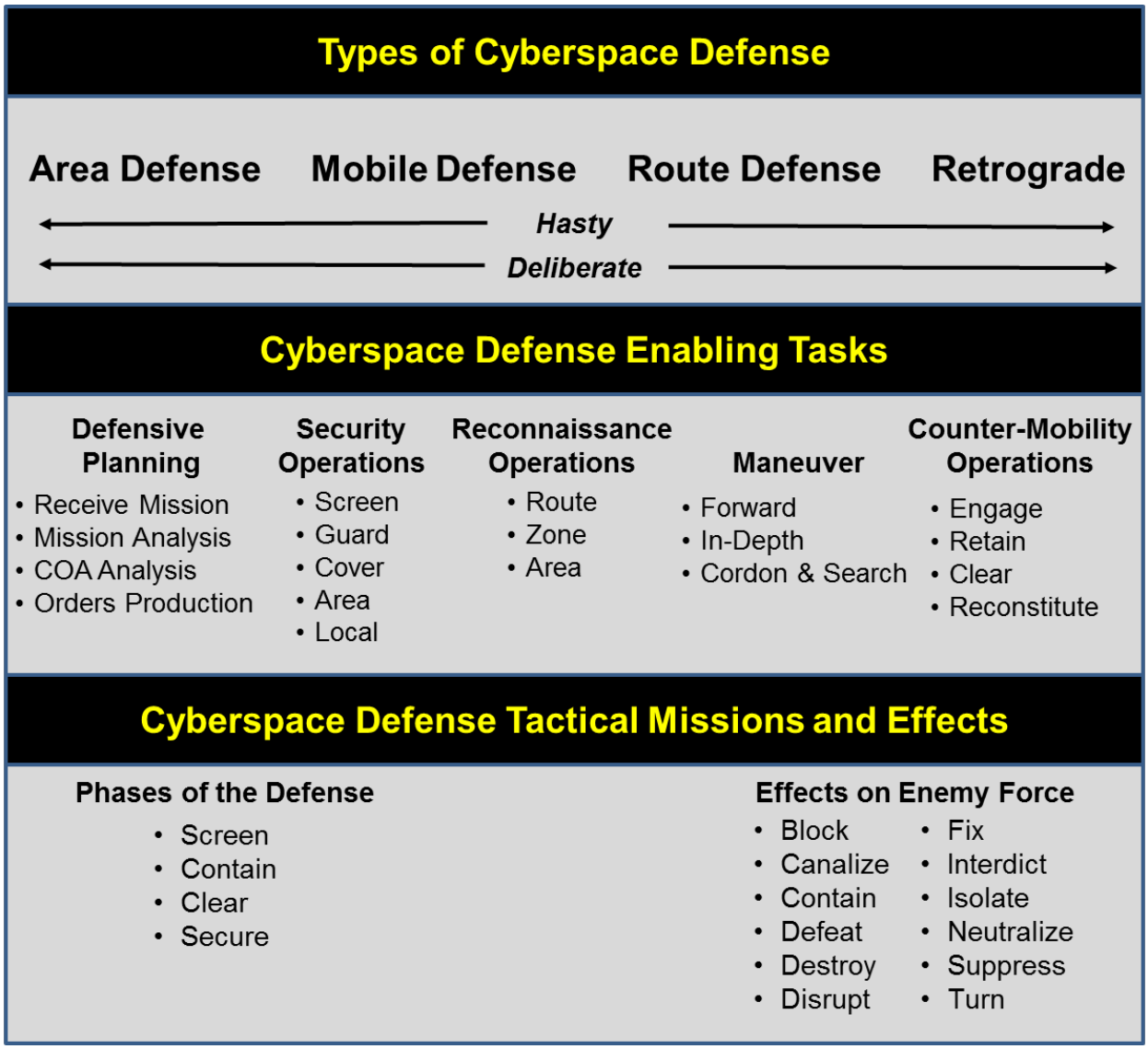


Figure 8. (U) Cyberspace Defense Doctrinal Hierarchy

4.2.1 (U) Types of Cyberspace Defense

- **Area Defense.** The area defense in cyberspace concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright. The focus of the area defense is on retaining terrain where the bulk of the defending force positions itself in mutually supporting, prepared positions. Units maintain their positions and control the terrain between these positions. The decisive operation channels actions into engagement areas (e.g. honey pots), possibly supplemented by a counterattack. An element in reserve may or may not take part in the decisive operation. These elements can reinforce, add depth, block, or restore the position by executing a mobile defense, counterattack, seizing the initiative, and destroy the enemy's cyberspace capabilities. Units at all echelons can conduct an area defense. Units at all echelons may implement an area defense in conjunction with tasks utilized to sustain the network.

- **Mobile Defense.** In a mobile defense, cyberspace defenders set the conditions for the destruction or defeat of the enemy's OCO capabilities through the use of defeat mechanisms. The mobile defense allows the enemy to advance to a point where they are exposed. The Army can request or employ OCO-focused CMFs as a striking force in order to execute a counterattack in a mobile defense. Other CMFs can be used to fix an attacking enemy force in position, to help channel attacking enemy forces into specific virtual areas. A mobile defense requires a virtual area of operations with considerable depth. Cyberspace defenders must be able to shape the area of hostilities, causing an enemy force to overextend itself. Likewise, the commanders and leaders must be able to freely move CMFs within cyberspace to set the conditions for the enemy to be cut off and destroyed.

- **Route Defense.** Route defense concentrates on denying adversary forces access to specified terrain, and designated cyberspace capabilities therein, utilized by friendly forces to pass operational data and information. A defended route may connect two or more cyberspace capabilities and traverse one or more designated areas or sections of cyberspace. Figure 9 shows a route defense with the friendly forces deployed on the blue highlighted path from a regional capability to an enterprise capability.

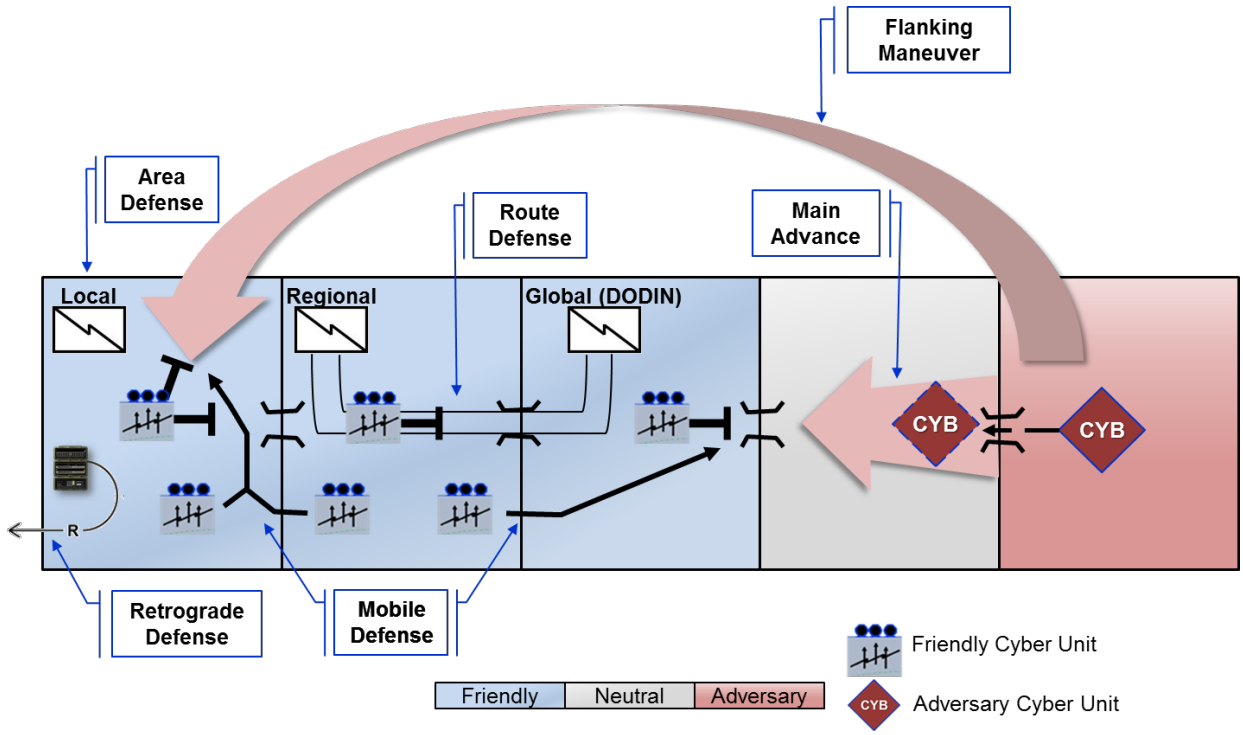


Figure 9. (U//FOUO) Types of Cyberspace Defense

- **Retrograde.** A retrograde involves organized movement of net-enabled capabilities away from the enemy. The enemy may force these actions, or commanders and other leaders may direct them voluntarily. The retrograde is not conducted in isolation. It is part of a larger effort designed to regain the initiative and defeat the cyberspace threat. There are three forms of the retrograde: delay, withdrawal, and retirement. A delaying operation is an action in which commanders and other leaders trade space for time. Yielding some ground to the enemy gains

time while retaining some level flexibility and freedom of action. A withdrawal operation is a planned retrograde operation in which a unit experiencing a cyber incident moves net-enabled assets way from the enemy. Commanders and other leaders voluntarily direct the disengagement from the enemy to preserve critical assets or release them for a new mission. A retirement consists of a unit not experiencing a cyber incident at the time moving critical assets as not to be a potential target for cyberspace threats. In each form of the retrograde, critical cyber assets are moved to another location, whether the location be physical or logical.

(U) Cyberspace defense actions can be executed in either a hasty or deliberate manner. Hasty actions are performed when a commander or other leader directs immediately available forces, using fragmentary orders (FRAGOs), to perform activities with minimal preparation, planning, and time for execution. Deliberate actions are performed when a commander or other leader leverages detailed intelligence concerning the situation to develop and coordinate detailed plans, including multiple branches and sequels. A commander or other leader organizes forces specifically for the operation to provide fully synchronized cyberspace defenders across global, regional, and local levels. When a type of cyberspace defense is performed deliberately, cyberspace defenders conduct extensive rehearsals while conducting shaping operations to set the conditions for decisive operations.

4.2.2 (U) Cyberspace Defense Enabling Tasks

(U) Enabling tasks support the establishment of the cyberspace defense. They are usually employed by cyberspace defenders as shaping or supporting operations for the mission. The implementation of the intrusion kill chain model becomes the driver for executing the tasks sequentially or simultaneously, aligned with capabilities to counter the adversary in a designated AO. Cyberspace defenders can measure the performance as well as the effectiveness of these tasks, and plan additional integration to rectify any operational gaps. Fundamentally, this approach is the essence of defending in cyberspace – basing decisions and measurements on a keen understanding of the network and adversary.

4.2.2.1 (U) Defensive Planning

(U) Planning is the process by which staffs translate a leader's intent into a specific course of action for preparation and execution, focusing on the expected results. Put another way, planning is the art and science of understanding a situation, envisioning a desired future, and laying out an operational approach to achieve that future. Similar to other military activities, the establishment of the cyberspace defense benefits from deliberate planning. Planning is NOT static. Planning for the defense must parallel an organization's overall operations planning cycle and incorporate the use of the Military Decision Making Process (MDMP). MDMP integrates the activities of cyberspace defenders across echelons to understand the situation and mission; develop and compare courses of action; decide on a course of action that best accomplishes the mission; and produce an operation plan or order for execution. The MDMP results in an improved understanding of the situation and a plan or order that guides the force through preparation and execution. Similar to ULO, MDMP applied to the cyberspace defense consists of multiple steps – each step consisting of various inputs, a method (step) to conduct, and outputs.

1. **(U) Receipt of Mission.** Cyberspace defenders initiate the MDMP upon receipt of or in anticipation of a mission. Individuals often begin planning in the absence of a complete and approved higher headquarters' operation plan (OPLAN) or operation order (OPORD). In these instances, the cyberspace defenders begin a new planning effort based on a warning order (WARNO) and other directives. This requires active collaboration with defenders both horizontally and vertically across echelons.

2. **(U) Mission Analysis:** An effective mission analysis as outlined in Table 1 considers the potential impact cyberspace has on the operational environment. Supported and supporting cyberspace defenders participate in planning actions that help identify the problem statement, mission statement, commander's intent, planning guidance, initial commander's critical information requirements, essential elements of friendly information, and updated running estimates. Defensive planning contributes to overall mission analysis by participating in the intelligence preparation of the battlefield (IPB) with the intelligence community.

(U) A key output of IPB is the identification of KT-C and MRT-C. KT-C and MRT-C consist of those physical, logical, and cyberspace persona elements of the network that enable mission essential functions. These might include major lines of communications; key access points for the defense, observation and launch points for the offense; or opportunities to create bottlenecks. In cyberspace, key terrain involves network links and nodes (or even individual administrator accounts) that are essential to a particular friendly or adversary capability. Cyberspace defenders determine high value terrain through the collection, analysis, evaluation, and interpretation of network information, combined with other relevant factors, to predict the effect of the virtual terrain on operations. Specific to terrain analysis of friendly cyberspace, defenders decompose their assigned missions to the point of identifying the net-enabled capabilities required to implement each mission. Each identified capability includes the minimum performance standards and conditions necessary to achieve mission success.

(U//FOUO) Cyberspace defenders define MRT-C in a prioritized order to create a CAL. Figure 10 provides a simple representation of the phases required. Planners must understand the graph and data flows as a perquisite to determining mission essential capabilities. Cyberspace defenders (as the mission owner) analyze key tasks and available units. Each unit determines the mission essential task required to achieve mission assurance. Moreover, planners ascertain the critical capabilities and resources required to execute the mission essential tasks. Intelligence and current trends dictate which critical resources are deemed most vulnerable and indicate what adversaries might deem as high value targets.

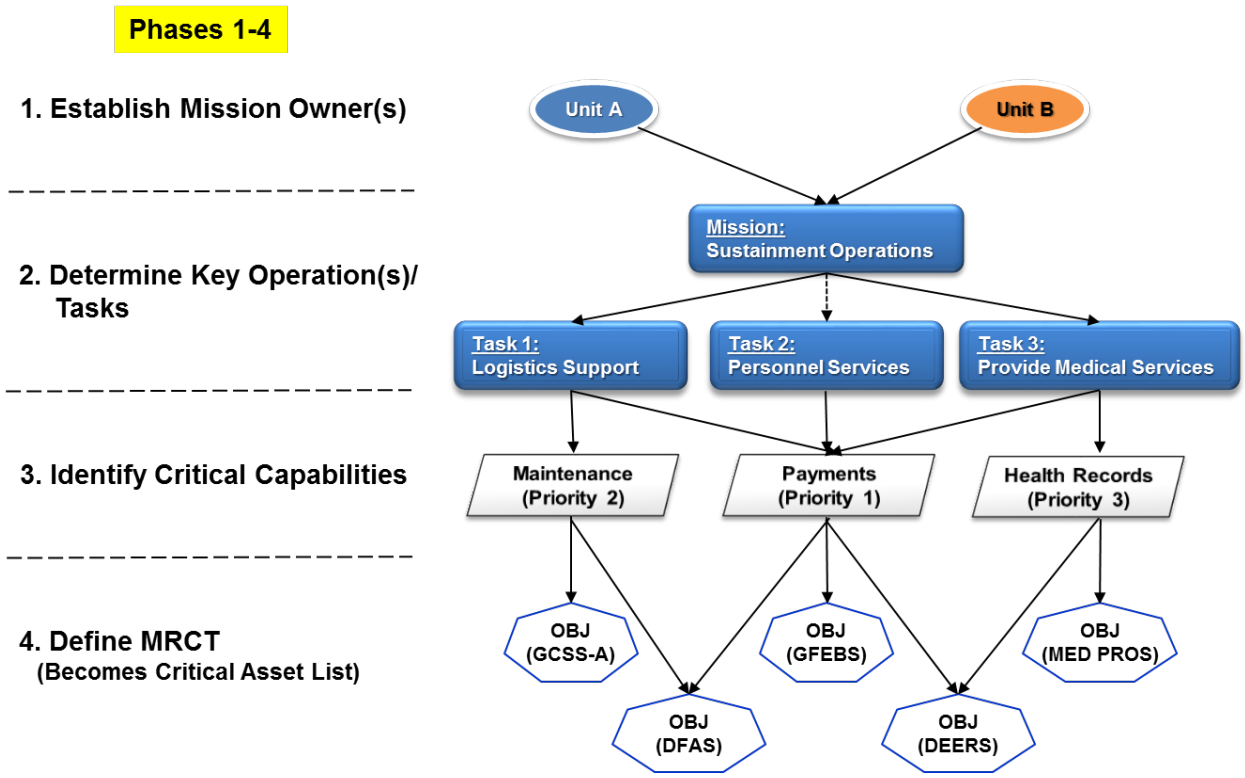


Figure 7. (U//FOUO) Define MRT-C/Develop Critical Asset List

(U//FOUO) Commanders assume risk related with resourcing constraints that create a gap in operational capacity; resulting in cyberspace defenders reducing the CAL down to a smaller DAL as shown in Figure 11. The intent is to coordinate, integrate, and synchronize resources so elements in the DAL become objectives for supporting defenders. The assigned team defends the designated critical network resources/MRT-C and incorporate the threats TTPs along determined known attack vectors to assess readiness.

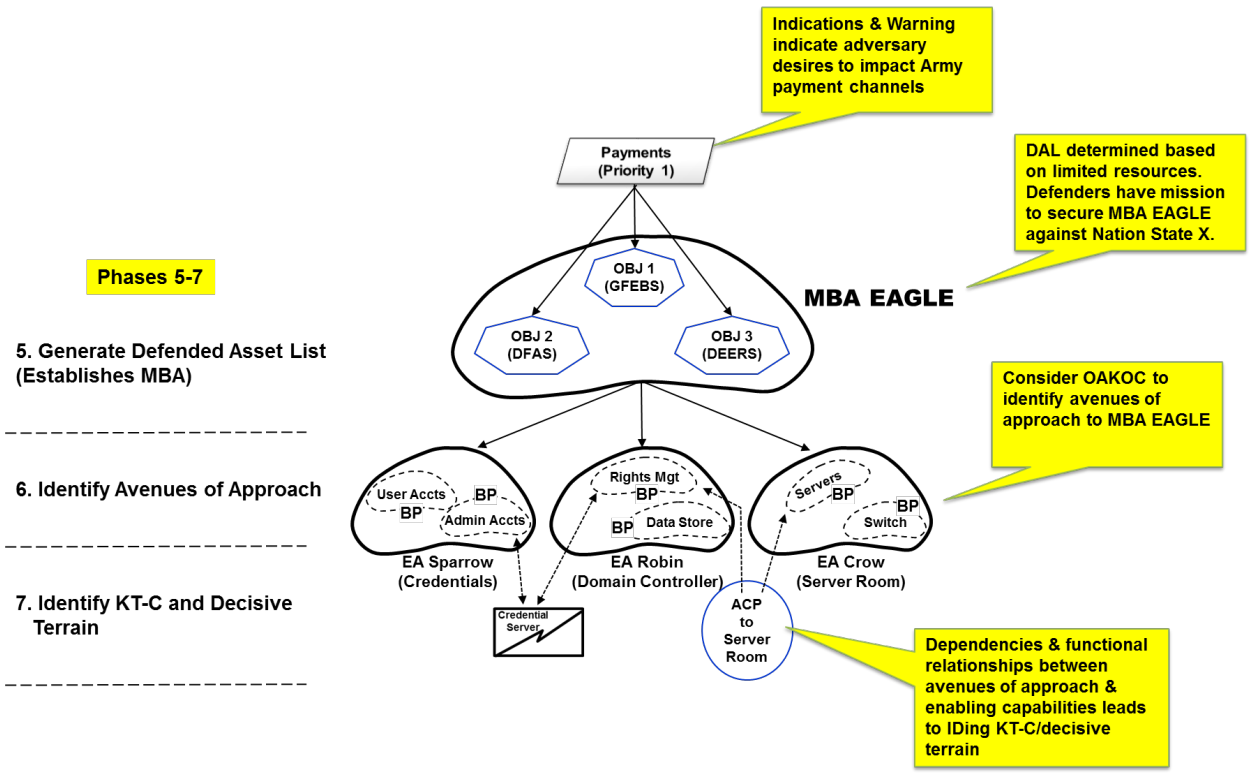


Figure 8. (U//FOUO) Develop a DAL/Identify KT-C & Decisive Terrain

(U//FOUO) Even though cyberspace has many unique characteristics, the general concepts of key terrain hold true. In a defense-in-depth strategy, defenders consider OAKOC to identify avenues of approach to a MBA. Avenues of approach include aspects of cyber persona, logical (e.g. data), and physical infrastructure. The process of identifying KT-C focuses on the technical environment (e.g. types of transport, types of operating systems, types of information services), relationships between physical and cyberspace elements, and linking missions and mission dependencies with the technical environment. Cyberspace defenders should factor known and potential paths to the terrain; legitimate and non-legitimate means combatants have to gain access; access restrictions exist in the environment; and how quickly can these be modified. Moreover, cyberspace defenders should think about how the terrain affects visibility for forces in the operating environment (both friendly and adversary forces). Lastly, cyberspace defenders must determine if the terrain affects fields of visibility by limiting or improving the ability to create effects inside the environment?

(U//FOUO) During mission analysis, planners use threat assessments to identify relevant internal and external threats and vulnerabilities the adversary wishes to exploit; the type of capabilities or TTPs adversaries are known to use; and their intents and objectives. The threat is specifically assessed in the context of the terrain (e.g. how might a threat employ TTPs given the operational environment?). During threat assessments cyberspace defenders identify significant gaps in what is known about the adversary and other relevant aspects of the OE and formulate intelligence requirements (IR). IRs are general or specific subjects upon which there is a need for the collection of information or the production of intelligence. Based on the IRs, the Intelligence staff develops more specific questions (those items of information that must be collected and

processed to develop the intelligence required by the commander). IRs related to cyberspace may include: threat TTPs, personnel status and readiness of adversaries' equipment, and unique cyberspace signature identifiers. Likely cyberspace threats and vulnerabilities are identified in accordance with adversary intents and cyberspace/EW capabilities. A key portion of this analysis is to assess the potential impact on friendly assets as a result of increasing the defensive posture of the network. For example, increasing security in cyberspace or deploying additional tools to analyze networks can cause slower network operational speeds. At the conclusion of the mission analysis, applicable products and information are generated or gathered.

Inputs	Cyberspace Defense Actions	Outputs
• Mission statement • Initial commander's intent • Initial commander's planning guidance • Initial commander's critical information requirements • Initial essential elements of friendly information • Updated intelligence preparation of the battlefield • Cyberspace defense specified and implied tasks • List of net-enabled capabilities that may require the generation of defensive effects • Updated running estimate. • List of cyberspace defense related assumptions	• Provide input to the assessment of relative unit readiness. • Identify vulnerabilities of friendly actors. • Provide input to the development of options for decisive, shaping, and sustaining operations. • Provide DCO input to the development of military deception courses of action • Develop initial scheme of DCO for each course of action • Develop statements and sketches for each course of action • Analyze KT-C and critical assets and develop list of tentative defended assets • Develop primary, alternate, contingency, and emergency communications plan for each course of action. • Develop input for the operations execution matrix. • Provide input and participate in the course of action development brief as required.	• For each course of action developed include: – Draft cyberspace defense concept of operations with tasks – Draft input to DAL – Draft input to target synchronization matrix – Draft maps and overlays – Draft network infrastructure diagrams and charts • Updated running estimate including assumptions • Draft Appendix: Defensive Cyberspace Operations

Table 1. (U) Mission Analysis

- **(U//FOUO) Course of Action Development and Analysis:** During mission analysis supported and supporting cyberspace defenders integrate and synchronize capabilities into each COA, thereby identifying which COA best accomplishes the mission. Cyberspace defenders must address how cyberspace defense capabilities support each COA and apply them to timelines, critical events, and decision points (Table 2). COA analysis step requires planners to overlap the outputs from terrain analysis with the threat assessment. Included in this step is the need for a risk assessment to determine the severity if a compromise is successful. Furthermore, COA analysis includes determining system and network links to find interconnectivity with key systems (which is part of KT-C). Combined with mission analysis, COA analysis generates a potential set of negative effects (events/incidents) likely to be generated against key information/infrastructure by the threat.

(U//FOUO) Subsequent to determine impacts of likely attacks, planners should determine what internal defensive measures will be employed at critical points in the network. Countermeasures, by the employment of devices and/or techniques, impair the operational effectiveness of enemy activity. In cyberspace, countermeasures can be used to identify the source of a threat to Army networks and use non-intrusive techniques to stop or mitigate offensive activity in cyberspace. Countermeasures should not destroy or significantly impede the operations or functionality of the defended network. Based on an organization's capacity, tools availability, and/or authorities to employ required countermeasures, COA analysis will determine the need for augmentation support from either regional or global cyberspace defenders.

(U) When augmentation support is required, the organization and supporting cyberspace defenders will begin to integrate and synchronize activities. Coordination includes the following:

- Establishing communication links to ensure continuous contact during execution
- Exchanging Standard Operating Procedures
- Ensuring all key players are represented, integrated, and actively involved in planning and coordinating activities
- Understanding of the situation and problems to solve
- Unity of effort toward achieving a common goal
- Determining the resources, capabilities, and activities necessary to achieve their goal
- Facilitating the integration and synchronization of capabilities and activities wherever possible

(U) Both the supported unit and supporting defenders seek to establish unity of effort. The supported unit builds a partnership with the supporting defenders early in the planning phase as a key activity for preparation and continued execution. The supported unit should ensure to coordinate with those providing augmentation to achieve the following:

- Supporting element is represented, integrated, and actively involved in planning and coordinating activities
- The supported unit and augmentation force share an understanding of the situation and problems to solve
- The supported unit and supporting element integrate and synchronize capabilities and activities wherever possible
- The supported unit and supporting cyberspace defenders collectively determine the resources, capabilities, and activities necessary to achieve their goal

(U//FOUO) During the coordination process, the supported unit strives to provide the supporting element with as much of the following information as possible:

- **Network Configuration.**
  - Characterize network:
    - ✓ Hostnames
    - ✓ IP address and subnet scheme

- ✓ Routing configuration
- ✓ Access Control List
- ✓ Bandwidth utilization
- ✓ Device configurations

- Characterize ports and protocols for:

  - ✓ Network devices: Firewall, Router, Switches
  - ✓ Applications: web, exchange, SharePoint, database
  - ✓ Security: SEIM, IDS, HBSS, Web Proxies, PKI

- Characterize usual communications flow:

  - ✓ Which hosts communicate to what other devices?
  - ✓ What security tools communicate to what other hosts, where the communication terminates?

- Characterize connections:

  - ✓ List devices making outside the network connections
  - ✓ List services and protocols allowed to outbound traffic
  - ✓ Get/Post request outside web server, HTTP responses
  - ✓ List geographical connections (place and occurrences)

- **Domain Information.**

  - User and Privilege Accounts

    - ✓ List domain accounts and their permissions
    - ✓ List privilege accounts and identify usual connection times
    - ✓ Net group administrators

  - DNS

    - ✓ DNS configuration
    - ✓ DNS queries

  - Domain Controller

    - ✓ Read/write authority
    - ✓ Global catalog server
    - ✓ Local security policy
    - ✓ Net Shares
    - ✓ Roles

- **Applications configuration and reports.**

  - List enterprise applications (Exchange, SharePoint, web server, etc.)
  - List normal ports, protocols, and services for these applications.
  - Other and special application configuration
  - IDS reporting
  - ACAS/STIG/SCAP report

- **Host.**

  - System Details

    - Hostnames
    - BIOS info
    - hardware info
    - network interface info
    - systeminfo

  - Network Config & Communication Detail

    - IP configuration
    - shares (net use)
    - connections (netstat)
    - ARP

  - DNS Information

    - \etc\hosts
    - displaydns

  - Service Information

    - Task list
    - Services associate with each task list
    - Service list configurations

  - Process Information

    - Process list
    - Jobs list
    - Startup list
    - Domain config

  - Local users and groups

    - Net users

    - Net local group administrators

- Registries
- Hashes for Driver/DLL
- Approved software
- List Executables
- Schedule task lists
- Event logs in not collected by SEIM

(U) As part of the defensive planning process; cyberspace defenders at all levels must come together to outline key objectives; scope the mission; provide details in reference probable cyberspace threats, attribution, indicators of compromise, known vulnerabilities, and critical infrastructure. Supported and supporting cyberspace defenders utilize the MDMP as necessary to produce feasible, agreed upon COAs that establish triggers and decision points based on limits or thresholds to countermeasure performance or effectiveness. For example, if network degradation results in a 30% decrease in data throughput or there is evidence of data capture, certain tailored response actions (TRA) are implemented.

Inputs	Cyberspace Defense Actions	Outputs
• Updated running estimate including assumptions • Revised planning guidance specific to the cyberspace defense • Consolidated course of action statements and sketches • Draft Appendix 1 to Annex H (Signal)	• In collaboration with the staff, wargame enemy and adversary cyber capabilities against friendly capabilities and vulnerabilities for each course of action • Integrate and synchronize cyberspace defense into the concept of operations for each course of action • Develop and complete the wargame synchronization matrix tool from a cyberspace defense perspective • Identify and record strengths and weaknesses associated with each course of action from a cyberspace defense perspective • Provide input for the development of the decision support matrix and decision support template • Provide input and participate in the war-game briefing as required	• For each course of action war-gamed include: – Refined cyberspace defense input to the concept of operations with tasks – Refined cyberspace defense-related information requirements. – Refined cyberspace defense-related essential elements of friendly information – Refined input to DAL – Refined cyberspace defense input to synchronization matrix. – Refined maps and overlays – Refined network infrastructure diagrams and charts • Draft Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal) and/or draft Risk Mitigation Plan

Table 2. (U) Course of Action Analysis

- **(U) Course of Action Comparison:** During COA comparison, supported and supporting cyberspace defenders evaluate the advantages and disadvantages of each COA from their perspectives using the inputs shown in Table 3. They present their findings for the others' consideration. It is critical TRAs are developed and war-gamed to determine their appropriateness to each potential trigger. At the conclusion of the COA comparison, supported

and supporting cyberspace defenders together generate a list of pros and cons for each COA. The team also develops a prioritized list of the COAs.

Inputs	Cyberspace Defense Actions	Outputs
• Updated running estimate including assumptions • Refined courses of action • Evaluation criteria • War-game results	• In collaboration with the staff, conduct an analysis of advantages and disadvantages for each course of action, emphasizing cyberspace defense aspects. • Provide input to the decision matrix tool as required • Recommend the most supportable course of action from a cyberspace defense perspective • Provide input and participate in the course of action decision briefing as required	• For each course of action include final draft: – Input to the concept of operations with tasks – Cyberspace defense-related information requirements – Cyberspace defense-related essential elements of friendly information – Input to the defended asset list – Cyberspace defense input to target synchronization matrix – Maps and overlays – Network infrastructure diagrams and charts

Table 3. (U) Course of Action Comparison

- **Course of Action Approval:** Supported and supporting cyberspace defenders generate a COA decision brief as an output (Table 4) to help finalize a commander's or other leader's intent based on the COA selected. Commander or other leader guidance provides the team with the final intent, any new critical information requirements, risk acceptance, and direction on the priorities. The output from the effort is finalized in an applicable execution matrix.

Inputs	Cyberspace Defense Actions	Outputs
• Updated running estimate including assumptions • Evaluated courses of action • Recommended course of action	• Receive and respond to final planning guidance from the commander or other leader • Assess implications and take actions to finalize outputs • Provide input to the warning order	• For the approved course of action include refined: – Input to the concept of operations – Finalized list of cyberspace defense tasks – Cyberspace defense-related information requirements – Cyberspace defense-related essential elements of friendly information – Input to the DAL – Cyberspace defense input to target synchronization matrix – Maps and overlays – Network infrastructure diagrams and charts

Table 4. (U) Course of Action Approval

- **Orders Production, Dissemination, and Transition:** Supported and supporting cyberspace defenders provide the appropriate input for several sections of the operation order or plan and associated annexes or appendixes as required (Table 5). This may include input to other functional area annexes such as intelligence, signal, and civil affairs operations as required.

Inputs	Cyberspace Defense Actions	Outputs
• Approved course of action and any modifications • Refined commander's intent • Refined commander's critical information requirements • Refined essential elements of friendly information • Updated running estimate including assumptions • Refined draft Appendix 1 to Annex H (Signal)	• Conduct a more detailed war-game of the selected course of action as required • Participate in the staff plans and orders reconciliation as required • Participate in the staff plans and orders crosswalk as required • Finalize input to cyberspace defense-related operation order appendices and tabs. • Provide input and participate in the operations order brief	• Draft Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal) and/or draft Risk Mitigation Plan • Final Appendix 2 (Information Network Operations) to Annex H (Signal)

Table 5. (U) Orders Production, Dissemination, and Transition

4.2.2.2 (U) Security Operations

(U) Security operations are those operations undertaken to provide early and accurate warning of enemy activities, to provide the force protecting the cyberspace capabilities with time and maneuver space within which to react to the enemy, and to develop the situation that allows for the effective use of the critical assets. As part of security operations; units ready, protect, and ensure resiliency for MRT-C and KT-C. The ultimate goal of security operations is to protect a unit from surprise and reduce the unknowns in any situation. Similar to the land domain, security operations conducted in cyberspace are shaping operations. As a shaping operation, security operations prevent enemy surveillance and reconnaissance assets from determining target system configurations (e.g. IP address, operating system, host services, etc.) and potential weaknesses.

(U) Security operations lead to the survivability of cyberspace capabilities. Survivability is critical to the success of the cyberspace defensive no matter what defensive task is performed. When preparing area and mobile defenses, the network/system administrators supporting the defensive effort help local, regional, and/or global cyberspace defenders prepare survivability positions. The execution of security operations as a cyberspace defense enabling task enables survivability that translates to readiness and resiliency. The focus should be on the ability to execute the mission. Alternate and supplemental positions can translate to network re-routing that ensures traffic flow. If a unit requires a certain level of data throughput (Req Data Rate) and the enemy is degrading throughput (Deg Data Rate) to a certain level, then readiness and resiliency equates to Req Data Rate > Deg Data Rate.

(U) Security operations encompass screening, covering, guarding, area security, and local security.

- **Screening.** Screening is a security task that primarily provides early warning for the protected assets.

- **Cover.** Cover is a form of security operations in which the primary task is to protect the main body (in this case – MRT-C), through mission assurance actions, by fighting the enemy on the network to gain time while also observing and reporting information and preventing enemy

reconnaissance and offensive actions. Units either conduct a cover mission inside or outside friendly networks, operating independently from those implementing DODIN operations (to include cybersecurity) and DCO-IDM directly within the AO.

- **Guarding.** Guarding is a form of security operations whose primary task is to protect the main body (in this case – MRT-C), through mission assurance actions, by fighting the enemy on the network to gain time while also observing and reporting information and preventing enemy reconnaissance and offensive actions. Units conducting a guard mission CANNOT operate independently because they rely on those implementing DODIN operations (to include cybersecurity) and DCO-IDM directly within the AO.

- **Area Security.** Area security is a security task conducted to protect assets, routes, and actions within a specific virtual area of responsibility. Area security measures can deter, detect, or defeat enemy reconnaissance efforts while creating standoff distances between the enemy and enclaves containing KT-C and MRT-C.

- **Local Security.** Local security is a security task that includes low-level security activities conducted on cyberspace assets to prevent surprise by the enemy. Local security measures can help lessen the impact of enemy cyberspace operations and attempt to contain incidents until additional support is brought to bear.

(U) The screen, guard, and cover security tasks, respectively, incorporate increasing employment of cyberspace defense capabilities. Area security preserves a commander's or other leader's freedom to move resources, provide for mission command, and conduct sustaining operations. Local security provides immediate protection to friendly force net-enabled capabilities. All levels of cyberspace defenders (global, regional, and local) are capable of conducting security operations. Ultimately, successful security operations depend on properly applying three fundamentals:

- **Early and Accurate Warnings and Alerts.** Early and accurate warnings and alerts related to the cyberspace defense include attack sensing and warnings (AS&W), indications and warnings (I&W), and vulnerability alerts. AS&Ws assist cyberspace defenders with identifying changes in the network. AS&W includes the detection, correlation, identification, and characterization of a large spectrum of intentional/unauthorized activity, including intrusions and attacks, in near-real time. It couples this with notification to cyberspace defenders so they can implement an appropriate response. AS&W is enabled through a system of integrated sensors and discovery TTPs, all supported by data fusion and analysis, diagnostics, long-term trend and pattern analysis, and warning communications channels and procedures. I&Ws provide information related to a change in adversary activities. I&Ws include those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to operations. Vulnerability alerts ensure units are informed of newly identified system vulnerabilities and deficiencies, and receive and implement appropriate corrective measures. Vulnerability alerts are essential to the overall cyberspace defense as a primary means for improving the unit's defensive posture.

- **Provide adequate reaction time.** System hardening is a critical enabler to achieve reaction time and maneuver space. System hardening is the process of securing a system or network by reducing its attack surface. By the nature of the process, the more functions a system or network performs, the larger the surface. Since most systems or networks are dedicated to one or two functions, reduction of possible attack vectors is done by the removal of any protocols, software, user accounts, or services that are not related and required to the mission. Hardening includes all, but is not limited to the following:

    - Disable unnecessary hardware
    - Remove unnecessary software
    - Restrict use of IP space
    - Disable or remove unnecessary usernames and passwords
    - Disable or remove unnecessary services
    - Apply updates and patches

- **Orient efforts on net-enable capabilities to be defended.** Unlike reconnaissance activities, which orient efforts on the enemy; security operations orient efforts on defended assets. In doing so, security operations are driven by outcomes of vulnerability assessments. Vulnerability assessments provide an ongoing capability to determine the adequacy of cybersecurity measures. In particular, vulnerability assessments apply a variety of techniques (e.g., network discovery, network and host vulnerability scanning, and penetration testing) to identify vulnerabilities for which an advanced or sophisticated cyberspace threat could exploit. The objective is to ultimately remediate vulnerabilities identified. As a way to increase the discovery of vulnerabilities not discovered by routine assessment measures, red teaming/threat emulation activities are performed within a specific, virtual AO. Threat emulation is fundamentally different than penetration testing in that it is an independent and threat based activity simulating an opposing force and focused on readiness improvements. The activity emulates the capabilities and methods of an adversarial force; and it should be utilized across high/extremely high risk areas to identify exploitable vulnerability paths.

4.2.2.3 (U) Reconnaissance & Surveillance

(U) Reconnaissance in friendly cyberspace is a task undertaken to obtain, by observation or other detection methods, information about the activities and resources of an enemy or adversary operating within a specific AO. As an enabler to the execution of reconnaissance, “surveillance” conducted by cyberspace defenders involves the systematic observation of friendly cyberspace through visual or electronic means. Reconnaissance and surveillance are focused collection efforts. A commander or other leader orient their reconnaissance assets by identifying a reconnaissance objective within the AO. The reconnaissance objective in friendly cyberspace can be information about a specific vulnerability, indicator of compromise, or other mission or operational variables, such as specific hardware, software, or network traffic flow considerations. The commander or other leader assigns a reconnaissance objective based on priority information requirements.

(U) The responsibility for conducting reconnaissance operations in friendly cyberspace does not reside solely with one unit. Every organization has an implied mission to monitor its networks

and information systems for friendly and enemy dispositions. Although cyberspace defenders at the regional and local level should conduct some form of reconnaissance within their area of responsibility, global cyberspace defenders are specifically trained in reconnaissance tasks. The three forms of reconnaissance operations applicable to friendly cyberspace are the following:

- **Route Reconnaissance.** Route reconnaissance is a directed effort to obtain detailed information of a specified network or other virtual route and all cyberspace terrain from which the enemy could influence movement along that route. That route may be a satellite link or even a physical access point to a specific system. Route reconnaissance provides new or updated information on route conditions, such as degradation and user/cyberspace threat activity. A commander or other leader directs a route reconnaissance be executed when wanting to gain awareness of a specific route for friendly movement of data and information.

- **Zone Reconnaissance.** Zone reconnaissance is a form of reconnaissance that involves a directed effort to obtain detailed information on all KT-C and MRT-C, critical assets, and enemy forces within a virtual AO. A commander or other leader directs a zone reconnaissance mission when additional information is required before establishing battle positions and committing cyberspace defenders to a mission. Zone reconnaissance is appropriate when the enemy situation is vague or existing knowledge of KT-C and MRT-C is limited.

- **Area Reconnaissance.** Area reconnaissance is a form of reconnaissance that focuses on obtaining detailed information about the KT-C, MRT-C, and enemy activity within a prescribed area of responsibility. An area reconnaissance is conducted across multiple network enclaves or within areas of the network that act as centralized, boundary access points or data centers. The primary difference between an area reconnaissance and a zone reconnaissance in friendly cyberspace is that in a zone reconnaissance, cyberspace defenders first move to the AO in which the reconnaissance will take place. In an area reconnaissance, cyberspace defenders conducting the reconnaissance start from a several points of presence into network boundaries.

(U) Critical to reconnaissance is the process of tipping and cueing. Tipping is normally performed by the intelligence community; and the act makes available pieces of addition information to cyberspace defenders that indicate an otherwise unknown fact or probability of an attack. Cyberspace defenders undertake measures to seek out and discover adversary activity on KT-C and MRT-C. When detected, information about the activities and resources of the enemy or adversary must be attributable to effectively destroy them. The most challenging aspect of attributing actions in cyberspace is connecting a cyberspace actor (cyber-persona) or action to an actual individual, group, or state actor, with sufficient confidence and verifiability to hold them accountable. Cyberspace defenders present characteristics, artifacts, and impacts of attacks that cue those on both the intelligence and OCO side. Intelligence and/or cyberspace operators use this information to conduct cyberspace S&R, cyberspace OPE, and/or cyberspace attacks the result in DCO-RA effects.

(U) Successful reconnaissance and surveillance is supported by an appropriate information collection plan. Cyberspace defenders develop an initial synchronization plan to acquire information to help answer those priority intelligence requirements (PIR) based on the available reconnaissance and surveillance assets. The plan assigns specific information collection tasks to

specific elements for action. Cyberspace defenders utilize data stored to analyze, predict, and act upon cyberspace incidents. The objective is to gain value from higher levels of analytic maturity, moving from information and hindsight to optimization and foresight. Analyses are meant to be predictive, prescriptive, descriptive, or diagnostic:

- Predictive analytics – when will it happen?
- Prescriptive analytics – how can it be prevented from happening?
- Descriptive analytics – what happened?
- Diagnostic analytics – why did it happen?

(U//FOUO) Figure 12 illustrates the process for leveraging surveillance and reconnaissance in support of the cyberspace defense using a cyber fusion approach. Analysts within an Analytic Support Element, along with the cyberspace defenders aligned to an operation, receive a mission and overlay what is known about the defended terrain and likely threat in order to develop a situational template. Terrain and friendly cyberspace analysis is facilitated by an understanding of the defended network, key terrain, and a commander's PIR. This understanding is enhanced by various friendly reporting. A threat doctrinal template is generated from all source intelligence and technical analysis. The intent of the template is to highlight relevant internal and external threats; the vulnerabilities they wish to exploit; the type of capabilities or TTPs they are known to use; and their intents and objectives. The resulting situational template leads to detailed problem statements. Problem statements are specifically developed in the context of the terrain (e.g. how might a threat employ a specific TTP on critical assets based on information derived from various intelligence and assessment reports?). This requires analyst to determine significant gaps in what is known about the adversary and other relevant aspects of the operational environment to formulate IRs. Based on the IRs, more specific problem statements are developed (those items of information that must be collected and processed to develop the intelligence required by the commander). IRs related to cyberspace may include threat TTPs, personnel status and readiness of adversaries' equipment, and unique cyberspace signature identifiers.

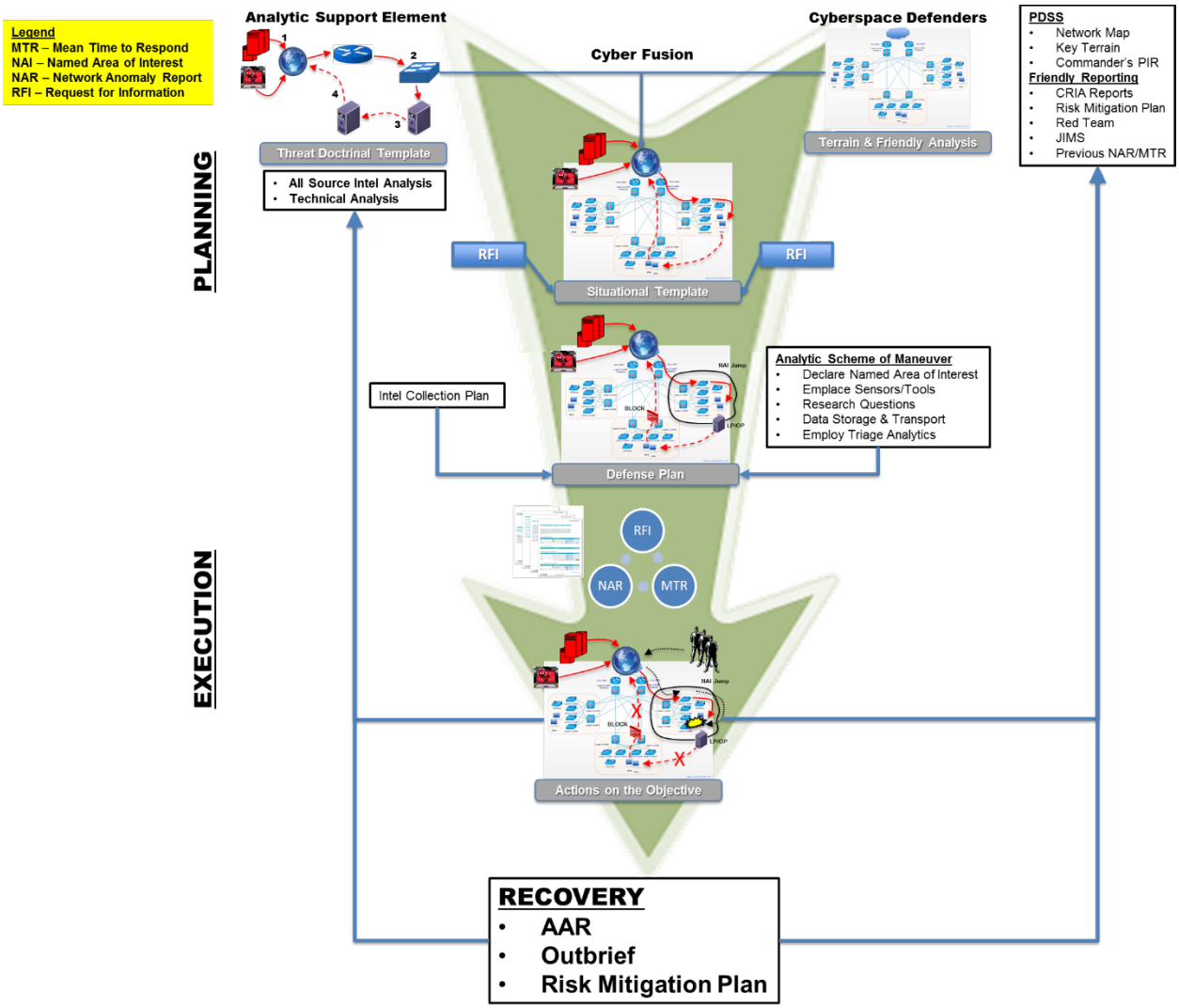


Figure 9. (U//FOUO) Reconnaissance and Surveillance Process

(U//FOUO) Cyberspace defenders then develop a hypothesis to test leveraging collection data. A hypothesis is a single, tentative guess assumed for use in devising experimental tests applied to a problem statement. The hypothesis must be clearly stated, but not so specific as to constrain the data selected. This bound specifications for analytic requirements, workflow, delegation, and collaboration. It additionally drives IPB. That means analysts should be able to tailor the intelligence collection plan in order to show whether the hypothesis is true or false. After the hypothesis has been developed, cyberspace defenders consider what data sources and methods are likely to yield the necessary information to support the analysis to be performed. Part of selection and determination involves timing. If the reason for analyzing data is to identify low-level reconnaissance activities, then the selection needs to be executed during the period the beaconing occurs. Therefore, data selection needs take place at key stages of activity. If the purpose of the selection is to measure performance, then the scope of the data selection is much broader.

(U//FOUO) The aggregation of existing data sources and with the determination of additional data requirements will identify gaps. Data gaps influence how cyberspace defenders tune sensor capabilities running on prepositioned or deployed platforms. Data gaps will highlight sensor vantage points closer to assets on the critical or defended asset list, key terrain in cyberspace, and other relevant input sources (see Figure 13). Ideally, these vantage points are segments within the network that will provide the required visibility with minimal redundancy.

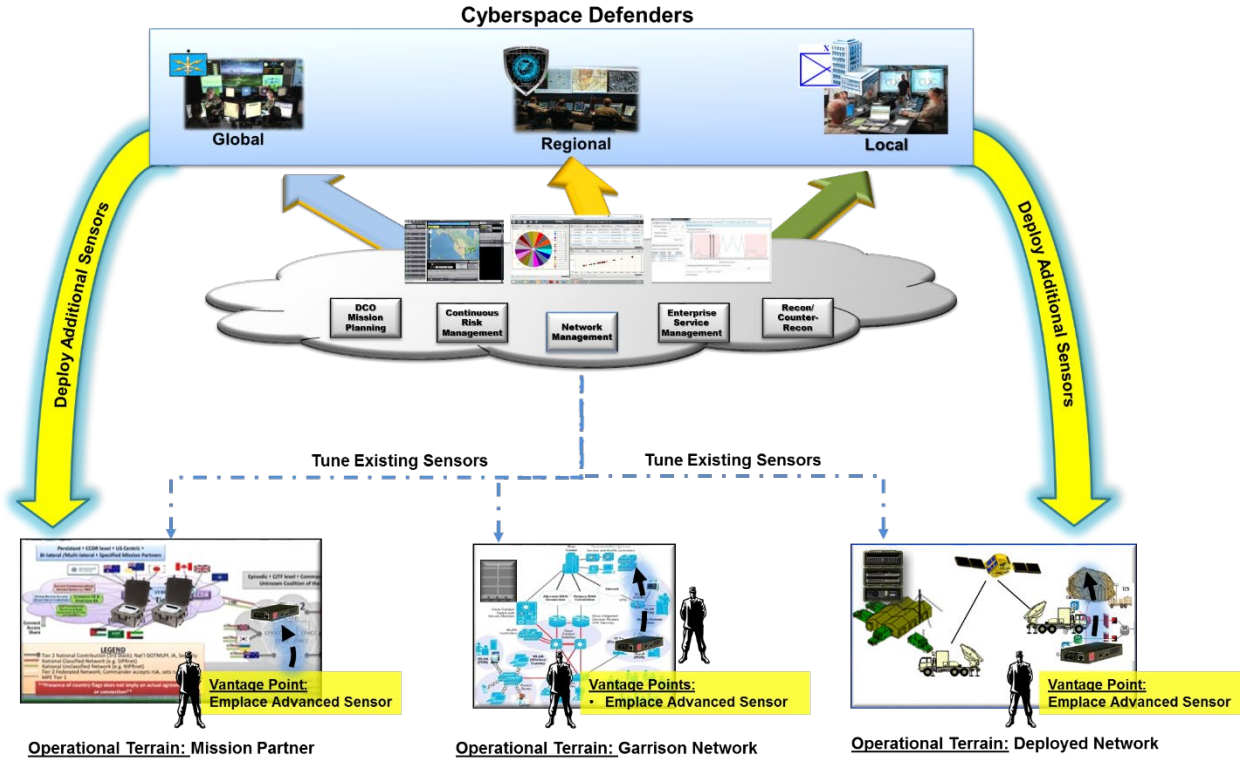


Figure 10. (U//FOUO) Vantage Points and Additional Sensor Placement

(U//FOUO) Cyberspace defenders use their understanding of the supported unit's mission, specific information requirements, and available sources of information to plan, conduct, refine, and record the results of demands on collected information. From the execution of queries, cyberspace defenders create outputs, conclusions, or projections regarding threats and relevant aspects of friendly cyberspace to answer known or anticipated requirements that assist in making decisions. Cyberspace defenders develop the situation to predict threat COAs and PIRs. Through predictive analysis, defenders attempt to identify threat activity or trends that present opportunities or risks to the friendly force. They often use indicators developed for each threat COA as the basis for their analysis and conclusions. Finally, reconnaissance and surveillance in friendly cyberspace enables defenders to continually monitor and evaluate the situation, particularly significant threat activities and changes in the operational environment.

4.2.2.4 (U) Maneuver

(U) Maneuver in friendly cyberspace is the employment of forces to an AO through movement in combination with other supporting activities to achieve a position of advantage in respect to the enemy. Basically, a maneuver technique is how a unit positions its subordinate elements in

order to negotiate terrain to set the conditions to achieve its mission. Maneuver is impacted by tactical mobility. Tactical mobility in cyberspace is a function of the relationship between network/system mobility, available cyberspace capabilities, and protection. The level of network mobility provided to cyberspace defenders is based on factors such as available bandwidth, access privileges, routing, host configurations, and other technical characteristics. Given access to advanced cyberspace capabilities, tailored to mission and threat, cyberspace defenders can move within a virtual AO against most cyberspace threats, unless faced with an adversary who can neutralize protection measures in order for it to out-maneuver friendly forces. Local cyberspace defenders, given their knowledge and access to the designated network have a network/system mobility advantage in comparison to regional and global cyberspace defenders. But local cyberspace defenders possess common cybersecurity capabilities that offer a limited level of protection. Global cyberspace defenders possess more advanced cyberspace defense capabilities to conduct DCO missions, yet, unless the designated network is already pre-configured for remote operations, network/system mobility is hampered. Effective maneuver with a high degree of tactical mobility leads to the creation of massed effects against the advanced or sophisticated cyberspace threat.

(U) A maneuvering force can use one or a combination of three techniques; influenced by METT-TC and determined by the control, dispersion, flexibility, and speed desired.

- **In Tandem.** When contact with the cyber threat is highly unlikely and speed is a requirement, then the leader of a maneuvering force will generally coordinate the deployment of elements in tandem. Using the “in tandem” technique, the team as a whole maneuvers simultaneously. Because speed is critical; it is likely that one element will be responsible for establishing and managing the observation post and virtual battle positions, while the other element configures the environment for surveillance and tool employment. When comparing the “in tandem” technique with others, several characteristics step out. First, and most obvious, is that it generates the most speed. Because of the “simultaneous” aspect of the technique, it is the complex. To be successful, proper coordination with the network owner is critical to ensure configurations for access can be executed at a moment’s notice.

- **Tandem Overwatch.** When enemy contact is possible and speed is still important, the leader of a maneuvering force will likely utilize a tandem overwatch. Within a tandem overwatch, the two mission elements are essentially utilizing the “in tandem” technique, while the support element is conducting overwatch. In this scenario, the support element is responsible for the initial setup and management of the observation post and virtual battle positions. The mission elements prepare the main battle and engagement areas. As with the “in tandem” technique, proper coordination with the network owner is critical to ensure configurations for access can be executed at a moment’s notice. But because operations commence as soon as the mission elements move past the line of departure and reach the landing zone, the technique is more complex than executing an in tandem maneuver.

- **Bounding Overwatch.** Bounding overwatch is utilized when the leader of a maneuver force expects immediate contact with the enemy. As the name implies, in bounding overwatch there will be elements conducting maneuver and those who will support the maneuver from already established observation posts, battle positions, and engagement areas. The concept is

pretty basic. There is essentially a mission element maneuvering to the main battle area, while another element positions itself in a designated engagement area. The mission element providing the overwatch enables the supported element using counter-mobility techniques against the enemy. Once the supported mission element adequately emplaces itself, it will halt, execute actions, and be prepared to enable the maneuver of the other element. This process continues as the tactical situation dictates. The critical variable in bounding overwatch is the virtual terrain. Obviously, the overwatch elements need to fight on the terrain, while having observation of the maneuvering element. Second, the virtual terrain by which the mission element is conducting movement must be obscure to the point of providing good cover and concealment from the enemy. The "bounding overwatch" technique is the most complex of the three because it requires continually integration and synchronization between the mission elements, supporting element, and local security force.

(U) Maneuver as a cyberspace defense enabling task can be executed using in-depth, forward, and cordon and search methods.

- **In-Depth.** Cyberspace defenders conduct maneuver throughout the depth of the virtual AO in preparation for follow-on activities meant to disrupt the enemy's cyberspace capabilities. This sets the conditions for cyberspace defenders to regain the initiative. Through in-depth maneuver, a commander or other leader uses economy of force measures in areas that do not involve a decisive operation or main effort to defeat the enemy.

- **Forward.** Forward maneuver leads to cyberspace defenders initiating a tactical conflict with an enemy conducting operations on KT-C and/or MRT-C. Forward maneuver involves cyberspace defenders skillfully moving to an engagement area in order to destroy the enemy and recover from an attack by concentrating all necessary cyberspace defense capabilities and supporting systems. This includes organic and augmentation. Forward maneuver allows cyberspace defenders to take full advantage of the AO and to rapidly appear and focus efforts when desirable. Cyberspace defenders designate engagement areas based on attack vectors and influence the size and shape of virtual engagement areas so as to best array forces that can observe. It is critical that engagement not affect friendly use of cyberspace to conduct net-enabled operations.

- **Cordon and Search.** Cordon and search activities focus on cyberspace threats (internal/external) not detected by routine system administration or other defensive means. While normal detection measures rely on triggers that an incident has occurred, searching relies on discovering indicators of compromise. Indicators of compromise are those artifacts or behaviors that reside in memory, storage, or network traffic that may seem benign at the surface, yet, fall outside the baseline of network behavior in reference to purpose or time. Examples of indicators consist of suspicious registry modifications, hard-coded IP addresses, and sporadic network traffic that appears to be initiated by a command node. Leveraging intelligence, the goal is to search and discover previously unknown indicators and characterize them so an incident can be mitigated or defeated. The outcome of cordon and search activities should ultimately tell a story as to what happened, why it happened, and what is the impact? It should address the mission assurance gap created when other efforts to harden and defend have failed to keep adversaries

out. Although the purpose of detection is to establish a persistent presence on the network, search activities add the aspect of agile mobility.

(U) The fundamentals of maneuver in friendly cyberspace are:

- Focus all efforts on finding the enemy
- Task organize the force and use mission elements to deploy and defend rapidly in any virtual AO
- Keep support elements forces within reach to facilitate a flexible response
- Maintain contact regardless of the course of action (COA) adopted once contact is gained
- Supporting security operations are essential to the success of maneuver to contact

(U) Maneuvering forces (e.g. global cyberspace defenders) typically request the security element (e.g. local cyberspace defenders) to act as a covering force to accomplish specific tasks independent of the main body such as conduct mobility (open access to maneuver force) and selected counter-mobility (e.g. close specific network ports) activities. Mission elements will conduct decisive operations in coordination with local security forces. Decisive operations consist of actions on the objective. As part of actions on the objective, defenders maneuver to battle positions to amass overwhelming combat power across main battle and engagement areas. A mission element leader then task organizes the element to defend one or more objectives at a time. By carefully synchronizing the effects of mission elements, defenders improve the likelihood of success.

(U) The maneuvering force must gain and maintain contact with the enemy. This is a critical aspect of local security since the enemy may try to break contact and distance itself from the critical assets to give it time to determine follow-on actions. The leader's intent determines the level of contact to maintain pressure on the enemy and seize key or decisive terrain. After successful maneuver to an AO, establishing battle positions, and preparing both main battle and engagement areas, the mission support element performs aggressive reconnaissance. This reconnaissance effort should start almost immediately after a defending force begins actions on the objective.

4.2.2.5 (U) Counter-Mobility

(U) As the term portrays, counter-mobility denies mobility to enemy cyberspace forces. Counter-mobility operations are those combined defensive activities that use or enhance the effects of obstacles (e.g. firewall rule, router access control list, and system updates) to deny an adversary freedom of movement and maneuver in friendly cyberspace. Cyberspace defenders employ obstacles and disruptive actions to unhinge the enemy's reconnaissance and attacks. They integrate reinforcing countermeasures with existing obstacles that improve the restrictive nature of the virtual AO and halt or slow enemy OCO. Additionally, cyberspace defenders mitigate reconnaissance or offensive operations by upsetting the enemy's tempo and synchronizing mass effects designed to interfere with the enemy's ability to implement the kill chain process and achieve intents. The goal is to canalize enemy movement into virtual engagement areas and prevent it from withdrawing any part of its cyberspace capabilities.

(U) Counter-mobility operations stress rapid emplacement and flexibility of obstacles. Friendly forces must keep pace with the advancing enemy and be prepared to emplace obstacles accordingly. Time and resources will not permit developing the virtual AO's full defensive potential. A commander or other leader first considers likely enemy reactions, then plans use of available people, processes, and technologies to block avenues of approach or enemy withdrawal. Commanders, other leaders, and staffs furthermore plan use of virtual obstacles to contain an incident and prevent the enemy from covering its tracks by removing all indicators of compromise from the defended network. Counter-mobility operations in friendly cyberspace consist of four types of activities:

- **Engagement.** Engagement in cyberspace consists of a tactical conflict between opposing forces. Engagement area is defined by where a commander or other leader intend to contain and destroy an enemy cyberspace force within a virtual AO using all available cyberspace defense capabilities. Commanders issue Rules of Engagement that specify circumstances for initiating engagement with an enemy force which may be may be restrictive or permissive. For example, a commander or other leader could tell cyberspace defenders to wait until an enemy cyberspace force begins to generate denial effects before initiating counter-mobility operations. Engagement priority specifies the order in which the cyberspace defenders engage the enemy. Engagement priorities are typically based on the type or level of threat and mission objectives.

- **Retention.** Retain in friendly cyberspace is an enabling task in which a commander or other leader ensure KT-C and MRT-C already controlled by a friendly force remains free of enemy occupation or use. A commander or other leader assigning this task must specify the area to retain and the duration of the retention, which is time or event-driven. While a unit is conducting this task, it expects the enemy to attack and prepares to become decisively engaged. A unit tasked to retain a specific piece of MRT-C does not necessary require access to the hardware, applications, or data.

- **Clearing.** Clearing in friendly cyberspace is an enabling task that requires a force to neutralize and remove all remnants of a cyberspace incident from impacted systems or networks. The "clear" function is intended to impact an enemy's ability to conduct cyberspace operations within a designated AO so badly that the enemy cannot perform any function or be restored to a usable condition without it going entirely through the actions to gain and maintain access. The ability to clear eradicates the enemy from an AO that includes the route and the adjacent terrain. Clearing a virtual area normally requires assistance and integration between supporting cyberspace defenders and the main body (network operators assigned to supported units). This allows the main body to operate unimpeded, prevents the unnecessary delay in the main body's OPTEMPO, and defers response actions from the main body for as long as possible.

- **Reconstitution.** Cyberspace defenders conduct reconstitution activities to establish normal operation levels across the network. In response to unauthorized activity, reconstitution consists of orchestrated actions to dynamically reestablish, re-secure, re-route, reconstruct, or isolate MRT-C and data within near-real time. Reconstitution efforts should result in a unit achieving a desired level of operational effectiveness commensurate with mission requirements and available resources. Reconstitution in friendly cyberspace includes regeneration and

reorganization. Reconstitution begins the recovery process. Besides establishing normal operations levels, reconstitution may include withdrawals and retirements of cyberspace assets (to include information). Reconstitute, as a type of counter-mobility operation, attempts to gain time, preserve cyberspace resources, place the enemy in unfavorable positions, and/or avoid operations under undesirable conditions.

(U//FOUO) Reconstitution and Clearing are supported by the following processes or procedures:

- **Post-Incident Analysis.** Cyberspace defenders should conduct a postmortem on an incident to review the effectiveness and efficiency of cyberspace defense actions. Moreover, a detailed understanding of the incident (to include attack vector, impact, time necessary to eradicate, etc.) must be recorded as lessons learned. Post-incident analysis results in an update to the network readiness level, which in comparison to the previous defensive posture, lowers the risk of impact to operations through the intentional disruption of friendly information systems.

- **Prevention.** Cyberspace defenders improve operational, management, and technical controls by implementing approved recovery actions and conducting an after action review of the incident. Networks and systems should be inspected for the same potential vulnerabilities that were exploited by the adversary. The process establishes follow-up strategies to prevent similar incidents from reoccurring. Strategies can include notifications of mandated baseline, or minimum configuration of all hosts residing on the network.

4.2.3 (U) Cyberspace Defense Tactical Missions

4.2.3.1 (U) Defensive Missions Conducted by Friendly Forces

(U//FOUO) Global, regional, and/or local cyberspace defenders integrate activities in order to conduct one or a combination of the following three defensive missions (Figure 14):

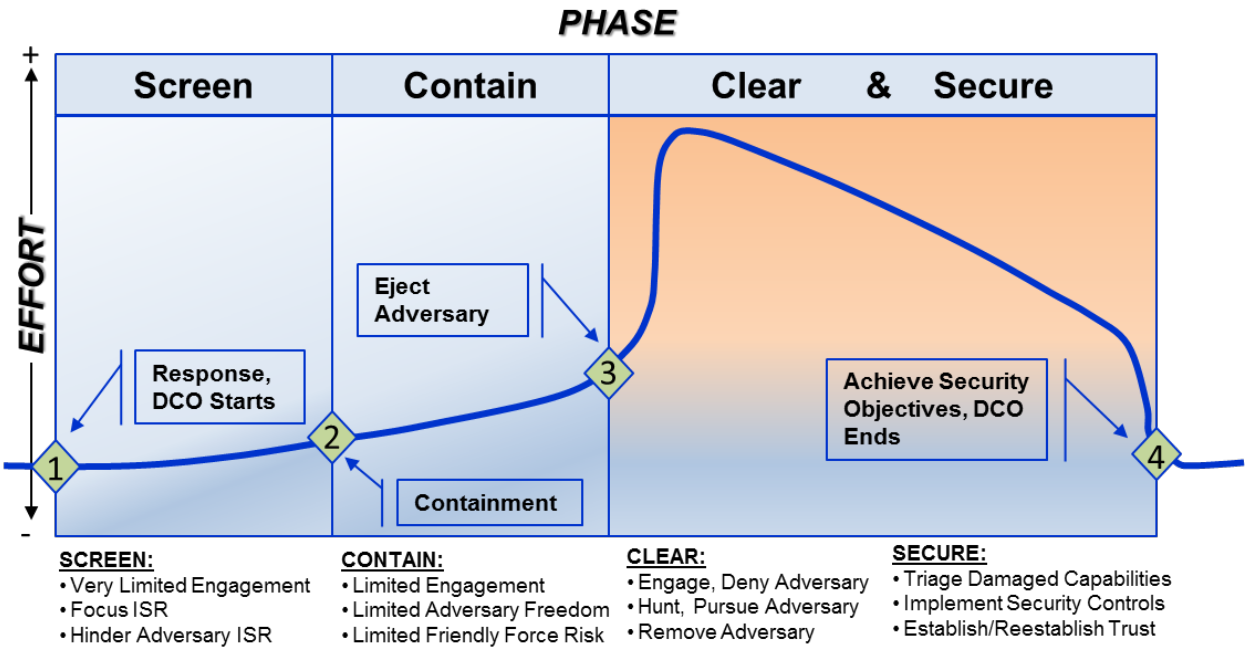


Figure 11. (U) Defensive Missions

- **Screen.** The objective of the screen phase is to locate the adversary, while simultaneously obscuring adversary ISR activities to deny them situational awareness of an impending defensive action. The screen is critical to enabling effective follow-on defensive actions. Screening actions may include executing activities to inform battlespace awareness, hindering adversary reconnaissance, and conducting harassing engagements. The completion of screening objectives triggers decision point two, transitioning the operation into the contain phase.

- **Contain.** The objective of the contain phase is to limit adversary freedom of action and their ability to deliver effects against friendly assets. Key to this phase is the disruption of adversary initiative to constrain their maneuver, force and effects generation capabilities. This is the first phase where active engagement occurs, preparing the environment for clearing operations. The commander must evaluate the success of containment activities to understand risk to friendly forces and assets. This risk evaluation constitutes decision point three, where the commander decides whether to transition into the clear phase.

- **Clear.** The objective of the clear phase is the removal (e.g. capture, withdrawal, and destruction) all adversary forces in an assigned area. This phase is conducted via either a clearing-sector or cordon-and-search types of operations. Clearing actions may include generation of either defensive or offensive effects, or a mix thereof. Friendly clearing actions should persist until adversary forces are removed or risk of their presence is sufficiently mitigated. Adversary forces that are expelled or withdraw must be prevented from reentering the cleared area.

- **Secure.** The objective of the secure phase, which can be conducted concurrently with clear, is to establish, or reestablish, the conditions necessary to transition to other cyberspace security activities. Where feasible, this is best conducted with an isolate-and-secure operation,

moving compromised or damage cyberspace capabilities into isolation, securing them, and transitioning them back into operations. Preferably, the transition back into operations occurs within a known safe area; however, if required, capabilities may be returned to a contested area. Failure to achieve securing objectives may require a return to clearing actions. In such circumstances the operational approach for clearing actions should be reevaluated. Decision point four, is the time at which, secure phase objectives are achieved and the commander makes the decision to conclude DCO.

4.2.3.2 (U) Cyberspace Defense Effects on Enemy Forces

(U) An effect is an outcome or result generated by certain actions. As with any other operation, cyberspace defense actions create effects on enemy forces:

- **Block.** Blocking is an effect that denies the enemy access to an AO or prevents its advancement along an avenue of approach.

- **Canalize.** Canalize is an effect in which an enemy movement is restricted to a narrow zone by exploiting MRT-C coupled with the use of obstacles, counter-fires, or friendly maneuver.

- **Contain.** Contain is an effect that stops, holds, or surrounds enemy forces or causes it to center their activity on a given front and prevents it from covering its tracks.

- **Defeat.** Defeat is an effect in which an enemy force has temporarily or permanently lost the means to conduct cyberspace operations within a designated AO. The defeated force is unwilling or unable to pursue its preferred course of action.

- **Destroy.** Destroy is an effect that damages enemy cyberspace force capabilities so badly that they cannot perform any function or be restored to a usable condition without the adversary starts the process of gaining and maintaining access to a target system over again.

- **Disrupt.** Disrupt is an effect that upsets enemy cyberspace capabilities, interrupts the enemy's timetable, or forces the enemy to execute actions prematurely.

- **Fix.** Fix is an effect that results in preventing an enemy from moving to any part of the defended network for a specific period.

- **Interdict.** Interdict is an effect in which an enemy is denied use of an AO or virtual route. Interdiction is meant to complement and reinforce effects generated from ongoing defensive operations.

- **Isolate.** Isolate is an effect that seals off an enemy from his sources of support, denies it freedom of movement, and prevents it from having contact with other enemy cyberspace capabilities.

- **Neutralize.** Neutralize is an effect that results in rendering enemy cyberspace capabilities incapable of interfering with a particular mission. While neutralize limits impact of a cyberspace attack, it does not remove the presence of compromise.

- **Suppress.** Suppress is an effect that results in the temporary degradation of the performance of an enemy cyberspace force or capability below the level needed to accomplish its mission.

- **Turn.** Turn is an effect that forces an enemy element from one avenue of approach or vector to another.

4.3 (U) Supporting DODIN Operations Activities

(U//FOUO) Even though defending cyberspace is reliant on EW, intelligence, and other IRCs, ultimately, activities must be performed within the Army's portion of the DODIN, as part of DODIN operations, in order for the virtual terrain to be molded and refined into an area that provides functionality, prevents against anomalous network activity, and offers cyberspace defenders maneuver space for which to fight. The execution of DODIN operations and DCO is an oddly cyclical, yet parallel process (Figure 15).

Figure 12. (U) Supporting DODIN Operations Activities

(U//FOUO) Figure 15 is not meant to denote that specific cyberspace defense actions align directly to one DODIN operations activity. The intent is to show a construct in which DODIN

operations supports the cyberspace defense, while outputs of the cyberspace defense must inform DODIN operations. Examples include the following:

- **Plan.** Planning DODIN operations must integrate DCO requirements and strive to achieve a balance between functionality and survivability. Appropriate staff receive a mission, update the running estimate, conduct the initial assessment, and develop preliminary recommendations, which guide subordinate units. Planners gather, analyze, and synthesize information to orient themselves on the task, current OE conditions, and the desired end-state. From this stems mission requirements for both the broader network and MRT-C. Both DODIN operations and DCO plans (DCO-IDM) are packaged together in a single annex so operators understand the concept of operations and required supporting information.

Engineer, Install, and Integrate. The activity of engineering translates the mission into specific work plans, technical orders and communications tasks that provide technical solutions to implement planning products. Engineering is the first step in establishing a defensible network and developing the maneuver space for cyberspace defenders to fight. Applicable personnel define performance metrics and design the network to determine the appropriate configurations. Configuration data offers network and system administrators with the technical information required to protect and ready the network during the installation and integration of cyberspace assets. Configuration data additionally factors necessary IP space, ports, authentications, and other connectivity requirements so access to the network is made available either remotely or onsite via warfighting platforms. Engineering, installation, and integration are not only performed to establish networks and services. These activities are conducted throughout the network's lifecycle and play an important role in updating and modernizing the Army's information enterprise to maintain protection and readiness.

- **Operate and Secure.** The "operate" activity establishes agreed upon service levels; restore service levels in accordance with the Commander's priority; and manage incidents, problems, performance, and change. "Operate" is key in obtaining and retaining confidentiality, integrity, and availability of the network, information systems, and data. As cyberspace defenders work to mitigate incidents, they coordinate with and rely on the operators to make the needed changes to network and systems in order to eliminate vulnerabilities.

- **Govern.** Upon recovery, changes to configurations, processes, and procedures have to be standardize to ensure the same vulnerabilities are not exploited by the adversary again. Cyberspace defenders recommend changes to processes, policies, organizations, and authorities to DODIN operations governance forums in order to achieve the Commander's intent.

4.4 (U) Mission Command of Cyberspace Defenders

(U) As it is with ULO, mission command in the cyberspace domain is the exercise of authority and direction by a commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of cyberspace operations. Exercised by commanders and other leaders, mission command blends the art of command and the science of control while integrating capabilities to execute cyberspace defense enabling and mission tasks.

(U) Enabled by a mission command system; commanders, other leaders, and staffs synthesize and guide actions across applicable levels (higher, lower, and lateral; as well as outside the military). Mission command systems facilitate decision-making that determined a course of action as the one most favorable to accomplish the mission. Moreover, mission command systems enable commanders, other leaders, and staffs to control the movement and placement of defensive capabilities through planning, maneuvering, and scheduling. This includes maintaining in-transit visibility of forces and material through the physical and virtual deployment and/or redeployment process. Mission command is a continuum that involves coordinating and integrating logistics, mission orders, and programs that span the global, regional, and local levels. Supporting mission command systems allow commanders, other leaders, and/or staffs to:

- Conduct the operations process: plan, prepare, execute, and assess
- Conduct knowledge management and information management
- Inform and influence subordinate and supporting forces
- Integrating, synchronizing, and coordinate all elements of the cyberspace defense

(U) All global and regional cyberspace defenders coordinate, conduct, and synchronize operations with the appropriate network owner. Depending on the specific line of operation (Defend the Nation, Protect the DODIN, CCMD Support, or Service-Retained), global cyberspace defenders adhere to a different specified mission command structure. While most global cyberspace defenders are assigned to the Cyber Protection Brigade, global defenders supporting the national mission are normally OPCON to the Cyber National Mission Force Commander. Global defenders focused on the DODIN operate under the control of DISA via JFHQ-DODIN. CCMD aligned defenders logically are OPCON to a CCMD Commander. Finally, Service aligned defenders directly support Service controlled AOs , but are OPCON by the USACPB.

5.0 (U) WARFIGHTING CAPABILITIES

5.1 (U) Required Cyberspace Defense Capabilities

(U//FOUO) The requirement to defend Army networks influences the identification of essential capabilities required to maneuver within friendly networks, conduct reconnaissance, counter the adversary, and execute mission command. Commanders from ARCYBER and other Army Service Component Commands down to the tactical level require cyberspace defense capabilities to execute national, joint, and/or Army operational and tactical missions. These capabilities enable ARCYBER to support USCYBERCOM and defend all Army networks as part of its Service-retained responsibilities. Additionally, these capabilities enable Army National Guard and Reserve forces to support USC Title 10 missions under the auspices of ARCYBER or other major commands. Moreover, these capabilities provide cyberspace support to corps and below commanders in order to protect and defend their organic, deployable net-enabled assets. Finally, cyberspace defense capabilities permit the Army to defend other specified cyberspace and critical infrastructure as part of defense support to civil authorities and host nations.

(U//FOUO) The end-state goal for the Army is to integrate solutions (materiel and non-materiel) that enable cyberspace defenders to operate effectively and efficiently through the domain at the global, regional, and local levels. To achieve this, the following capabilities are required across the Army:

- Leverage intelligence/cyber ISR and analytics to actively predict and conduct counter-reconnaissance (search and discover) against advanced cyberspace threats (to include insider threats) and vulnerabilities that do not trigger or generate warnings using routine detection measures.

- Outmaneuver adversaries by performing preapproved, automated, agile, internal countermeasures that stop or mitigate cyberspace attacks; and when authorized, conduct response actions external to friendly networks in order to create effects that render the adversary's offensive cyberspace capabilities ineffective.

- Conduct cyberspace defense mission planning and protection that identifies and assures the availability of tasked critical assets and infrastructure supporting Army, DOD, host nation, and civil authority actions or missions.

- Achieve survivability of networks, IT platforms, and data through counter-mobility actions, dynamic movement of tasked critical assets, and security enhancement measures.

- Conduct mission assurance actions that dynamically re-establish, re-secure, re-route, reconstitute, or isolate degraded or compromised MRT-C.

- Conduct site exploitation and forensic analysis to determine technical and operational impacts of intrusions.

- Evaluate the defensive posture of KT-C and MRT-C using vulnerability assessment methods and threat emulation in order to recommend or direct changes to ensure operational readiness.

5.2 (U) DCO Infrastructure, Platforms, and Tools/Payloads

(U//FOUO) The purpose of this CONOPS is not to offer recommendations for DODIN operations, OCO, EW, Intelligence, and other IRC solutions that are critical elements for establishing the cyberspace defense. These capabilities must be codified within the corresponding CONOPS and strategies. However, this document should be leveraged by the appropriate authors to influence those capabilities. Ultimately, this CONOPS is meant to highlight those warfighting capabilities needed to fill DCO gaps.

(U//FOUO) Defense of cyberspace requires the development of new solutions based upon an infrastructure, platform, and tool/payload paradigm. For the purpose of this CONOPS, the term "infrastructure" is defined as "the collection of hardware and software/firmware that enables the instantiation and/or execution of software platforms". The infrastructure can be viewed as containing a physical layer; and an abstraction layer when applicable. The physical layer consists

of the hardware resources that are necessary to support the services to be provided via platform deployment, and typically include physical servers, storage and network components. The abstraction layer consists of the software deployed across the physical layer, enabling a common interface to underlying hardware resources providing on-demand services, broad access, resource pooling, and elasticity. The term "platform" is defined as a capability provided to the operator that enables the employment of necessary tools and payloads onto the infrastructure. Platforms are installed on the infrastructure and consist of software such as operating systems, middle-ware, runtimes, databases, web servers, and development environments. A cyberspace "tool" is software, data, or an application that supports or directly causes effects as a result of executing cyberspace defense tactical mission tasks. They are accomplished or managed within a platform. Cyberspace tools are comprised of scripts, analytics, and associated data.

(U//FOUO) Cyberspace defenders require the development of capabilities aligned to the cyberspace defense enabling tasks described Section 4.2. It is important to note the DCO portfolio (Figure 16) consists of a comprehensive array of unique, but mutually supporting solutions. Similar to the Stryker vehicle, .50 caliber rifle, infrared devices, and Blue Force Tracker; DCO solutions can be mixed and matched based on the mission and threat to generate a capability greater than the sum of its whole. But, each solution is managed as a separate program.

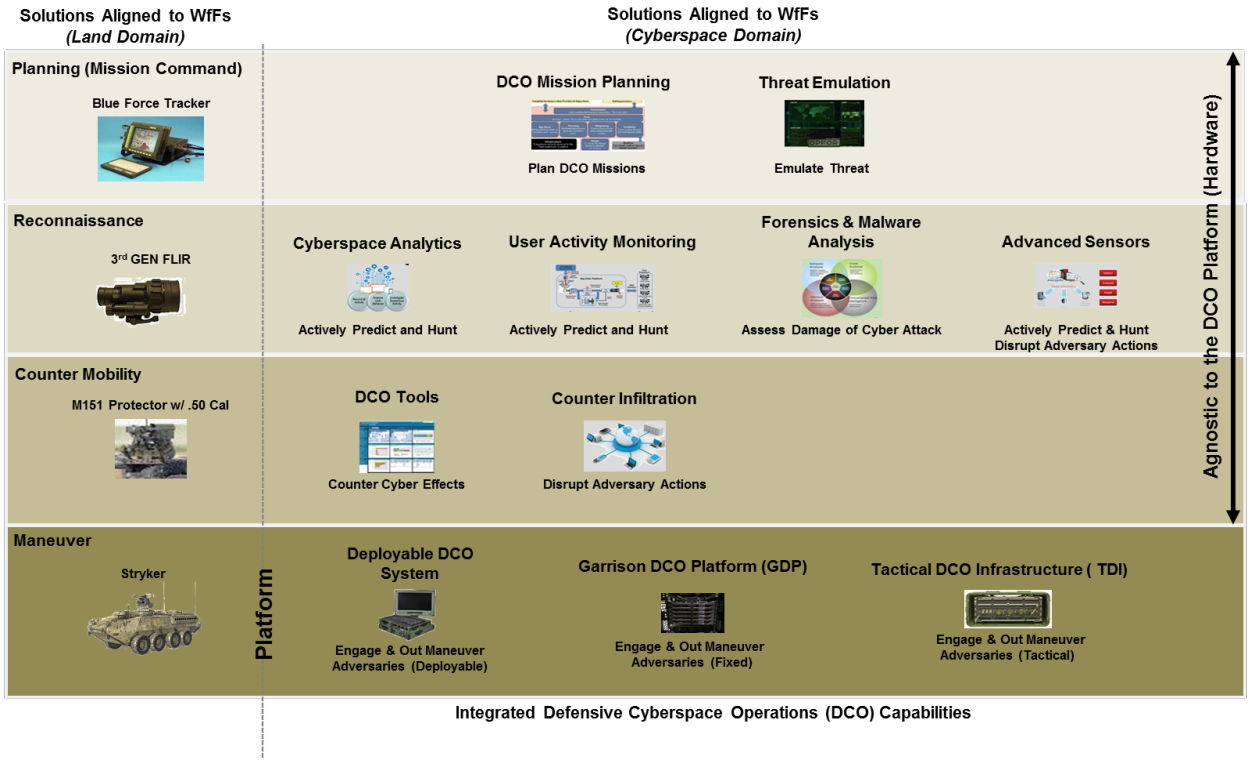


Figure 13. (U//FOUO) DCO Capabilities Portfolio

While the solutions mentioned above may not be employed at the time of publishing this CONOPS, the solutions are described in the present tense below, as these capabilities are forecast to become programs of record.

5.2.1 (U) Cyberspace Analytics

(U//FOUO) The cyberspace analytics capability offers interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate reconnaissance activities meant to discover the presence of advanced or sophisticated cyberspace threats and vulnerabilities. A key feature of cyberspace analytics is the ability to facilitate the identification of threat trends, behavior patterns, and TTPs relative to associated portions of the information environment. The cyberspace analytics capability offers an integrated platform that can be leveraged across all security enclaves (NIPRNET, SIPRNET, and JWICS) to enhance both DCO and DODIN operations. Figure 17 represents an open, standard cyberspace analytics architecture that provides a common solution capable of ingesting, storing, processing, sharing, and visualizing multiple petabytes of data across distributed data sets. A standard architecture ensures consistency amongst agencies, Services, classification domains, and distributed environments. Additionally, a common standard enables separate organizations to develop mutually supporting analytics independently. The supporting compute and storage resources for data ingest, storage, and processing are provided by an underlying, dedicated infrastructure. Data feeds stored by the cyberspace analytics solution provide the blue feed for DCO Mission Planning and Cyberspace Situational Understanding in Support of CEMA solutions.

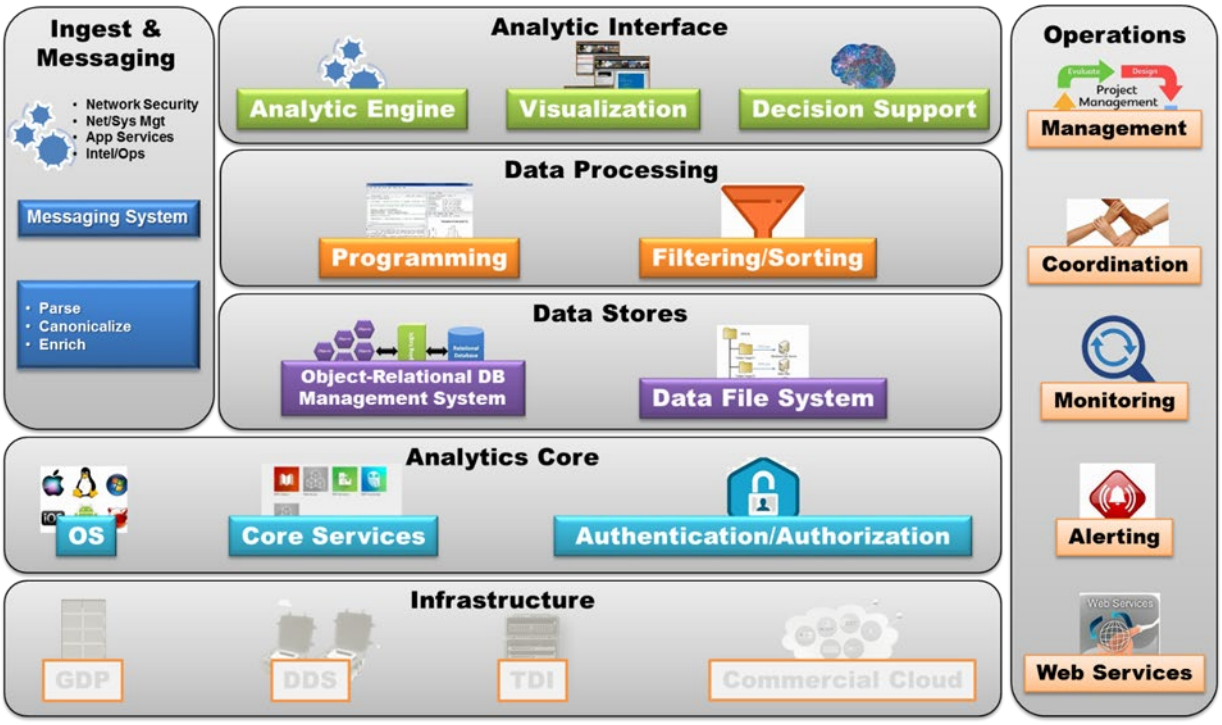


Figure 14. (U//FOUO) Cyberspace Analytics Operational View

5.2.2 (U) DCO-Maneuver Capabilities (DCO-MC)

(U//FOUO) DCO-MCs are the Army's premier DCO warfighting capabilities that enable various cyberspace defenders at the global, regional, and local levels to maneuver to a position of

advantage for the purpose of engaging and initiating a tactical operation against cyber threats and vulnerabilities in defense of KT-C and mission critical, net-enabled capabilities. The DCO-MCs place supported units in a position of advantage over the enemy by rapidly employing cyberspace defenders into an AO to establish the appropriate battle positions for follow-on actions (e.g. security operations, counter-recon, and counter-mobility). Cyberspace defenders spin up virtual platforms to execute DCO actions in real-time, enabling commanders to take immediate measures and facilitate decentralized execution of the cyberspace defense.

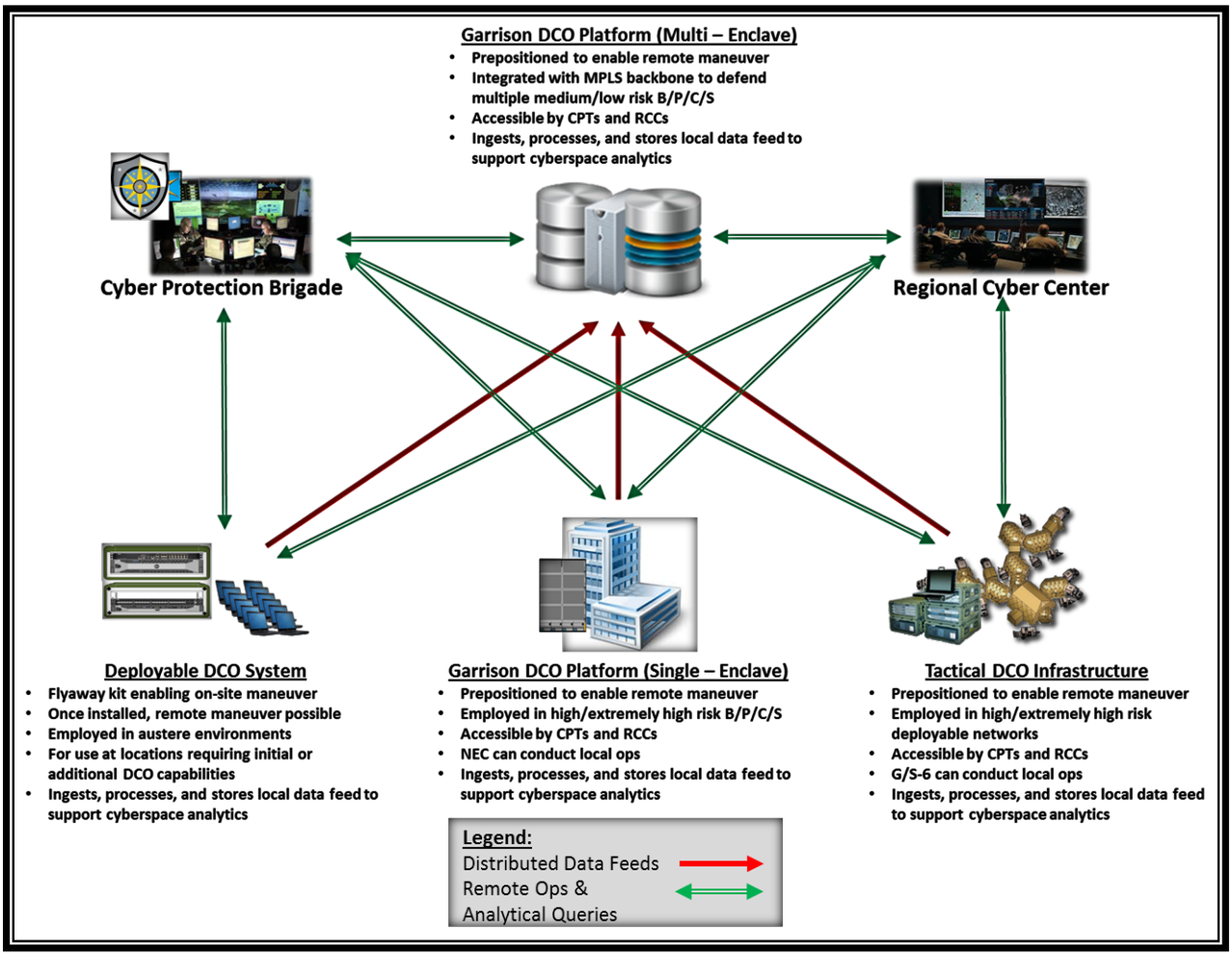


Figure 15. (U//FOUO) DCO-Maneuver Capability Types

(U//FOUO) DCO maneuver warfighting platforms make it possible for cyberspace defenders to move in and out of battle positions to conduct multiple actions against multiple threats in support of multiple missions. Figure 18 shows there (3) types of DCO-MCs (Garrison DCO Platform (GDP), Deployable DCO System (DDS), and Tactical DCO Infrastructure (TDI); along with the flow of data feeds, and the interconnections that enable the conduct of remote and onsite operations:

- **Garrison DCO Platform (Single-Enclave):** a GDP defending a single network enclave consists of pre-positioned, dedicated compute and storage resources residing at high/extremely high risk installations. The solution provides global or regional cyberspace defenders (e.g. CPTs

and RCCs) a remote maneuver capability in order to augment and/or support local cyberspace defenders with preserving an organization's ability to utilize mission critical data, networks, net-centric capabilities, and other designated systems. A single-enclave GDP is integrated with a garrison network in a way to enable surveillance by ingesting high-volumes of data and enabling visibility of layer 2 & 3 traffic laterally traversing within and out of a B/P/C/S. This supports aggregation and correlation of mission relevant data tied to installations the Army has deemed a priority for the employment of physical and virtual defensive countermeasures.

- **Garrison DCO Platform (Multi-Enclave):** a GDP simultaneously providing over-watch for several network enclaves consists of pre-positioned, dedicated compute and storage resources integrated with the MPLS backbone in a way that allows global and regional cyberspace defenders to maneuver to a position of advantage in support of multiple B/P/C/S for which separate GDPs are not required. A multi-enclave GDP is configured to perform more robust data ingest, processing, and storage and act as a centralized data repository to enable the execution of appropriate analytic queries. Because a multi-enclave GDP is integrated with the MPLS backbone at a higher level, it provides visibility of inter-base (layer 3) traffic entering or traversing multiple installations. The result is the development of insights only available by looking across a broad array of enclaves ("locally obscure, globally obvious" – patterns that only become known when understanding the big picture).

- **Deployable DCO System (DDS):** The DDS is a deployable (fly-away) kit, with dedicated compute and storage, for austere environments that do not have prepositioned infrastructure or locations for which prepositioned DCO resources do not provide adequate capacity. The DDS allows global cyberspace defenders (e.g., CPTs) to jump into a network, physically, onsite and gain a position of advantage to augment organic local and/or regional cyberspace defenders (e.g. 255S/25Ds and RCC DCO-Division). The DDS supports maneuver and surveillance activities on a defended network. The DDS is tailorable to support both hasty and deliberate missions utilizing initial and sustained configurations.

- **Tactical DCO-Infrastructure (TDI):** The TDI is pre-positioned, dedicated compute and storage resources residing at echelons corps and below, integrated with high/extremely high risk deployable networks. The TDI provides global or regional cyberspace defenders (e.g. CPTs and RCCs) a remote maneuver capability in order to augment and/or support local cyberspace defenders (e.g., 255S/25D) with preserving an organization's ability to utilize mission critical data, networks, net-centric capabilities, and other designated systems. The TDI is integrated with a tactical network in a way to place defenders at a position of advantage by enabling high-volume data ingest and visibility of mid/upper-tactical internet traffic laterally traversing within and out of a Tactical Operations Center (TOC) or Tactical Command Post (TAC). This supports aggregation and correlation of mission relevant data tied to the operational and tactical level.

5.2.3 (U) DCO Tool Suite

(U) The DCO Tool Suite is a flexible and dynamic (JIE and Command Post Computing Environment compliant), software based suite of warfighting capabilities that enable CPTs, RCCs, and in some cases local defenders, to perform DCO and cybersecurity missions. DCO

tools consist of software, data, or applications that support or directly cause effects related to CMF and cyberspace workforce tasks. They are executed or managed within a platform.

(U//FOUO) How the Army employs its tools within a DCO-MC environment is important. In general, the Army organizes tools by function, yet licensing is also an important factor. Tools are encapsulated into purpose-built platforms, compatible with both deployable and prepositioned capabilities. There are three (3) general types:

- **Publicly available security distributions.** These virtual machines (VM) are managed by open source teams outside of the Army's direct control and there is no restriction to the use of these VMs.

- **VMs containing licensed tools.** These VMs are typically containerized along with an operating system (OS) and vendor-licensed software installed. As the Army has a limited number of licenses, these VMs need to be managed carefully.

- **Orchestrated VMs.** These VMs exist with just enough OS to be able to receive instructions from a host cloud computing OS via an orchestration engine to launch multiple composite cloud applications. These VMs install software during provision time and are the most flexible. Orchestrated VMs are configured and loaded with tools during provisioning and leverage multiple tool and software repositories.

(U//FOUO) DCO tools are functionality aligned to identified performance characteristics. Functional categories consist of site survey; risk assessment; observation; intel support; counter-mobility; developer/operator (DEVOPS), event correlation, and command and control:

- **Site Survey.** Utilize passive and active methods to generate a comprehensive baseline evaluation of the defended network, key terrain, tasked critical assets, and processes for the purpose of obtaining detailed information about specified routes and all terrain from which the enemy could influence movement along that route. The "site survey" capability will be used to evaluate the defended network through a mission impact analysis to identify risks and develop mitigation and countermeasure recommendations. A site survey can focus on network analysis, host analysis, and network mapping.

- **Risk Assessment.** Provide the ability to determine the adequacy of cybersecurity measures for critical assets consisting of various operating systems (e.g. Windows, Linux, and iOS), devices (network and host), as well as websites, mobile, radios, Army warfighting platforms, other devices, and architectures.

- **Observation.** Provide the ability to conduct ongoing observation and analysis (passively and actively) of the operational states of critical networks and systems to provide decision support regarding situational awareness and deviations from expectations. Observation also maintains the ongoing awareness based on signatures and behaviors of networks and systems. Signatures and behaviors will seek out indicators of compromise, which are those artifacts or behaviors that reside in memory, storage, or network traffic that may seem benign at the surface, yet, fall outside the baseline of network behavior in reference to purpose or time.

- **Intel Support.** Provide the ability to understand the operational environment and associated threats. Intel support enables the use of intelligence products (open source (OSINT), SIGINT, HUMINT, and others). The focus of the function is analyzing real-world relationships between information that is publically accessible on the Internet to determine interesting associations.

- **Counter-mobility.** Provide capability that employs disruptive actions on defended networks and devices supporting multiple platforms (covers all major operating systems and architectures. This function is meant to result in the emplacement of obstacles out in front of KT-C and MRT-C along anticipated avenues of approach that result in the interdiction, isolation, blocking, and neutralization of cyber threats and vulnerabilities. A sub aspect of counter-mobility is "clearing" meant to remove all remnants of a cyberspace incident from impacted systems or networks. Clearing consists of verifying either mitigation or actions to remove the indicators of compromise did not generate new indicators of compromise. Clearing enables the conduct of reconstitution activities to establish normal operation levels across the network. The Clearing capability should assist in cyberspace defenders in conducting a postmortem on an incident to review the effectiveness and efficiency of cyberspace defense actions.

- **Developer/Operator (DEVOPS).** Provide opportunities to facilitate foundational, rapid, and real-time development of required payloads (code) by developers at the global and regional levels. The function supports a set of practices that emphasize the collaboration and communication of both software developers and cyberspace defenders while automating the process of software delivery and infrastructure changes. This function offers use of a high-level, general-purpose, interpreted, dynamic programming language that emphasizes code readability, and allows programmers to express concepts in code efficiently.

- **Event Correlation** – provide the ability to better understand the technical details, root cause(s), and potential impacts of a cyberspace incident. This function identifies connections and trends between incidents within a designated defended network in the short term and patterns across enterprise-wide incidents in the long term.

- **Command & Control** – allow leaders to command and control the configuration and management of DCO tools without adversely impacting or degrading the defended network such that it cannot adequately support operations. The function is performed through the storage and management of tools in a central location (variant of DCO infrastructure) to reduce the impact to users. In a centralized model, tools are retained in a repository.

- **Industrial Control Systems/Supervisor Control and Data Acquisition (ICS/SCADA)** – provide a capability to protect and defend ICS using the SCADA architecture. The function includes planning and visualization that generates, optimizes, verifies, and examines sequences of mechanical assembly by directly exploiting three-dimensional computer-aided design models.

5.2.4 (U) Forensic and Malware Analysis

(U//FOUO) The Forensics and Malware Analysis (F&MA) warfighting capability adheres to the global standard in digital investigation technology for global or regional cyberspace defenders who need to conduct efficient, forensically-sound, data collection and examination either remotely or locally using a repeatable and defensible process. Forensics gives cyberspace defenders the ability to triage by quickly viewing and searching potential evidence in order to determine whether further examination is warranted. A portable capability enables cyberspace defenders to review information stored on deployed computers in real-time – without altering or damaging the information. Forensic examination will determine subsequent actions in order to collect, process, search, and analyze evidence from portable electronic devices, removable media, system hard drives, and random access memory. The Malware Analysis capability is a software-based application utilized by global and regional defenders to analyze malicious code. Malware analysis provides a sandbox-like, virtual environment that allows for the conduct of real-time, automated and dynamic malware decomposition and behavior analysis. Malware Analysis allows for the submission of malware samples in a member-only, protected environment in order to collaborate and receive assistance. It also enables analysts to check samples against popular open source tools and identify malware families using correlation and visualization tools. This feature of malware analysis is possible due to an inherent number of algorithms capable of identifying similarities between malware samples.

5.2.5 (U) Insider Threat Detection

(U//FOUO) Insider threat detection warfighting capability is a software-based, scalable user activity monitoring (UAM) solution that proactively identifies and mitigates internal risks associated with the theft or misuse of critical, mission essential data. UAM assists with the establishment of the Army's Insider Threat Protection (specifically Line of Effort #3 – Protect the Network) that utilizes full-spectrum solutions to assess, deter, deny, defend, defeat, and evolve against the insider threat. UAM facilitates the ability to identify insiders threats based on policy violations, as well as the capturing of certain risk behaviors that rate the likelihood of an incident caused by a trusted insider. UAM correlates "pattern of life" data to drive endpoint activity monitoring and control, the capturing and analysis of user actions (with the ability to replay), investigations, and the adaptation of an organization's insider threat countermeasures. It identifies individuals who are at higher risk for being targeted by foreign intelligence or those who are more likely to misuse elevated access privileges. UAM provides cyberspace defenders with a picture of the insider threat risk profile across an organization.

5.2.6 (U) DCO Mission Command and Planning (DCOMP)

(U//FOUO) DCOMP is an application-based, scalable warfighting capability for Army DCO mission command and planning at the global, regional, and local levels. As Figure 19 portrays, DCOMP enables integration, coordination, and synchronization of supported and supporting cyberspace defenders. DCOMP integrates network security requirements, intelligence, and vulnerability analyses, with a commander's operation order (e.g. mission statement, commander's intent, planning guidance, initial commander critical information requirements/essential elements of friendly information, and assumptions), and other military decision-making process outputs, and actions to identify KT-C and mission critical assets; determine probable attack vectors; and produce a set of relevant internal defense measures,

triggers, and decision points. The result is the automated production of the appropriate operations order (OPORD) appendix, which is then war-gamed in a simulation engine for evaluation and improvement. DCOMP utilizes the final OPORD to rapidly provision necessary platforms so cyberspace defenders can execute mission in near real-time. Cyberspace defenders use DCOMP to provide input to the operations process via the detailed information on cyberspace effects generated within the operational environment. Commanders, other leaders, and staffs utilize a common operating picture to assist force management (e.g. what cyberspace defenders are available; what knowledge, skills, and abilities do they possess; and what is their locations), battle tracking (e.g. event management), logistics management, prioritization of efforts, as well as directing and synchronizing actions.

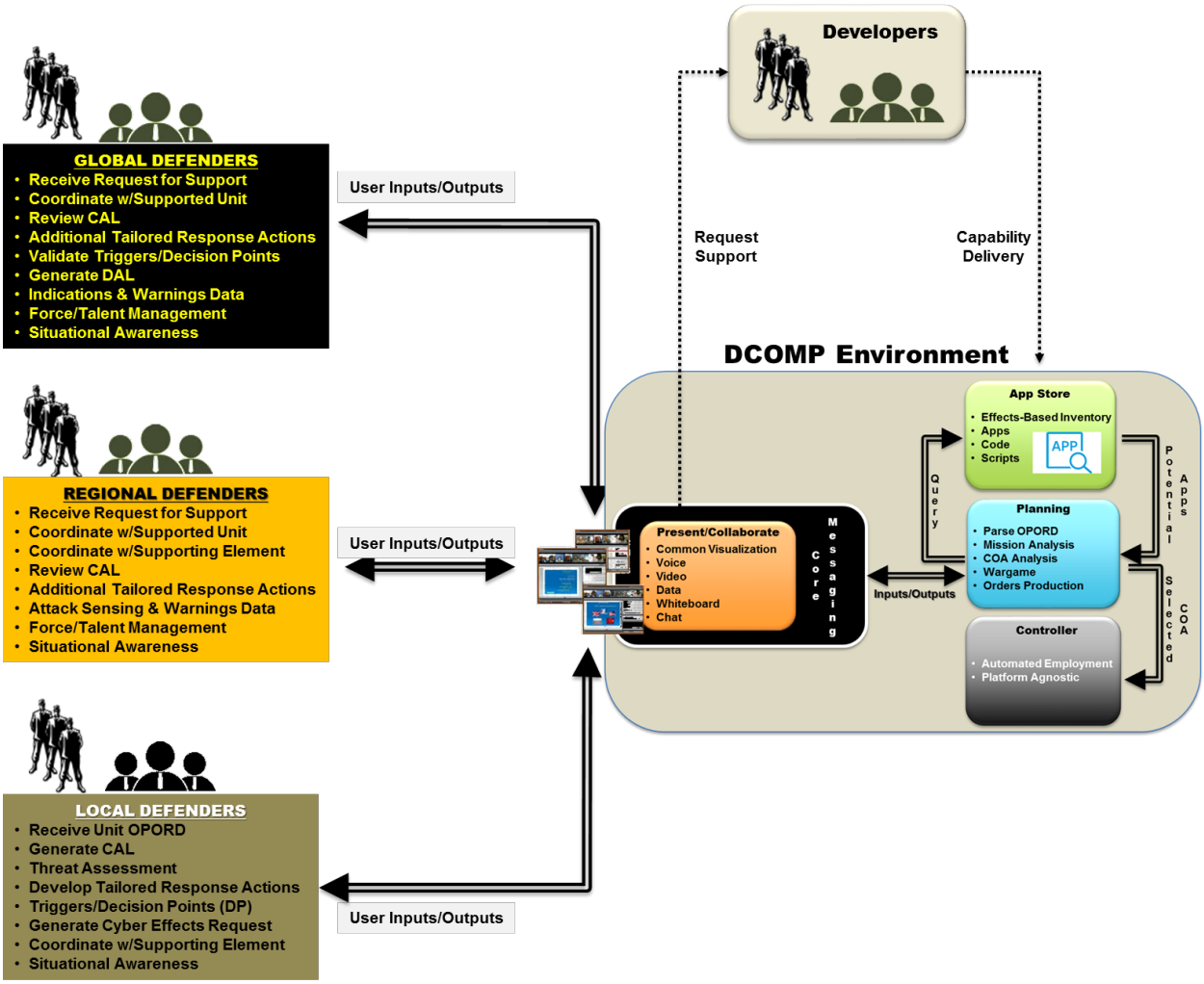


Figure 19. (U//FOUO) DCOMP Environment

(U//FOUO) DCOMP leverages a modular framework that enables cyberspace defenders to execute a common workflow across multiple echelons using a standard presentation and collaboration component. An App Store acts as an arms room to maintain a core set of warfighting capabilities. Using the output of planning and wargaming, the solution acts as a decision support system to automatically select the correct COA that includes infrastructure types, application of tailored response actions (TRA), tactics, and capabilities based upon

mission type, activity, and authorities. The solution receives data feeds to generate situational awareness related to execution of the plan and overall assessment. As the capability matures, DCOMP will begin intelligently suggesting tools and actions based upon identified cyber threats and vulnerabilities. Building upon this, DCOMP can then present a wider array of activity sequencing suggestions, as well as combine app suggestions with activity planning, where users focus more on validating intelligence suggestions and nominating courses of action and plans for approval than they do building them.

5.2.7 (U) Advanced Cyber Sensors

(U//FOUO) An advanced sensor offers a simple, very small, low-cost device that is conceptually employed similar to a Platoon Early Warning system along likely avenues of approach. Advanced sensors provide an automated monitoring and incident handling capability lower in the network architecture (access layer) to conduct over-watch for high-risk units or systems that normally operate out of view ("last mile") from traditional, routine security or DCO measures.

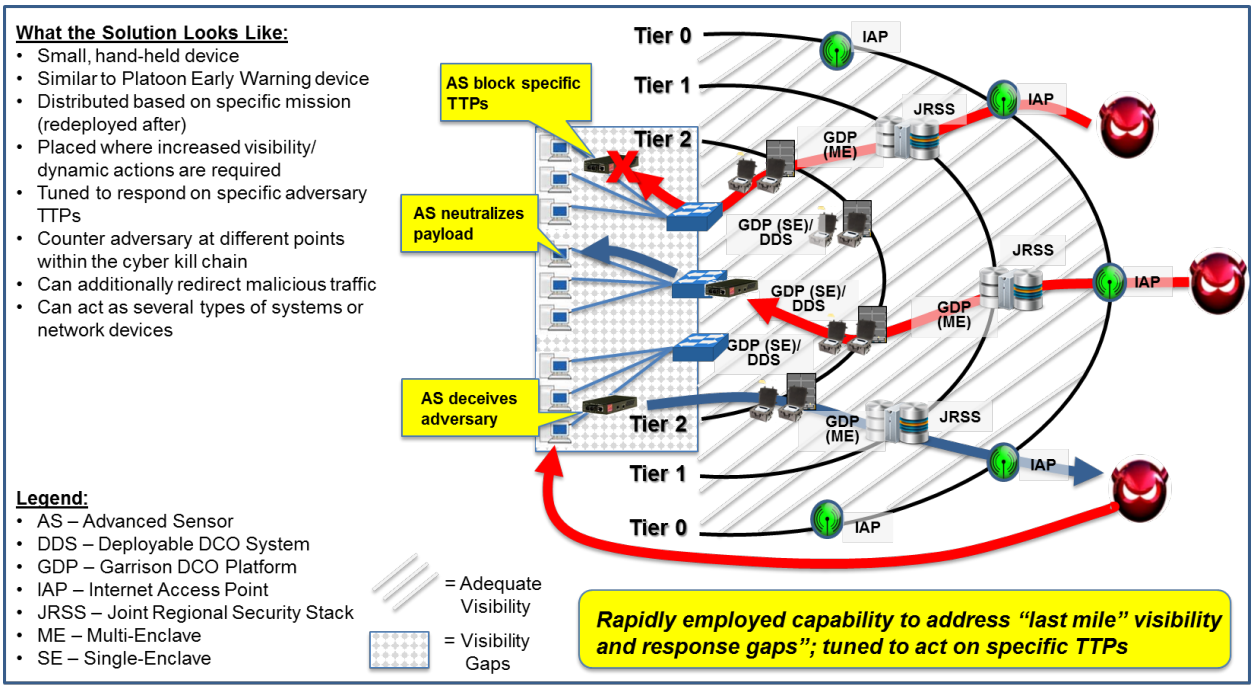


Figure 16. (U//FOUO) Advanced Sensor Operational View

As Figure 20 depicts, the primary measure of effectiveness of an advanced cyber sensor is real-time discovery of specific advanced or sophisticated cyber threats and vulnerabilities on a critical system or segment of the network. When a TTP is detected, advanced sensors can execute a myriad of tailored response actions (block, neutralize, deceive, redirect, etc.) on the associated payload. The result is an increased ability to interrupt the adversary at the beginning of the cyber kill chain by employing counter-measures during the reconnaissance and weaponization phases; and neutralizing and/or deceiving the adversary during the delivery, exploitation, and installation phases. To enable this approach, advanced cyber sensors incorporate indications and warnings (I&W) algorithmically to provide identification and reporting of time-sensitive information on developments that could involve a threat to the network.

5.2.8 (U) Cyber Threat Counter-Infiltration

(U//FOUO) The cyber threat counter-infiltration capability consists of an array of components that retrogrades mission critical assets from virtual areas under a cyberspace threat actor's control using stealth, deception, surprise, or clandestine movements. The capability changes the identity of assets between relatively small time periods based on mathematical algorithms. Mission critical assets within the same virtual area of operations share certain, common information, which results in an asset not only knowing it's next identity and location, but it is additionally aware of the next identity and location of all other mission critical systems. As time progresses, systems within the same AO retrograde in unison. Characteristics of a system that can change consist of IP address, media access control address, ports, protocol, services, computer name, etc. The capability allows commanders and leaders to trade space for time by slowing down the advanced persistent threat's without becoming decisively engaged.

5.2.9 (U) Threat Emulation

(U//FOUO) The Threat Emulation warfighting capability consists of a solution used to gain access to evaluated networks and systems through multi-vectors of unknown ("blackbox"), partially known ("graybox"), or known ("whitebox") access methods. Threat Emulation enables the implementation of real world threat TTPs against risk areas such as web services, endpoints, passwords and identities, phishing and social engineering, mobile devices, and wired/wireless network systems in order to reveal critical security exposures. Threat Emulation empowers users to replicate multi-staged attacks that pivot across systems, devices, and applications in order to identify exploitable vulnerability paths to an organization's KT-C and MRT-C. Moreover, Threat Emulation offers "What-If" attack analyses that demonstrate and document the severity of exposures by not only replicating how an attack would compromise and interact with vulnerable systems, but by also depicting what data would be at risk and why. Threat Emulation establishes a collaborative environment for Threat Emulation and Assessment Teams that allow them to interact in the same workplace against the same environment across multiple instantiations to support rehearsals in an AO. This capability provides a common view of vulnerable assets and determines if network defenses can actually detect threat emulation activity. Additionally, the collaborative environment produces comprehensive reports that assist in planning remediation, demonstrating the effectiveness of layered defenses, validating compliance, as well as validating the implementation of remediation actions.

Annex A. (U) References

Army Cyberspace Operations Capability Based Assessment Final Report V18, pg. 24, 39, and 40, 2 July 2013

Army Doctrine Publication (ADP) 2-0, Intelligence, 31 August 2012

Army Doctrine Publication (ADP) 3-0, Unified Land Operations, November 2016

Army Doctrine Reference Publication (ADRP) 3-0, Unified Land Operations, November 2016

Army Doctrine Reference Publication (ADRP), The Operation Process, May 2012

Army Doctrine Reference Publication (ADRP), Mission Command, May 2012

Field Manual (FM) 3-12, Cyberspace and Electronic Warfare Operation, April 2017

Field Manual (FM) 3-13, Information Operations, December 2016

Field Manual (FM) 3-90-2, Reconnaissance, Security, and Tactical Enabling Tasks, March 2013

Field Manual (FM) 6-0, Commander and Staff Organization and Operations, May 2014

Field Manual (FM) 6-02, Signal Support to Operations, 22 January 2014

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains Whitepaper, Lockheed Martin, 24 October 2010

Joint Cyberspace Concept, 01 October 2015

Joint Information Environment Concept of Operations, Version 2.0, 25 January 2013

Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms, July 2017

Joint Publication 3-0, Joint Operations, January 2017

Joint Publication 3-12(R) Cyberspace Operations, February 2013

Joint Publication 3-13.1 Electronic Warfare, February 2012

Joint Publication 6-01, Joint Electromagnetic Spectrum Management Operations, March 2012

MIL-STD-25250, "Joint Military Symbology", 10 June 2014

U.S. Army LandCyber White Paper 2018-2030, 9 September 2013

U.S. Army TRADOC Pamphlet 525-2-1, The U.S. Army Functional Concept for Intelligence, 2020-2040, February 2017

U.S. Army TRADOC Pamphlet 525-3-0, The U.S. Army Capstone Concept, 19 December 2012

U.S. Army TRADOC Pamphlet 525-3-1, Change 1, The U.S. Army Operating Concept (AOC), 2020-2040, October 2014

U.S. Army TRADOC Pamphlet 525-3-3, The U.S. Army Functional Concept for Mission Command, 2020-2040, February 2017

U.S. Army TRADOC Regulation 71-20-3, The U.S. Army Training and Doctrine Command Concept Development Guide, December 2011

Annex B: (U) Tactical Vignette

(U//FOUO) The vignette below is based upon Vignettes 1 and 2 from the U.S. Army Cyberspace Operations Capability Based Assessment. It illustrates how the establishment of the cyberspace defense supports commanders operating in a CONUS garrison environment during Phases 0 and 1, and prior to seizing the initiative in Phase 2.

(U//FOUO) IAW the installation as a docking station (IaaDS) concept, an infantry BCT fully utilizes its mission command systems and deployable network while in garrison. IaaDS enables the BCT to connect its expeditionary, net-enabled systems to the Installation Campus Area Network (ICAN) when operating from garrison locations such as the motor pool, a unit headquarters, a Mission Training Complex (MTC), etc. This connectivity also enables the extension of a mission network such as the Afghan Mission Network (AMN) across the Army's portion of the DODIN (a warfighting network) to facilitate pre-deployment training and familiarization with theater resources.

(U//FOUO) The installation Network Enterprise Center (NEC) is the BCT's first line of support for securing mission command networks and systems. The NEC provides support for the Host Based Security System (HBSS) and cybersecurity related incidents. The BCT's tactical systems have live/full access to cybersecurity services through IaaDS to ensure scanning and vulnerability patching is up-to-date and potential security risks have been mitigated or removed. The Regional Cyber Center (RCC) provides cybersecurity services to the BCT for baseline protection, network monitoring and threat detection, incident analysis and response, and general mitigation and remediation of incidents.

(U//FOUO) The BCT S-6, Information Assurance/Computer Network Defense (IA/CND) Cell, in collaboration with the Cyber Electromagnetic (CEM) Element, utilizes the ICAN or deployable assets to connect to the persistent training solution to gain access to a realistic operational environment which simulates the BCT's mission command network and systems. The team is subjected to threat scenarios and capabilities, and local cyberspace defenders counter using cybersecurity tools and platforms that facilitate the performance of applicable TTPs. In the end, the team trains and retains cyberspace defense related knowledge, skills, and abilities, as well as the team is certified as fully mission capable.

(U//FOUO) The BCT is directed to deploy and support an operation in the CENTCOM AOR. The BCT S-6, as a member of the staff, integrates network planning with the overall BCT operational planning activities. The BCT S-6 Section uses the DCO mission planning capability to identify key information and infrastructure that will be vital to every day functions based on EEFIs and the CCIRs. The BCT S-6 IA/CND Cell then requests a threat assessment from the BCT S-2 to identify relevant internal and external threats; the vulnerabilities they wish to exploit; the type of capabilities or TTPs they are known to use; and their intents and objectives. Key information/infrastructure is overlapped with the threat assessment to generate an initial risk profile for the operation that leads to the determination of internal defensive measures (in coordination with the supporting RCC) to be employed at critical points in the network.

(U//FOUO) Through the execution of MDMP via the DCO mission planning capability, the BCT S6 IA/CND Cell determines it does not have the capacity and tools to counter likely threats. Subsequently, the BCT sends an effects request that flows from the BCT staff to division and corps headquarters, to the FORSCOM G-39, and then to ARCYBER. ARCYBER conducts a mission analysis that results in the ACOIC tasking the Cyber Protection Brigade (or Cyber Warfare Support Battalion in the future), which then identifies a CPT or elements of a CPT to support. Additionally, ARCYBER tasks a RVAT to emulate adversaries' cyberspace operations against the organization to identify mission critical vulnerabilities. Concurrently, designated global cyberspace defenders begin integration, coordination, and synchronization with the BCT's IA/CND Cell to plan, train, and implement mitigations for threats and vulnerabilities. The BCT's cybersecurity posture is enhanced by correcting deficiencies in security and defensive operations, policies, and procedures with the end-state of an improved and self-sustaining cyberspace defense.

(U//FOUO) As a BCT continues preparation for deployment, the BCT IA/CND Cell will coordinate through FORSCOM and ARCYBER with the CONUS RCC to begin operational integration (e.g. Enterprise Security Manager (ESM)) and initiate the transfer of cyberspace defense responsibilities to the RCC supporting the theater of operations. The CPT will assist the BCT IA/CND Cell with ensuring the TDI is integrated into the tactical network infrastructure and remote access can be achieved via the Global Agile Integrated Transport (GAIT) and supporting Regional Hub Node. During this phase of preparation, the CPT and BCT S-6 Section will configure the network and systems in order to provide the CPT access on demand when the mission dictates. The TDI will provide the framework from which a CPT can maneuver and augment the BCT's local cyberspace defenders by implementing countermeasures in real-time when requested, enabling the BCT Commander to take immediate action in response to an imminent or occurring cyberspace attack. The RCC will additionally assist the BCT S-6 with receiving cybersecurity services and configuring DODIN operations tools (HBSS, ESM, and Assured Compliance Assessment Solution (ACAS)) so they properly reflect Joint and Army mandates and best practices. The CPT must also ensure DODIN operations feeds are integrated with the cyberspace analytic platform residing on the TDI to collect questionable or anomalous Tier 2 data that must be correlated and analyzed toward determining an event.

(U//FOUO) At this point, the BCT has established the local security necessary to enable the preservation of critical cyberspace capabilities so those capabilities can be applied at the desired time and place. Incident management plans and network damage controls have been developed; and measures have been employed and assessed that offer early and accurate warning of enemy operations. This presents a CPT with time and maneuver space to augment the BCT so as to develop the situation and allow for the effective use of protected assets.

Annex C. (U) Business Operations Vignette

(U//FOUO) The vignette below is focused on a scenario in which a division requires business services critical for the projection of its headquarters to an area of hostilities. It illustrates how establishing the cyberspace defense supports business operations in an enterprise environment.

(U//FOUO) The division leverages defense business systems to receive relevant services. A defense business system is an information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and IT and cybersecurity infrastructure, used to support business activities such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management.

(U//FOUO) The division G-4 must coordinate the necessary logistical support. The Army's logistical system of choice is the Global Combat Support System-Army (GCSS-A). GCSS-A is an Enterprise Resource Planning (ERP) solution that uses commercial software to provide one management information system to perform the Army's supply, maintenance, property accountability, and associated financial management functions in near real-time. GCSS-A is web-based and accessible from any computer with connectivity to the Army's enterprise network.

(U//FOUO) The server side of GCSS-A, along with the associated data, is housed within a DISA operated core data center (CDC). Subsequently, DISA is the division's first line of support for ensuring the availability of the GCSS-A application. Additionally, DISA is responsible for the confidentiality and integrity of created, modified, or stored data. DISA utilizes a Joint Regional Security Stack to control the flow of data in and out of the CDC. The supporting RCC manages the day-to-day operation and configuration of the Army's portion of the CDC for which the division utilizes for GCSS-A.

(U//FOUO) The Army Cyberspace Operations Integration Center (ACOIC) receives the order to increase protection and readiness of the associated GCSS-A platform, search for adversary activities meant to gain access and modify the division's GCSS-A data, and eradicate the enemy if necessary. The ACOIC subsequently tasks the Cyber Protection Brigade, which employs a CPT in support.

(U//FOUO) The designated CPT prepares for the mission by utilizing the predictive analysis capability that leverages the continually operating cyberspace analytics platform to identify trends and behavior patterns of threats and TTPs relative to the specific components of GCSS-A. The CPT feeds data to intelligence centers via the ACOIC, to look for attribution and potentially prepare for DCO-RA through grey space. The CPT uses the output of predictive analysis to support DCO mission planning. The DCO mission planning capability enables the CPT to determine which tools or payloads are available to counter the probable threat. The DCO mission planning capability also generates an executable plan, evaluates the plan via a modeling and simulations engine, and automates the execution of the plan through control of prepositioned, defensive infrastructure. Given there are no pre-prepositioned DCO maneuver capabilities tied to

the Army slice of the CDC, the CPT is sent to the location and integrates a DDS with the associated architecture.

(U//FOUO) The CPT uses the DCO tool suite to improve and harden the defenses around the division's GCSS-A data. The CPT then recons the MRT-C to cordon and search for the adversary's presence using data collected by the cyberspace analytics platform. The CPT determines that the adversary has implanted malware on the server and modified the backside web page script to load the malware on any computer that accesses the GCSS-A supply site.

(U//FOUO) The CPT notifies the supporting RCC. The RCC begins to conduct incident analysis to determine the appropriate response across the enterprise. The CPT locally conducts efficient, forensically-sound data collection and examination using the forensics examination capability. This allows the CPT to quickly triage the incident by viewing and collecting the evidence so GCSS-A can once again become operational. The malware is collected, all presences of it is removed from GCSS-A systems, and the artifact is then sent to the ARCYBER Forensics and Malware Cell for analysis in sandbox-like, virtual environment that allows for the conduct of real-time, automated and dynamic malware decomposition and behavior analysis. The malware is checked against popular open source tools and identified to be malware meant to load on users systems that is meant to steal login credentials.

(U//FOUO) Local cyberspace defenders are directed to employ the threat detection/counter-infiltration tool to search for indicators of compromise within the memory and files of those systems used to access GCSS-A in order to detect, illuminate, and remove malicious activity caused by the malware. This provides the division with real-time protection for critical systems so it can continue to prepare for deployment.

(U//FOUO) At this point, the CPT has eradicated the threat from GCSS-A to enable the preservation of logistical services so those capabilities can enable mission assurance. The CPT will continue to search for adversary activity on the MRT-C and maneuver against and engage the threat using the DDS as necessary. The RCC has employed additional security measures across its portion of the enterprise using the change management process.

Annex D: (U) Cyberspace Defense Tasks

(U) Cyberspace defense tasks must describe what well-trained, well-led, and well-equipped Soldiers and civilians do to ensure freedom of action in and through cyberspace. The tasks below are meant to provide a common language and reference system for doctrine, combat, and training developers. Proponents and schools should use these tasks, the associated measures of performance, and a unit's table of organization and equipment to establish unit-specific, collective cyberspace defense task training and evaluation outlines. Proponent training and evaluation outlines provide the measurable conditions and standards to be used in evaluating an organization and individuals' abilities to perform these tasks. The tasks should also provide a basis for establishing a unit-specific combined arms training strategy. They can inform and supplement the Digital Training Management System by providing a catalog of tasks to assist in identifying and developing a unit mission-essential task list (METL). Codified cyberspace defense tasks in this CONOPS are meant to help commanders develop a METL. Cyberspace defense tasks are primarily linked to Army Task (ART) 5.9.1.2 (Conduct Defensive Cyberspace Operations) and ART 5.10.3 (Conduct Cybersecurity [Activities]). Similar to the need for DODIN operations, OCO, EW, Intel, and other IRC CONOPS, related tasks within those areas that support the cyberspace defense will have to be listed in the associated ARTs. The ARTs for local, regional, and global cyberspace defenders are as follows:

1. (U) Local Cyberspace Defense Tasks

(U) ART 5.10.2.3 Conduct Cybersecurity [Activities]

(U) Cybersecurity prevents 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. Cybersecurity functions consist of identify, protect, detect, respond, and recover. Cybersecurity aids an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

No.	*Scale*	*Measure*
01	Yes/No	Unit included cybersecurity as a key element of operational planning activities
02	Yes/No	Unit performed cybersecurity risk management that enhanced the security and resilience of net-enabled operations
03	Yes/No	Cybersecurity efforts and activities considered and accounted for cyberspace threats in all directions, at all times, and in all environments
04	Yes/No	Unit integrated cybersecurity with all other network operations to provide strength and structure to overall effort
05	Yes/No	Unit's critical assets were not compromised and achieved mission assurance
06	Number	Of security layers applied to mission critical systems to counter likely cyberspace threats
07	Number	Of redundancies applied at critical points of failure that offered equal or greater capability.

(U) ART 5.10.2.3.1 Identify Mission Critical Assets, Cyberspace threats, and Vulnerabilities

(U) Units develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. This ART provides understanding of the mission, the resources that support critical functions, and the related cybersecurity risks. This allows an organization to focus and prioritize its efforts, consistent with its risk management strategy and mission needs.

No.	*Scale*	*Measure*
01	Yes/No	Unit conducted an inventory of the organization's physical devices and systems and software applications
02	Yes/No	Unit mapped associated communication and data flows
03	Yes/No	Unit assigned mission assurance categories to systems based on importance of the information they processed relative to achieving commander's goals and objectives
04	Yes/No	Unit identified mission critical assets by determining priorities, objectives, and activities.
05	Yes/No	Unit complied with applicable Army, joint, Department of Defense, and national policies, laws, procedures, and processes
06	Yes/No	Unit determined likely natural or man-made/intentional or unintentional threats and threat agents based on intelligence threat assessment
07	Yes/No	Unit monitored external data sources to maintain currency of threat condition
08	Yes/No	Unit conducted a vulnerability assessment to discover flaws, loopholes, oversights, or errors that a threat source can exploit
09	Yes/No	Unit performed routine vulnerability assessments and vulnerability management procedures to manage system and network vulnerabilities
10	Yes/No	Unit applied remediation actions specified in the vulnerability management. If unit cannot implement the vulnerability management, it submitted a mitigation plan to the Army Cyber Command vulnerability tracking databases
11	Time	Required to share scanning results with appropriate entities to help eliminate similar vulnerabilities in other information systems
12	Number	Of times unit requested intelligence on latest threat tactics, techniques, and procedures
13	Number	Of vulnerabilities discovered through scheduled and unscheduled vulnerability scanning

(U) ART 5.10.2.3.2 Protect Networks, Information Systems, and Data

Units develop and implement the appropriate safeguards to ensure delivery of critical services. This ART supports the ability to limit or contain the impact of potential cyberspace events.

No.	*Scale*	*Measure*
01	Yes/No	Unit applied or assigned an information condition based on the status of information systems, military operations, and intelligence assessments
02	Yes/No	Unit protected networks, information systems, and data by utilizing access control
03	Yes/No	Unit protected data at rest and in transit utilizing communications security
04	Yes/No	Unit implemented principles, structures, and standards for hardware and software acquisition and lifecycle management
05	Yes/No	Unit implemented host-based security to protect information systems from viruses and malware
06	Yes/No	Unit implemented telecommunications and network security for transmissions over private and public communications networks and media
07	Yes/No	Unit established alert thresholds of network monitoring systems
08	Yes/No	Unit created a continuity of operations plan in case of incidents that interrupt or may interrupt normal operations
09	Yes/No	Unit implemented physical security measures to protect the network and systems against damage, loss, or theft
10	Yes/No	Unit implemented electronic protection to protect personnel, facilities, and equipment from friendly or enemy use of the electronic spectrum that degrade, neutralize, or destroy friendly combat capability

11	Time	Unit had internal policies and implements operations security to protect against social engineering type attacks
12	Percent	Of users who received cybersecurity training

(U) ART 5.10.2.3.3 Detect Anomalous Network Activity

(U) Units develop and implement the appropriate activities to identify the occurrence of cybersecurity events. This ART enables timely discovery of cyberspace events.

No.	*Scale*	*Measure*
01	Yes/No	Unit baselined all network and information systems configurations and behaviors
02	Yes/No	Unit employed technologies such as intrusion detection systems and other sensor and logging devices to discover and report anomalous behavior
03	Yes/No	Unit incorporated monitoring of the physical environment and personnel activity
04	Yes/No	Unit was postured to support law enforcement and counter-intelligence activities when applicable
05	Time	Taken to categorize and report incidents to the appropriate entities
06	Number	Of network anomalies detected over a 24-hour period
07	Percent	Of time unit monitored network for anomalous activity to provide timely warning of incidents and attacks

(U) ART 5.10.2.3.4 Respond to Anomalous Network Activity

(U) Units develop and implement the appropriate activities to take action regarding detected cybersecurity events. This ART supports the ability to contain the impact of potential cyberspace events.

No.	*Scale*	*Measure*
01	Yes/No	Unit had a well-defined plan that described processes and procedures for dealing with an incident
02	Yes/No	Unit developed activities to prevent expansion of an event, lessen its effects, and create conditions to eradicate the cause
03	Yes/No	Unit collected logs and other forensic evidence for examination and validation
04	Time	Required to handle incidents and achieve mission assurance
05	Time	Required to understand technical details, root causes, and operational impact of incident

(U) ART 5.10.2.3.5 Recover Networks, Information Systems, and Data

Units develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity events. This ART supports timely recovery to normal operations to reduce the impact from cyberspace events.

No.	*Scale*	*Measure*
01	Yes/No	Unit conducted a post-incident analysis and review of incident handling procedures
02	Yes/No	Unit developed follow-up strategies that supported prevention goals
03	Time	Required to establish normal operation levels across the network and eradicate threat

2. (U) Regional Cyberspace Defense Tasks

(U) Regional cyberspace defenders also conduct cybersecurity tasks listed above that provide for an area defense. Along with these tasks, regional cyberspace defense tasks are executed as part of a broad range of cybersecurity services; implemented as an enterprise DCO capability. DoDI 8530.01 identifies a specific set of cybersecurity services that are required to support the cyberspace defense. These services include: Enterprise Protection, Vulnerability Assessment and Analysis; Vulnerability Management; Forensics/Malware Analysis; Attack Sensing and Warning (AS&W) and Indications and Warning (I&W); Insider Threat Identification and Evaluation; Cyber Incident Handling; and Information Security Continuous Monitoring. Note that this is the minimum set of services, aspects of which are implemented and executed at various levels within the Army's portion of the DODIN. The following tasks are mapped to RCC Mission Essential Task List as part of the RCC Standardization effort conducted by ARCYBER and NETCOM.

(U) Provide Enterprise Protection Services

(U) Units develop and disseminate the appropriate safeguards in order to protect the network, information systems, and data across the enterprise. This supports the ability to limit or contain the impact of potential cyberspace events.

No.	*Scale*	*Measure*
01	Yes/No	Unit identifies protection needs (e.g. security controls) for networks and systems within the enclave
02	Yes/No	Unit electronically pushes software updates, security patches, and service releases to end user devices
03	Yes/No	Unit operates, maintains, configures, and monitors web proxy services
04	Yes/No	Units blocks user access to Internet sites that have been deemed inappropriate for use by a government owned and operated computer system
05	Yes/No	Unit manages and configures network protection devices (e.g. firewalls, remote access, IDS/IPS, router ACLs, and anti-virus)
06	Yes/No	Unit performs security reviews with stakeholders to identify gaps in security architecture that results in the development of a security risk management plan
07	Yes/No	Unit provides input to the Risk Management Framework process and related documentation (e.g., system lifecycle support plans, concept of operations, operational procedures, and maintenance training materials)
08	Yes/No	Unit provides policy guidance to network/system administrators, leaders, and users
09	Yes/No	Unit maintains deployable DCO kit to support associated missions
10	Yes/No	Unit promotes awareness of security issues and ensures sound security principles are well socialized
11	Yes/No	Unit creates and distributes regional technical cybersecurity instructions

(U) Perform Vulnerability Assessment and Analysis

(U) Vulnerability Assessment and Analysis provide an ongoing capability to determine the adequacy of cybersecurity measures. In particular, vulnerability assessment and analysis applies a variety of techniques (e.g., network discovery, network and host vulnerability scanning, penetration testing) to identify vulnerabilities and conformance with recommended policies and configurations, and to assess impact and risk associated with these findings.

No.	*Scale*	*Measure*
01	Yes/No	Unit identifies constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the supported organization
02	Yes/No	Unit identifies risk tolerance for supported organization
03	Yes/No	Unit identifies priorities and trade-offs considered by the organization in managing risk
04	Yes/No	Unit conducts network and host-based scanning with results being provided into the enterprise COP data store for stakeholder review and action, where appropriate
05	Yes/No	Unit conducts Information Assurance Vulnerability Management compliance scanning and maps results to associated Plan of Actions and Milestones
06	Time	Required to isolate non-IAVM compliant asset
07	Yes/No	Penetration testing is conducted within the scope of established test plans and procedures
08	Number	Of threats and vulnerabilities identified from vulnerability assessment
09	Yes/No	Unit verifies software, network, and information system accreditation and assurance document
10	Time	Required for unit to implement cybersecurity audit processes
11	Yes/No	Unit maintains deployable DCO kit to support associated missions
12	Yes/No	Unit maintains knowledge base of applicable policies, regulations, and compliance documents related to DCO/cybersecurity
13	Yes/No	Unit prepares reports that identify technical and procedural findings linked to known or potential vulnerability risks
14	Yes/No	Unit reviews and analyzes intelligence products to determine operational risks

(U) Manage Vulnerabilities

(U) Vulnerability Management proactively prevents the exploitation of Army network and system vulnerabilities within an enterprise. Vulnerability management is an ongoing practice of identifying, categorizing, remediating, and mitigating asset vulnerabilities. The primary objective of vulnerability management is to detect and remediate vulnerabilities in a timely fashion based on threat and mission. Vulnerabilities can be mitigated or accepted based on risk management decisions (e.g., threat impact is low; correction would impact mission operations). These actions will be managed IAW appropriate laws and applicable Army, DOD, and joint regulations.

No.	*Scale*	*Measure*
01	Yes/No	Unit assists supported organization with developing an appropriate course of action to mitigate risk and evaluates POA&M for feasibility and suitability
02	Yes/No	Unit provides the appropriate expertise to assist the inspected organization with recommended computing and network environment corrections before, during, and after the Command Cyber Readiness Inspection.
03	Time	Required to implement the selected course of action to mitigate risk
04	Yes/No	Unit maintains knowledge base of applicable policies, regulations, and compliance documents related to DCO/cybersecurity
05	Yes/No	Unit prepares reports that identify technical and procedural findings, and provides recommendations for remediation
06	Yes/No	Unit assists supported organization with selection of cost-effective security controls to mitigate risk
07	Yes/No	Unit develops risk monitoring strategy for supported organizations that includes purpose, type, and frequency
08	Yes/No	Unit monitors supported organization network and information systems to verify compliance, determine effectiveness of risk response measures, and identify changes
09	Yes/No	Unit establishes procedures for dissemination of cybersecurity advisories, alerts, and warnings to supported organizations, including those originating out Army and DOD
10	Yes/No	Unit inspects monitoring results to confirm that the level of risk is within acceptable limits
11	Yes/No	Unit reports IAVM compliance in the appropriate database

(U) Analyze Forensics and Malware

(U) Forensics and Malware Analysis helps an organization protect against and respond to software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Forensics and malware analysis helps prevent the Enterprise from a damaging attack by countering unauthorized changes made to software and hardware by malicious code that could otherwise leak information or disable capabilities.

No.	*Scale*	*Measure*
01	Time	Required for unit to triage the effects of malware
02	Yes/No	Unit captures and analyzes network traffic associated with malicious activities using appropriate monitoring tools
03	Yes/No	Unit assists LE/CI in the gathering and preservation of evidence and artifacts collected using a forensically sound process
04	Yes/No	Unit analyzes intrusion artifacts to determine mitigation techniques
05	Yes/No	Unit conducts analysis of log files, file signatures, hashes, timelines, and other information against established databases to determine source of intrusion
06	Yes/No	Unit has the ability to reconstruct malicious cyberspace activity
07	Yes/No	Unit provides technical summary of findings from analysis
08	Yes/No	Unit maintains forensic/malware toolkit
09	Yes/No	Unit writes and publishes cybersecurity techniques, guidance, and reports on incident findings

(U) Identify Insider Threat Activity

(U) Insider Threat Protection (ITP) identifies and evaluates user activity through an auditing capability that recognizes and evaluates anomalous activity or technical exploitation of Army information. ITP creates procedures to maintain audit data, preserve data chain of custody, and respond to anomalous user activity on Army networks. The compilation of this information allows mission commanders to direct the mitigation of potential damage to data, contacting the applicable Army component. Insider Threat is different in many ways than in current systems. The increased visibility that provides system awareness to the commander also provides increased opportunities for the hostile insider. It also potentially makes the hostile insider's actions more visible to cyberspace defenders. B/P/C/S can see the actions of insiders within their respective network; they must share information to identify hostile insiders and distinguish their actions from unusual but authorized use.

No.	*Scale*	*Measure*
01	Yes/No	Unit collects logs from systems accessed by privilege users
02	Yes/No	Unit assist supported organizations with ITP measures
03	Yes/No	Unit reviews and verifies separation of duties within supported organizations
04	Time	Required for unit to triage detected insider threat event
05	Yes/No	Unit shares data collection with LE/CI
06	Yes/No	Unit operates and maintains ITP system

(U) Sense and Warn of Attacks and Indications

(U) Attack Sensing and Warning provides detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that

an appropriate response can be developed. Indications and Warning provides detection and reporting of time-sensitive information on developments that could involve a threat to the enterprise system. I&W service provides the Enterprise a warning that something *may be about to* happen; AS&W provides the Enterprise a warning that an attack *is* happening. In the context of Event Management and Incident Management, these services are drivers to prioritizing network operations monitoring activities, and may change EM and IM response workflows and escalation criteria. For instance, an indication of a particular form of potential malicious activity may cause Service Desk personnel to immediately escalate particular calls directly to cyberspace defense elements, rather than following a more deliberate assistance script, as would normally be the case.

No.	*Scale*	*Measure*
01	Percent	Unit has ability to implement near real-time detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities, and distinguish these incidents/events from benign activities across 95% of the enterprise
02	Yes/No	Unit identifies network mapping and operating system fingerprinting activities
03	Time	Required to receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
04	Yes/No	Unit validates Intrusion Detection System (IDS) alerts against network traffic using packet analysis tools
05	Yes/No	Unit conducts or coordinate cordon and search activities against advanced persistent threats that evade routine security measures
06	Yes/No	Unit determines tactics, techniques, and procedures (TTPs) for intrusion sets
07	Yes/No	Units supports DCO forces that operate in an area of operation

(U) Conduct Cyber Incident Handling

(U) Incident Handling protects, monitors, analyzes, and detects unauthorized or anomalous activity on the Army networks. Information such as classified data spills, unauthorized access, and outages are collected and distributed through an enterprise ticketing system. In many ways, incident handling is accomplished using the same incident and problem management processes as the rest of network operations, but cyber incidents require a separate sub-process since these tend to occur as a result of malicious activities intended to disrupt or degrade services, rather than as a result of human error or material failures, have different reporting criteria and may or may not adversely affect one or more services.

No.	*Scale*	*Measure*
01	Yes/No	Unit provides daily summary reports of network events and activity relevant to cybersecurity practices
02	Yes/No	Unit implements appropriate command and control procedures in response to incident
03	Yes/No	Unit tracks and documents incidents from initial detection through final resolution
04	Yes/No	Unit provides technical support to DCO forces to validate and resolve incidents
05	Yes/No	Unit performs analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and Intrusion Detection System [IDS] logs
06	Time	Required for unit to perform incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation
07	Yes/No	Unit characterizes and analyzes network traffic to identify anomalous activity and potential threats to network resources

08	Yes/No	Unit correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
09	Yes/No	Unit analyzes cyberspace events from various sources within the enterprise and determine possible causes of such events (to include weaknesses exploited, exploitation methods, and effects on system and information).
10	Yes/No	Unit develops appropriate payloads to be delivered through associated cybersecurity/DCO tools
11	Yes/No	Unit performs incident trend analysis and reporting
12	Yes/No	Unit documents and escalates incidents that attain specified criteria to echelons required to meet authority requirements
13	Yes/No	Unit writes and publishes guidance and reports on incident findings to appropriate constituencies (provide threat based informational briefs and bulletins to supported commands)
14	Yes/No	Unit administers test bed(s), and test and evaluate new cybersecurity/DCO applications, rules/signatures, access control list, and configurations of service provider managed platforms
15	Yes/No	Unit coordinates with cyberspace defenders to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, anti-virus, and content blacklists) for specialized applications
16	Yes/No	Unit provides initial, interim, and final technical reports into Army Cyber Incident Database (ACID) based on findings from forensics and incident analysis

(U) Continuously Monitor Networks/Systems

(U) Continuous monitoring is the ongoing observation and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations. Continuous monitoring also maintains the ongoing awareness of information security, vulnerabilities, and threats to support organizational and operational risk management decisions. This includes the ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, cyber hygiene, and operational readiness. The output of continuous monitoring supports the development of cyberspace situational understanding, which is an end-to-end comprehension of what is occurring in cyberspace to facilitate the planning, preparation, execution, and assessment of operations. The objective is to know and observe all entities (red/blue/white/grey users and non-person entities) operating on Army networks. Cybersecurity requires an operational view of the enterprise environment to provide an understanding of threats, vulnerabilities, attacks, networks, systems, services, applications, and other data to influence and support command decision-making.

No.	***Scale***	***Measure***
01	Yes/No	Unit monitors and provides awareness of network topologies to understand data flows through the network
02	Yes/No	Unit collects and provides network utilization and status data
03	Yes/No	Unit provides network performance reporting, trending, and management capabilities (to include information on network devices, sensors, links, and services outages)
04	Yes/No	Unit monitors internal/external data sources to provide awareness of evolving network threats and trends
05	Yes/No	Unit researches, analyzes, and creates products/reports from multiple intelligence and operational sources to provide awareness of critical assets
06	Yes/No	Unit shapes, advises, tracks, and reports Commanders Critical Information Requirements (CCIRs)
07	Yes/No	Unit identifies and provide awareness of facility, telecommunications, and information system problems (to include failures and Hazardous Conditions (HAZCONS))
08	Yes/No	Unit provide awareness of cyber events and incidents in accordance with applicable DOD/CYBERCOM/ARMY policies, orders, and timelines

09	Yes/No	Unit provides awareness of vulnerabilities identified through the penetration testing and the solutions implemented to address the root cause of the identified exposures
10	Yes/No	Unit maintains an on-line portal for user monitoring of cyber incidents in near-real-time
11	Yes/No	Unit provides amplified awareness (amplified incidents reports (AIR)) for major incidents or group of related incidents
12	Yes/No	Unit maintains and updates tools to conduct continual monitoring and analysis of network/system activities

3. (U) Global Cyberspace Defense Tasks

(U) Globally, cyberspace defenders focus on MRT-C by operating as a maneuver defense force that offers commanders quick reaction, cyberspace defense reinforcement, and security enhancement capabilities. Globally arrayed cyberspace defenders focus on four major lines of operations: Defend the Nation, Protect the DODIN, Combatant Command Support, and Service Support, with emphasis on performing DCO-IDM. This force possesses a unique skill set that differs from local or regional cyberspace defenders and it enables global cyberspace defenders to perform specialized missions. The following tasks are mapped to ART 5.9.1.2 (Conduct Defensive Cyberspace Operations) and 5.10.2.3 (Conduct Cybersecurity).

(U) Plan for the Cyberspace Defense

((U//FOUO) Planning is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. Planning results in a plan and orders that synchronize the action of cyberspace defenders in time, space, and purpose to achieve objectives and accomplish missions. Planning for the cyberspace defense parallels an organization's overall operations planning cycle and incorporates the use of the Military Decision Making Process (MDMP):

1. (U) Receipt of Mission. This task covers how cyberspace defenders are given a mission by higher headquarters or deduce a need for a change in the current mission. This task involves preparing for mission analysis, to include collecting materials for analysis, receiving the commander's preliminary guidance, determining requirements and time available, and sending warning orders to subordinates.

No.	*Scale*	*Measure*
01	Yes/No	Cyberspace defenders collected materials for analysis.
02	Yes/No	Commander provided adequate initial guidance.
03	Time	After receipt of mission to issue initial planning guidance.
04	Time	To alert cyberspace defenders of receipt of new mission.
05	Time	To issue warning order

2. (U) Mission Analysis: Cyberspace defenders analyze the received mission to define the problem and begin to determine solutions through the identification of specified and implied tasks. A key output of mission analysis is the identification of KT-C and MRT-C. This tasks results in a restated mission, the commander's guidance, commander's intent, initial commander's critical information requirements, planned use of available time, and a warning order.

No.	*Scale*	*Measure*
01	Yes/No	Unit developed mission analysis briefing for presentation to the commander.
02	Yes/No	Unit developed and approved restated mission, commander's guidance, commander's intent, commander's critical information requirements, use of available time, and warning order.
03	Yes/No	Unit developed reconnaissance and surveillance plan, initial themes and messages, a proposed problem statement, and the course of action evaluation criteria.
04	Yes/No	Mission statement included who, what, when, where, and why of the mission.
05	Yes/No	Unit performed time or distance analysis.
06	Yes/No	Unit developed assumptions to replace missing or unknown facts necessary for continued planning.
07	Yes/No	Commander issued planning guidance to staff and subordinate commands.
08	Yes/No	Staffs developed and maintained running estimate pertaining to their areas of expertise.
09	Yes/No	Unit issued a warning order.
10	Yes/No	Unit provided input to the assessment of relative unit readiness.
11	Yes/No	Unit identified vulnerabilities of friendly actors.
12	Percent	Of critical information and running estimates reviewed before mission analysis.
13	Percent	Of major topics within the intelligence preparation of the battlefield for which assessments were completed.
14	Yes/No	Unit provided input to the development of options for decisive, shaping, and sustaining operations.
15	Yes/No	Unit provided input to the development of military deception courses of action
16	Yes/No	Unit developed initial scheme of DCO for each course of action
17	Yes/No	Unit developed statements and sketches for each course of action
18	Yes/No	Unit analyzed KT-C and critical assets and develop list of tentative defended assets
19	Yes/No	Unit developed primary, alternate, contingency, and emergency communications plan for each course of action.
20	Yes/No	Unit developed input for the operations execution matrix.
21	Percent	Unit provided input and participated in the course of action development brief as required.

3. (U) Develop Courses of Action: Cyberspace defenders develop a course of action (COA) for analysis, evaluation, and selection as the one to accomplish the mission most effectively. This task includes analyzing relative cyberspace power, generating options, arraying initial forces, developing schemes of maneuver, assigning headquarters, and preparing COA statements and sketches. The commander has the option of directing a specific COA because of time available, staff proficiency, or other reasons.

No.	*Scale*	*Measure*
01	Yes/No	Unit developed distinguishable and complete COAs in terms of feasibility, suitability, and acceptability for mission accomplishment if executed.
02	Time	To provide the commander or leader with suitable, feasible, and acceptable COAs after receipt of operation order or warning order.
03	Yes/No	Unit established triggers based on limits or thresholds to countermeasure performance or effectiveness.
03	Time	To prepare complete COA statements and sketches.
04	Number	Of COAs that were completed.
05	Yes/No	COAs suitable to solving the problem (legally and ethically).

06	Yes/No	COAs fit within available resources.
07	Number	Of COAs presented to commander that were suitable, feasible, acceptable, and distinct from one another.

4. (U) Analyze Courses of Action: Cyberspace defenders develop criteria for success and examine each course of action (COA) for its advantages and disadvantages with respect to those criteria. This task normally includes the technique of wargaming. Cyberspace defenders visualize each COA objectively; focus intelligence preparation of the battlefield requirements; identify coordination requirements; anticipate critical operational events; determine conditions and resources required for success; and assess suitability, feasibility, acceptability, and operational risk of the COA.

No.	*Scale*	*Measure*
01	Yes/No	Unit identified advantages and disadvantages of COAs, measures of effectiveness, or measures of performance for evaluation.
02	Yes/No	Unit reviewed and revised commander's critical information requirements, as necessary, during the wargaming process.
03	Yes/No	Unit developed risk management plan for COA analysis.
04	Yes/No	Unit applied evaluation criteria (measures of effectiveness or measures of performance) to the wargaming analysis.
05	Yes/No	Methods applied during wargaming analysis included belt, box, or avenue-in-depth.
06	Yes/No	Unit used synchronization matrix or sketch note worksheet during wargaming analysis.
07	Time	To complete COA analysis.
08	Percent	Of completeness of COAs.
09	Percent	Of conformance of analysis to doctrine.
10	Percent	Of branches and sequels experienced identified in COAs.
11	Percent	Of capabilities ultimately required identified in COA analysis.
12	Percent	Of COAs analyzed against potential enemy COAs.
13	Number	Of limitations (ultimately identified during execution) identified during analysis.
14	Number	Of criteria of comparison and success identified during COA analysis.
15	Number	Of decision points and critical events identified and applied to commander's critical information requirements during war gaming.

5. (U) Compare Courses of Action: This task covers how cyberspace defenders evaluate courses of action (COAs) independently, against a set evaluation criteria, and against each other to determine the most ethical and effective one for mission accomplishment. Cyberspace defenders recommend for selection. This comparison also considers risk, positioning for future operations, flexibility, and subordinate exercise of initiative.

No.	*Scale*	*Measure*
01	Yes/No	Previously selected comparison criteria allowed for definitive comparison of COAs.
02	Yes/No	Unit developed risk management plan used during COA comparison.
03	Percent	Of comparison criteria eliminated before comparison.
04	Percent	Of comparison criteria eventually used, defined, and weighted before comparison began.

6. (U) Approve Course of Action: This task covers how commanders or other leaders decide and approve a course of action (COA) that is most advantageous to mission accomplishment and

is within the stated intent. Cyberspace defenders refine a commander's or other leader's intent and CCIRs to support selected COAs.

No.	*Scale*	*Measure*
01	Yes/No	COA brief was developed and presented to commander.
02	Yes/No	Commander evaluated COAs, selected a COA, and modified or rejected all presented COAs.
03	Yes/No	Modified COA or new COA created a new war game to consider products derived from that COA.
04	Yes/No	Revised commander's intent adequately addressed key tasks for force as whole, wider purpose; it was expressed in four to five sentences or bullets.
05	Yes/No	Commander decided level of risk to accomplish the mission and approved control measures.
06	Time	To issue warning orders.

6. (U) Produce Plan or Order: This task covers how cyberspace defenders prepare a plan or order to implement the selected course of action per the commander's decision by turning it into a clear, concise concept of operations and required support. The plan includes annexes and overlays as necessary to implement the plan. The plan or order accurately conveys information that governs actions to be taken and is completed in the correct format. This includes the establishment of graphic control measures, including fire support coordination measures.

No.	*Scale*	*Measure*
01	Yes/No	Orders or plans accomplished the mission and commander's intent. They were communicated effectively and completed with sufficient time for the force to complete required preparatory actions before execution.
02	Yes/No	Commander's intent refined and adequately addressed key tasks for the force as a whole, wider purpose; it was expressed in four to five sentences.
03	Time	To issue warning orders as required.
04	Time	Before execution to reissue commander's intent and concept of operations.
05	Time	To prepare plans and orders (after deciding on mission concept and commander's intent).
06	Time	To obtain approval of plans and orders.
07	Time	To issue plan or order (after approved).
08	Percent	Of functional responsibilities covered in operation plan.
09	Percent	Of accurate information in plans and orders issued and disseminated to subordinate units.
10	Percent	Of accurate information in operation order or plan to meet established objectives.
11	Number	Of instances where the operation plan or order conflicted with standards established under the law of war and international conventions.

(U) Protect Mission Relevant Terrain in Cyberspace (MRT-C)

(U//FOUO) Protection should preserve at least 95% of MRT-C so those capabilities can be utilized at the desired time and place. Protection of MRT-C includes the following measures:

1. Provide Cybersecurity Services. Cyberspace defenders ensure the delivery of services that offer early and accurate warning of enemy activities, provide the force protecting the cyberspace capabilities with time and maneuver space within which to react to the enemy, and develop the

situation that allows for the effective use of the critical assets. The ultimate goal of cybersecurity services is to protect a unit from surprise and reduce the unknowns in any situation.

2. Guard Protected Network. Cyberspace defenders protect the main body (in this case – MRT-C), through mission assurance actions, by fighting the enemy on the network to gain time while also observing and reporting information and preventing enemy reconnaissance and offensive actions. Units conducting a guard mission CANNOT operate independently because they rely on those implementing DODIN operations (to include cybersecurity) and DCO-IDM directly within the AO.

(U//FOUO) Based on the above tasks, the following measures will be collected.

No.	*Scale*	*Measure*
01	Yes/No	Unit ensures the delivery of cybersecurity services from appropriate organization
02	Yes/No	Unit applies hardening techniques to MRT-C
03	Yes/No	Unit observes enemy cyberspace activity and reports information to the appropriate staff and higher
04	Yes/No	Unit prevents further enemy reconnaissance or offensive cyberspace actions
05	Yes/No	Unit does not operate independently from supported organizations implementing DODIN operations
06	Percent	Unit preserves 95% of MRT-C

(U) Conduct Cordon and Search Activities in Friendly Cyberspace

(U//FOUO) Cordon and search activities are a form of counter-reconnaissance (search and discover) meant to seek out adversaries conducting reconnaissance or offensive operations within AO. To facilitate these activities, cyberspace defenders must accurately understand the enemy's capabilities and TTPs. This involves understanding how the enemy will evolve in reaction to friendly countermeasures. The following performance measures will be executed as part of this task:

1. Request Indications and Warnings (I&W). Cyberspace defenders receive I&Ws meant to sense changes in adversary activities. I&Ws include those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to operations.

2. Sense Cyber Attacks and Warnings (AS&W). Cyberspace defenders sense changes or anomalies in the network, including intrusions and attacks, in near-real time (< 10 mins). It couples this with the notification to cyberspace defenders so they can develop an appropriate response. AS&W is enabled through a system of integrated sensors and discovery TTPs, all supported by data fusion and analysis, diagnostics, long-term trend and pattern analysis, and warning communications channels and procedures.

3. Discover Indicators of Compromise. Cyberspace defenders search for and discover indicators of compromise consisting of artifacts or behaviors that reside in memory, storage, or network traffic that may seem benign at the surface, yet, they fall outside the baseline of network behavior in reference to purpose or time. The goal is to search for and discover 95% of previously unknown threats and characterize them in order for them to be mitigated or defeated.

Cordon and search activities the mission assurance gap created when other efforts to harden and defend have failed to keep adversaries out. Although the purpose of detection is to establish a persistent presence on the network, searching adds the aspect of agile mobility.

No.	*Scale*	*Measure*
01	Time	Unit receives time-sensitive intelligence that provides indications and warnings
02	Time	Unit is provided early and accurate warning of enemy activities that allows for maneuver space in which to react
03	Time	Required for unit to sense changes or anomalies in the network
04	Yes/No	Unit notifies supported organization
05	Yes/No	Unit discovers indicators of compromise in MRT-C
06	Percent	Unit characterizes 95% of previously unknown threats

(U) Mitigate a Cyber Attack

(U//FOUO) The primary objective of mitigation is to impact the enemy's mobility during an attack by disrupting the enemy in order to cause them to center their activity on a given front and prevent them from withdrawing any part of their forces for use elsewhere. The following performance measures will be executed as part of this task:

1. Employ Disruptive Cyberspace Actions. Cyberspace defenders employ disruptive actions (within one (1) hour) to unhinge the enemy's preparations and attacks. Disruption methods use obstacles to reinforce KT-C and MRT-C that result in the interdiction, isolation, blocking, and neutralization of cyberspace threats and vulnerabilities. Interdiction is a task where a force delays the enemy's use of an area or route. Isolation requires cyberspace defenders to seal off (both virtually and psychologically) an enemy from sources of support; and blocking uses obstacles to deny the enemy access to an area and prevents its advance in a direction or attack vector. Finally, neutralization renders an enemy's cyberspace reconnaissance or offensive cyberspace capabilities ineffective or unusable.

2. Conduct Incident Analysis. Cyberspace defenders perform an incident analysis. Incident analysis validates an incident type. The purpose of this analysis is to understand the technical details, root cause(s), and potential impact. Moreover, incident analysis strives to identify relationships and trends between incidents in the short term and patterns across incidents in the long term. This understanding will help to determine what additional information to gather, coordinate information sharing with others, and develop a course of action for response. This activity relies on effective acquisition, preservation, and timely reporting of incident data. Ultimately, incident analysis results in the coordinated development and implementation of courses of action (COA) that focus on clearing and reconstitution.

3. Report an Incident. Cyberspace defenders report incidents using a well-defined framework for the timely accounting of any event or incident. The report provides an accurate, meaningful, and complete understanding of the incident from initial detection to analysis and mitigation. This information feeds into a system, which provides a network damage assessment.

No.	*Scale*	*Measure*
01	Time	Required for unit to employ disruptive actions to unhinge the enemy's preparations and attacks
02	Time	Required for unit to interdict, isolate, block, or neutralize cyberspace threats and/or vulnerabilities
03	Yes/No	Unit understands the technical details, root cause(s), and potential impact
04	Yes/No	Unit identifies relationships and trends between incidents in the short term and patterns across incidents in the long term
05	Yes/No	Unit determines what additional information to gather, coordinates information sharing with others, and develops a course of action for response
06	Time	Unit reports a timely accounting of an event or incident to appropriate staff and higher

(U) Engage a Cyberspace threat

(U//FOUO) Engagement is meant to maneuver against and initiate a tactical conflict with an enemy conducting operations on KT-C and/or MRT-C. Maneuver enables cyberspace defenders to skillfully move to a designated area in order to destroy the enemy and recover from an attack with massed effects of all necessary cyberspace defense capabilities and supporting systems. The following performance measures will be executed as part of this task:

1. Designate Engagement Areas. Cyberspace defenders establish an engagement area to counter the threat. Engagement areas are designated based on attack vectors and consist of a size and shape to best array forces in order to observe and clear (destroy) 95% of validated adversary cyberspace activities. It is critical that engagement not affect friendly use of cyberspace to conduct net-enabled operations.

2. Conduct an Area Cyberspace Defense. Cyberspace defenders will establish and area defense. In an area defense, cyberspace defenders concentrate on denying enemy forces access to designated terrain in cyberspace for a specific time rather than destroying the enemy outright. The focus of the area defense is on retaining KT-C and/or MRT-C where the bulk of the defending force positions itself in mutually supporting, prepared positions. Cyberspace defenders maintain their positions and control the terrain between these positions. The decisive operation channels actions into engagement areas (e.g. honey pots), possibly supplemented by a counterattack. A reserve may or may not take part in the decisive operation. A reserve can be used to add depth, block, or reconstitute cyberspace resources.

3. Conduct a Mobile Cyberspace Defense. When directed, cyberspace defenders conduct a mobile cyberspace defense. In a mobile defense, cyberspace defenders set the conditions for the destruction or defeat of the enemy's offensive operations within four (4) hours through decisive actions. The mobile defense focuses on facilitating the defeat or destruction of the enemy capabilities by allowing it to advance to a point where they are exposed. A mobile defense requires a virtual area of operations with considerable depth. Cyberspace defenders must be able to shape the MRT-C, causing an enemy force to overextend its operations and dissipate its abilities.

No.	*Scale*	*Measure*
01	Yes/No	Unit remotely/physically maneuvers to MRT-C to engage cyberspace threat
02	Yes/No	Unit establishes virtual engagement area(s)
03	Yes/No	Unit establishes an area defense around MRT-C
04	Yes/No	Unit designates a reserve to add depth, block, or reconstitute cyberspace resources
05	Time	Unit conducts mobile cyberspace defense actions when directed
06	Time	Unit reports a timely accounting of an event or incident to appropriate staff and higher

(U) Conduct Clearing Activities on a Compromised Network

(U//FOUO) Clearing is meant to establish normal operation levels across the network and involves activities that eradicate the threat and remove the cause of the incident from the network and/or information systems enabled by vulnerabilities across organizational people, processes, and technologies. The following performance measures will be executed as part of this task:

1. Conduct Mission Assurance Actions. Cyberspace defenders conduct mission assurance actions in reaction to an incident. Mission assurance actions dynamically reestablish, re-secure, re-route, reconstruct, or isolate MRT-C and data within near-real time (< 10 mins). Reconstitution begins recovery process by utilizing organized movement of cyberspace resources or information flow away from the enemy. Reconstitute operations attempt to gain time, preserve cyberspace resources, place the enemy in unfavorable positions, and/or avoid operations under undesirable conditions.

2. Remove Remnants of Cyberspace Attack. Cyberspace defenders remove all remnants of a cyberspace attack from impacted systems or networks. The “clear” function is meant to destroy the enemy. Clearing a virtual area normally requires assistance and integration between supporting cyberspace defenders and the main body (organic cyberspace defenders assigned to supported units). This allows the main body to operate unimpeded, prevents the unnecessary delay in the main body’s OPTEMPO, and defers response actions from the main body for as long as possible.

3. Prevent Similar Cyberspace Attacks. Cyberspace defenders improve operational, management, and technical controls by implementing approved recovery actions and conducting an after action review of the incident. The process establishes follow-up strategies that prevent 95% of similar incidents from reoccurring. Strategies can include notifications of mandated baseline, or minimum configuration of all hosts residing on the network.

4. Conduct a Post-Incident Analysis. Cyberspace defenders conduct a postmortem on an incident to review the effectiveness and efficiency of cyberspace defense actions. Post-incident analysis results in an update to the network readiness level, which in comparison to the previous defensive posture, lowers the risk of impact to operations through the intentional disruption of friendly information systems.

No.	*Scale*	*Measure*
01	Time	Unit dynamically reestablishes, re-secures, re-routes, reconstructs, or isolates MRT-C and data
02	Yes/No	Unit performs an organized movement of cyberspace resources or information flow away from the enemy activities
03	Yes/No	Unit removes all remnants of a cyberspace attack from impacted systems or networks
04	Percent	Unit improves operational, management, and technical controls by implementing approved recovery actions that prevents 95% of similar incidents from reoccurring
05	Time	Unit conducts a post-incident analysis to review the effectiveness and efficiency of cyberspace defense actions
06	Time	Unit updates the network readiness level

Annex E: (U) Glossary

(U) Acronyms and Abbreviations

AA	assembly area
ACAS	Assured Compliance Assessment Solution
ACE	Army Corps of Engineer
ACOIC	Army Cyber Operations and Integration Center
ACP	access control point
ADCON	administration control
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AFRICOM	U.S. Africa Command
AO	area of operation
AOC	Army Operational Concept
AOR	area of responsibility
APT	advanced persistent threat
AR	Army Regulation
ARL	Army Research Lab
ART	Army task
ARCYBER	Army Cyber Command
ASCC	Army Service Component Command
AS&W	attack sensing and warning
AWFC	Army Warfighting Challenge
BCT	brigade combat team
B/P/C/S	bases/posts/camps/stations/tactical
BVAT	Blue Vulnerability Assessment Team
C2	command and control
CAL	critical asset list
CCIR	commander's critical information requirement
CCMD	combatant command
CCOE	U.S. Army Cyber Center of Excellence
CCRI	Command Cyber Readiness Inspection
CDR	commander
CEM	cyber electromagnetic
CEMA	cyber electromagnetic activities
CENTCOM	U.S. Central Command
CG	commanding general
CI	counter-intelligence
CIO	Chief Information Officer
CJCSM	Chairman Joint Chiefs of Staff Manual
CMF	Cyber Mission Forces
CND	computer network defense
CNDSP	computer network defense service provider
CNMF	cyber national mission forces
COA	course of action
CONOPS	concept of operations

CONUS	Continental United States
CPB	Cyber Protection Brigade
CPT	Cyber Protection Team
CSSP	Cybersecurity Service Provider
CUOPS	current operations
DAL	defended asset list
DDS	Deployable DCO System
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations-internal defensive measures
DCO-MC	DCO-maneuver capabilities
DCOMP	defensive cyberspace operations mission planning
DCO-RA	defensive cyberspace operations-response actions
DHS	Department of Homeland Security
DISA	Defense Information Services Agency
DOD	Department of Defense
DODIN	Department of Defense information networks
DOTMLPF - P	doctrine, organizational, training, materiel, leadership and education, personnel, facilities and policy
DREN	Defense Research and Engineering Network
DRU	direct reporting unit
EA	engagement area
EEA	essential elements of analysis
EEFI	essential elements of friendly information
EM	electromagnetic
EMS	electromagnetic spectrum
EP	electronic protect
EW	electronic warfare
FBI	Federal Bureau of Investigations
FM	field manual
F&MA	forensics and malware analysis
FORSCOM	U.S. Army Forces Command
FOUO	for official use only
FRAGO	fragmentation order
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
GCC	geographical combatant command
GDP	Garrison DCO Platform
HBSS	host based security system
HQDA	Headquarters Department of the Army
IA/CND	information assurance/computer network defense
IAW	in accordance with
IaaDS	installation as a docking station
ICAN	installation campus area network
ICS	industrial control system
IDS	intrusion detection system

IO	information operations
IP	internet protocol
IPB	intelligence preparation of the battlefield
IR	intelligence requirement
IRC	information related capability
ISR	intelligence, surveillance, and reconnaissance
I&W	indications and warnings
JFHQ-C	Joint Forces Headquarter-Cyber
JIE	joint information environment
JOA	joint operational area
JOC	Joint Operations Center
JP	Joint Publication
JRSS	joint regional security stack
JWICS	Joint Worldwide Intelligence Communications System
KT-C	key terrain in cyberspace
LD	learning demand
LE	law enforcement
LZ	landing zone
MBA	main battle area
MD5	Merkle-Damgard5
MDMP	military decision making process
METL	mission essential task list
METT-C	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MFSB	multi-function support brigade
MISO	military information support operations
MPLS	multi-protocol label switching
MRT-C	mission relevant terrain in cyberspace
NAI	named area of interest
NEC	Network Enterprise Center
NETCOM	U.S. Army Network Enterprise Technology Command
NIPRNET	Non-Secure Internet Protocol Network
NORTHCOM	U.S. Northern Command
OAKOC	observation, avenues of approach, key terrain, obstacles, and cover and concealment
OBJ	objective
OCO	offensive cyberspace operations
OC-T	observer, controller, trainer
OE	operational environment
OP	observation post
OPCON	operational control
OPE	operational preparation of the environment
OPFOR	opposing force
OPLAN	operations plan
OPORD	operations order
OS	operating system

OSINT	open source intelligence
PA	Public Affairs
PIR	priority intelligence requirements
PKI	Public Key Infrastructure
PNT	Positioning, Navigation and Timing
RCC	Regional Cyber Center
ROE	rules of engagement
RSOI	reception, staging, onward movement, and integration
RVAT	Red Vulnerability Assessment Team
S-2	intelligence staff officer
S-3	operations staff officer
S-6	signal staff officer
SA	Situational Awareness
SATCOM	satellite communications
SCADA	supervisory control and data acquisition
SCAP	security content automation protocol
SIEM	security information event and management
SIPRNET	SECRET Internet Protocol Router Network
SME	subject matter expert
SOF	Special Operating Forces
SOP	standard operating procedures
S&R	surveillance and reconnaissance
STIG	Standard Technical Implementation Guide
STO	special technical operations
TAC	Tactical Action Center
TAI	target area of interest
TDI	Tactical DCO Infrastructure
TOC	Tactical Operations Center
TP	Training and Doctrine Command Pamphlet
TRADOC	Training and Doctrine Command
TRA	tailored response action
TTP	tactics, techniques, and procedures
UAM	user activity monitoring
UAP	Unified Actions partners
ULO	unified land operations
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
U.S.	United States
USC	United States Code
VM	Virtual Machine
WIN-T	Warfighter Information Network-Tactical

(U) Terms

advanced persistent threat
An offensive cyberspace operation in which an unauthorized entity gains access to a network and stays there undetected for a long period of time.

area defense (cyberspace defense)
A type of defensive operation that concentrates on denying enemy forces access to designated key terrain in cyberspace and/or defended assets for a specific time rather than destroying enemy cyberspace capabilities outright.

battle handover (cyberspace defense)
A designated phase line in friendly cyberspace where responsibility transitions from the supported unit force to the supporting unit and vice versa.

battle position (cyberspace defense)
A defensive location oriented on likely adversary avenues of approach (both physical and logical).

clear (cyberspace defense)
An enabling task that requires cyberspace defenders to remove all remnants of enemy forces within an area of operation by eliminating all indicators of compromise

commander's critical information requirement
An information requirement identified by the commander as being critical to facilitating timely decision making. (JP 3-0)

common operational picture
(Army) A single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command. (ADRP 6-0)

concept of operations
A statement, in broad outline, of a commander’s assumptions or intent about an operation or series of operations. It is designed to give an overall picture and a useful visualization of how a future operation would be conducted. (TR 71-20)

cordon and search (cyberspace defense)
A technique of conducting a movement to contact that involves isolating a named area of interest and searching suspected virtual locations within that area to discover indicators of compromise.

counter-mobility (cyberspace defense)
A DCO action that impacts the enemy’s mobility during a cyberspace attack by blocking, containing, or isolating the enemy in order to cause them to center their activity on a given front and prevent them from withdrawing any part of their forces for use elsewhere. Counter-mobility

includes the construction of obstacles and emplacement of countermeasures to delay, disrupt, and destroy the enemy by reinforcement of the terrain.

cover and concealment (cyberspace defense)
A form of security operations in which the primary task is to protect the main body (in this case – MRT-C), through mission assurance actions, by fighting the enemy on the network to gain time while also observing and reporting information and preventing enemy reconnaissance and offensive actions.

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

cybersecurity
The 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. Incorporates the actions found in legacy Information Assurance and Computer Network Defense tasks. To be used throughout DOD instead of the term "information assurance (IA)." (DOD instruction 8500.01)

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 1-02)

cyber analytics (data research, trending)
A branch of analytics that applies to the domain of computers, networks, and related data. Analysis of voluminous network data, cyber analytics tells the story behind cyber data. Cyber analytics can be used to support computer security, computer or network administration, auditing, and many other application areas.

cyberspace attack
Actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. (JP 3-12)

cyberspace operations
The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 1-02)

cyberspace situational understanding

The requisite current and predictive knowledge of cyberspace and the OE upon which CO depend, including all factors affecting friendly and adversary cyberspace forces. (U.S. Army Cyberspace Situational Awareness Concept of Operation)

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 by an adversary. (JP 3-12)

cyberspace threat
Any circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a system resulting in a loss of confidentiality, integrity, or availability.

defense (cyberspace)
A task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions to retain decisive terrain in cyberspace or deny a vital area in cyberspace to the enemy.

defensive cyberspace operations
Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 1-02)

defensive cyberspace operations-internal defensive measures
DCO that are conducted within the DODIN. They include actively hunting for advanced internal threats as well as the internal responses to these threats. Internal defensive measures respond to unauthorized activity or alerts/threat information within the DODIN, and leverage intelligence, CI, LE, and other military capabilities as required. (JP 3-12)

defensive cyberspace operations - response actions
The deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. A designated Cyber National Mission Force (CNMF) mission, DCO-RA must be authorized IAW the standing ROE and any applicable supplemental ROE and may rise to the level of use of force. (JP 1-02)

defense-in-depth (cyberspace defense)
The siting of mutually supporting defense positions in friendly cyberspace designed to absorb and progressively weaken cyberspace attacks, prevent initial enemy cyberspace surveillance and reconnaissance, and allow defenders to employ additional cyberspace capabilities where needed.

Department of Defense information networks
The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. (JP 1-02)

Department of Defense information network operations
Operations to design, build, configure, secure, operate, maintain, and sustain DOD networks to create and preserve cybersecurity on the DODIN. (JP 1-02)

destroy (cyberspace defense)
An effect that permanently, completely, and irreparably denies the enemy access to a targeted system and prevents the enemy from generating effects within a friendly area of operations.

electromagnetic spectrum
The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into alphabetically designated bands. (JP 3-13.1)

electromagnetic spectrum management
Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. (JP 6-01)

electronic attack
Division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation 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 3-13.1)

engagement area (cyberspace defense)
A decisive point in which cyberspace defenders contain and destroy an enemy force with the massed effects of all available capabilities.

essential element of friendly information
(Army) A critical Operations Security (OPSEC) aspect of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. (ADRP 5-0)

guard (cyberspace defense)
A form of security operations whose primary task is to protect the main body (in this case – MRT-C), through mission assurance actions, by fighting the enemy on the network to gain time while also observing and reporting information and preventing enemy reconnaissance and offensive actions.

information assurance
Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. Also called IA. (Legacy term as directed by DoDI 8500.01)

information environment
The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information-related capabilities

Capabilities, techniques, or activities employing information to effect any of the three dimensions within the information environment to generate an end(s). (FM 3-13)

information condition (INFOCON)
A comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system also provides a framework and method used by the military to defend against or mitigate a computer network attack.

infrastructure
The collection of hardware and software/firmware that enables the instantiation and/or execution of software platforms.

integration
The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 1-02)

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. (JP 3-13)

joint information environment
A secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs). (JIE CONOPS)

kill chain (cyberspace defense)
An intelligence driven defense model for the prevention of cyberspace incidents that identifies what enemies must complete in order to achieve their objectives in friendly cyberspace and determines appropriate countermeasures to halt enemy progress at any stage of a cyberspace attack.

landing zone (cyberspace defense)
A virtual area in friendly cyberspace that is part of an operational area in which augmentation forces access the defended network from reach-back to establish a presence and emplace capabilities for follow-on actions.

line of departure (cyberspace defense)
A phase line crossed at a prescribed time by forces initiating an operation.

local security (cyberspace defense)
A security task that includes low-level security activities conducted on cyberspace assets to prevent surprise by the enemy.

main battle area (cyberspace defense)
The area where a unit deploys the bulk of its cyberspace power and conducts decisive operations to defeat an attacking enemy.

mobile defense (cyberspace defense)
Defense of an area or position in which maneuver is used leveraging key elements of the terrain in cyberspace to seize the initiative from the enemy and defeat the enemy through decisive actions.

named area of interest (cyberspace defense)
A virtual area where information that will satisfy a specific information requirement can be collected.

obstacles (cyberspace defense)
Any physical, logical, or persona obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in time and capability on the opposing force.

offensive cyberspace operations
Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 1-02)

operational environment
A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

platform
Capability provided to the operator to deploy onto the infrastructure the necessary tools and payloads.

planning
The art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. (ADP 5-0)

protection (cyberspace defense)
Preservation of the effectiveness and survivability of mission-related cyberspace capabilities deployed or located within or outside the boundaries of an assigned terrain in cyberspace.

reconnaissance (cyberspace defense)
A DCO action undertaken to obtain, by observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the characteristics of a particular area. Also called RECON. RECON types include area, pull, push, route, special, and zone. (JP 2-0)

retrograde (cyberspace defense)

A type of defensive operation that involves organized movement of net-enabled capabilities away from the enemy.

risk management
The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. (JP 3-0)

screen (cyberspace defense)
A security task that primarily provides early warning for the protected assets.

secure (cyberspace defense)
Operations undertaken to provide early and accurate warning of enemy operations, to provide the force protecting the cyberspace capabilities with time and maneuver space within which to react to the enemy, and to develop the situation to allow the effective use of the protected assets.

security area (cyberspace defense)
A virtual area used to confuse the enemy about the location of the commander's main battle positions, prevent enemy observation of preparations and positions, and keep the enemy from delivering effects on mission relevant terrain.

situational understanding
The product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables to facilitate decision-making. (ADP 5-0)

tool
Software that supports or directly causes effects related to cyberspace mission force and workforce tasks.

unified land operations
The army operating concept. How the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations.

working group
(Army) A grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function. (FM 6-0)

Annex F: (U) Intelligence Preparation of the Battlefield Processes with Cyberspace Defense Outputs

(U) Intelligence supports the cyberspace defensive tasks with IPB products to identify probable threat objectives and various approaches; patterns of threat operations; the threat's vulnerability to counterattack, interdiction, electronic warfare, and canalization by virtual obstacles; and the threat's capability to cyberspace attacks against friendly forces, insert capabilities into MRT-C and KT-C, and employ exploits and payloads. Intelligence support personnel also evaluate how soon the threat can employ offensive capabilities.

(U) Commanders choose to defend to create conditions for mission assurance that allows the Army to regain the initiative. Other reasons for conducting a defense include to retain decisive terrain or deny a vital area to the enemy, to attrit or fix the enemy, or to increase the enemy's vulnerability by forcing the enemy to concentrate forces. Intelligence support personnel support the commander's use of information collection assets to visualize the terrain, determine threat strengths and dispositions, and confirm or deny threat COAs. Defending commanders can then decide where to arrange their asset in an economy-of-force role to defend and shape the virtual battlefield.

(U) Intelligence support personnel lead the IPB process. Cyberspace defenders and other personnel assist in developing the IPB products required for planning. IPB starts immediately upon receipt of the mission, is refined throughout planning, and continues during preparation and execution based on the continuous assessment of operations. The following aspects of IPB support the cyberspace defense.

Step 1: Identify limits of the area of operations (external boundaries defined by joint forces commander); area of influence (geographical area the commander can influence); and area of interest (geographical area that extends outside the area of operations) will change as the situation changes.

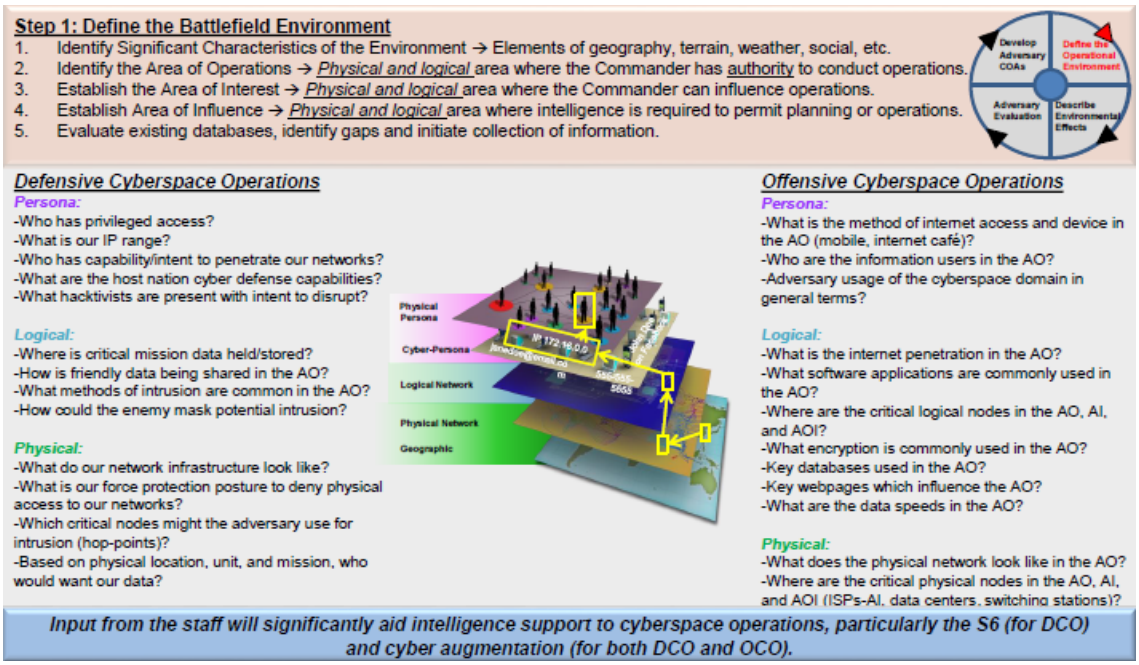


Figure F1. (U//FOUO) Define the Operational Environment

- Actions: Review known information on enemy, terrain, (OAKOC), weather, and ASCOPE

  ☐ Cyber: What are the adversary's physical and cyber personas, logical and physical networks, and geographic nodes?

  - Persona:
    - ✓ Who has privileged access?
    - ✓ What is our IP range?
    - ✓ Who has capability/intent to penetrate our networks?
    - ✓ What are the host nation's cyber defense capabilities?
    - ✓ What hacktivists are present with intent to disrupt?
    - ✓ What is the method of internet access and device in the area of operations (AO) (mobile, internet café)?
    - ✓ Who are the information users in the AO?
    - ✓ Adversary usage of the cyberspace domain in general terms

  - Logical:
    - ✓ Where is critical mission data held/stored?
    - ✓ How is friendly data being shared in the AO?
    - ✓ What methods of intrusion are common in the AO?
    - ✓ How could the enemy mask potential intrusion?
    - ✓ What is the internet penetration in the AO?
    - ✓ What software applications are commonly used in the AO?
    - ✓ Where are the critical logical nodes in the AO, area of influence (AI), and area of interest (AOI)?
    - ✓ What encryption is commonly used in the AO?

- ✓ Key databases used in the AO?
- ✓ Key webpages that influence the AO?
- ✓ What are the data speeds in the AO?

- Physical:
  - ✓ What do our network infrastructure look like?
  - ✓ What is our force protection posture to deny physical access to our networks?
  - ✓ Which critical nodes might the adversary use for intrusion (hop-points)?
  - ✓ Based on physical location, unit, and mission, who would want our data?
  - ✓ What does the physical network look like in the AO?
  - ✓ Where are the critical physical nodes in the AO, AI, and AOI (ISPs-AI, data centers, switching stations)?

☐ Review existing CONPLAN/OPLAN and identify the Cyber operational environment and requirements

☐ Review area of operations graphic (ATP 2-01.3, p. 3-4)

IPB Step 2: Determine how significant characteristics of the OE can affect friendly and threat/adversary operations. Identifying the desired end state is important in this step.

- Actions:
  - ☐ Describe how the adversary can affect friendly operations
  - ☐ Describe how terrain can affect friendly/adversary operations (terrain analysis for the AO and area of interest)
  - ☐ Describe how weather, light, and illumination data can affect friendly/adversary operations (ATP 2-01.3, p. 4-17)
  - ☐ Describe how civil considerations can affect friendly/adversary operations using ASCOPE and PMESII

- Outputs:
  - ☐ Adversary Overlay: depiction of current, physical adversary location in the AO and area of interest; includes identity, size, location, and strength (ATP 2-01.3, p. 4-3).

    - Cyber:
      - ✓ Physical and non-physical areas of operations / area of interest via identification of logical (e.g., hosts, servers, networks, ports) and physical (e.g., media communication infrastructure) networks
      - ✓ Known/suspected physical and cyber personas
      - ✓ Known/suspected number of actors/groups/dissemination intermediaries

  - ☐ Adversary Description Table: describes broad capabilities of each adversary depicted on overlay (ATP 2-01.3, p. 4-3)

    - Cyber:

- ✓ Consider the possible interdependence between the adversary's cyber capabilities and its military capabilities (e.g., the reliance on network communications infrastructure)
- ✓ Identify known/suspected technical expertise/capabilities/specialties/programs

☐ Modified Combined Obstacle Overlay: includes natural and manmade obstacles, avenues of approach (AA), key terrain, observation and fields of fire, cover and concealment, key facilities, and built up areas and civil infrastructure (ATP 2-01.3, pp. 4-4 thru 4-16)

- Cyber:
  - ✓ Obstacles: use of hardware and software, malware, firewalls, configurations
  - ✓ AAs: physical pathways to a target such as switches, routers, web servers, vectors
  - ✓ Key terrain: administrator accounts, DNS servers, network operating systems, switches, wireless device, main ISP inputs, vulnerable personal information
  - ✓ Observation and fields of fire: what portion of the network can be seen and from where
  - ✓ Cover and concealment:
    - Where can cyber threat actors hide their true identity and location (e.g., the Onion router, VPNs, multiple personas)
    - What are cyber threat actors using for protection (e.g., passwords, firewalls, software patches, anti-virus software, encryption software, non-attributable proxy systems, full disk encryption techniques)

Step 2: Describe Battlefield Effects

1. Analyze the Social Environment → ASCOPE-PMESII Crosswalk
2. Analyze the *Physical and Logical* Environment → Terrain Analysis (OAKOC) and develop Modified Combined Obstacle Overlay
3. Analyze the Weather → Visibility, winds, precipitation, cloud cover, temperature, humidity and effects.

Examples Civil Considerations for the Cyberspace Domain

ASCOPE/PMESII Crosswalk	Areas	Structures	Capabilities	Organizations	People	Events
Political	Political Websites; Strategic Objectives	Electronic Polling Sites; Gov't Servers	National Cyberspace Policy and Laws	Web presence of Pol. Organizations	Personas of politicians/leaders	Political Events hosted in cyber
Military	Mil Connectivity; Network types	Cyber Firing Arch or unit location by IP	CO Capability and Integration; ROE	MC, Fires, ISR, ADA Systems	Persona of key military officials	Historical Mil cyberspace activity
Economic	Websites or Servers for commerce	Connectivity of banks, industrial ICS	Online purchase; Financial websites	Private business cybersecurity	Personas of key land owners/employers	Cyberspace causes of Economic Loss
Social	Social Media; Blogs; Public Forums	Internet Cafes	General populace; Crowd Source	Web presence of Clans, Tribes, etc.	Personas; Influence Local Populace	CO Social events hosted/organized
Information	Common webpages in AO	Servers which host information/data	Data speeds and coverage	Media organizations on cyberspace	Key owners of websites	Key events in cyberspace
Infrastructure	802.11 Coverage	ISP, switching stations, VSATs, etc.	Data speeds, internet penetration	ISP/Telecom providers	Key contractors or builders	Maintenance or addition of domain

Social considerations for cyberspace can be developed and interwoven as part of the normal ASCOPE / PMESII analysis, not just information and infrastructure, which will aid target development.

Figure F2. (U//FOUO) Define the Environmental Effects

- ☐ Key facilities: public switched telephone networks (PSTNs), radio stations, media kiosks, internet cafes, electric power and other supervisory control and data acquisition (SCADA) systems, 3G towers, main hubs for data via mobile devices
- ☐ Terrain Effects Matrix: describes effects of OAKOC factors (ATP 2-01.3, p. 4-17)
- ☐ Weather, Light, and Illumination Charts/Tables: describes weather, light, and illumination effects on friendly/adversary operations (ATP 2-01.3, pp. 4-21 thru 4-28)

  - Cyber: Weather effecting data transmission (e.g., solar flares)

- ☐ Civil Consideration Data Files, Overlays, and Assessments: includes voting locations, organizations and bases locations, population/demographics overlays (ATP 2-01.3, pp. 4-36 thru 4-39)

  - Cyber:
    - Use of non-government organizations to provide tacit/explicit support (e.g., proxy media disseminators or internet cafes)
    - Use of government and non-combatant facilities for cyber attacks or media activity

Step 2: Describe Battlefield Effects

1. Analyze the Social Environment → ASCOPE-PMESII Crosswalk
2. Analyze the *Physical and Logical* Environment → Terrain Analysis (OAKOC) and develop Modified Combined Obstacle Overlay
3. Analyze the Weather → Visibility, winds, precipitation, cloud cover, temperature, humidity and effects.

Terrain Analysis of the Cyberspace Domain

Terrain	Geographic Considerations	Cyberspace Considerations
Observation/ Fields of Fire	-Ability to see the threat and the area where a weapon system can effectively engage.	-Ability to see within networks, subnets, password protection and encryption used in the AO.
Avenues of Approach	-An air or ground route that leads an attacking force to an objective or key terrain.	-Methods/path of adversary intrusion or methods of access to key terrain.
Key Terrain (Critical Asset)	-A locality or area the seizure, retention, or control of which affords a marked advantage to either combatant.	-A physical or logical node which affords a marked advantage to either combatant.
Obstacles	-Natural or man-made terrain features that stop, impede, or divert military movement.	-Network features such as intrusion detection systems, firewalls, and encryption.
Cover and Concealment	-Protection from observation and protection from the effects of direct and indirect fires.	-Our electromagnetic signature, cyber hygiene, and ability to limit attribution within cyberspace.

The outputs from the terrain analysis could include a modified combined obstacle overlay (MCOO) specific to cyberspace. Who does the Cyberspace domain favor?

Figure F3. (U//FOUO) Define the Environmental Effects (Continued)

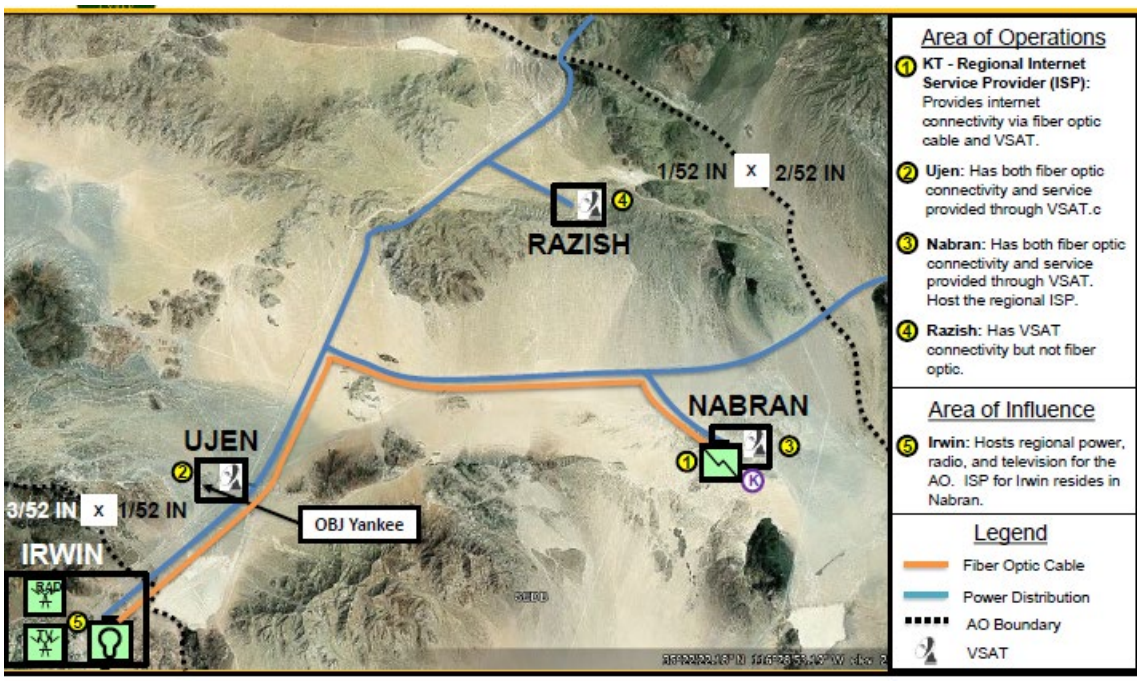


Figure F4. (U//FOUO) Example of Step 2 (Persona and Physical Layers)

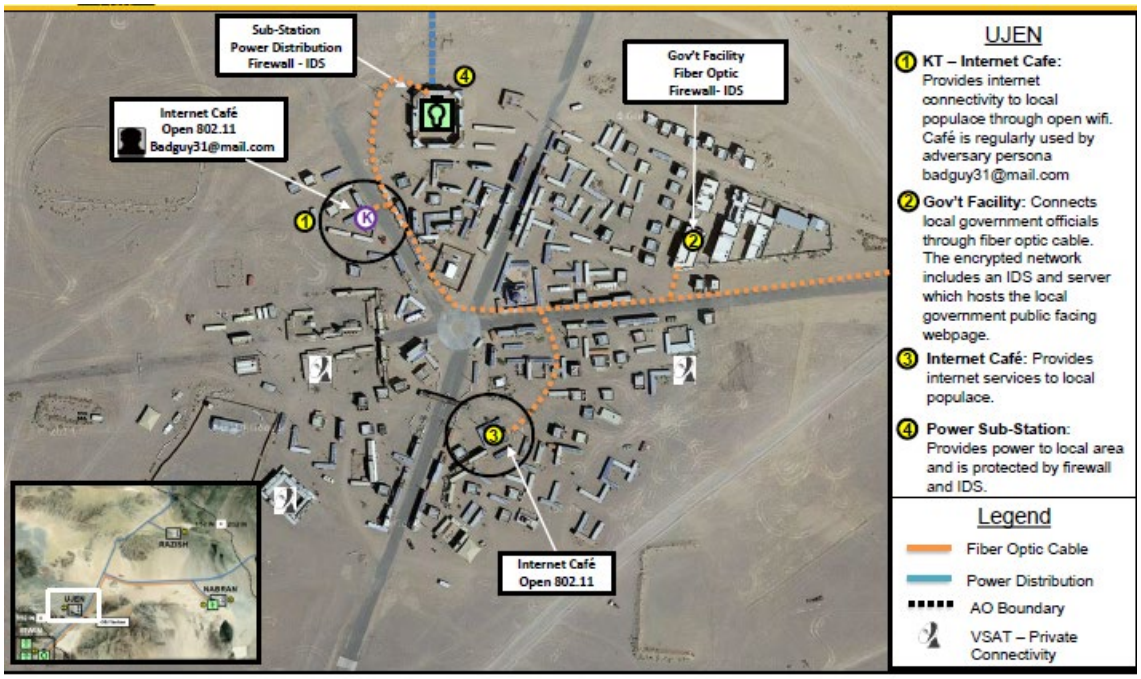


Figure F5. (U//FOUO) Example of Step 2 Continued (Information Overlay)

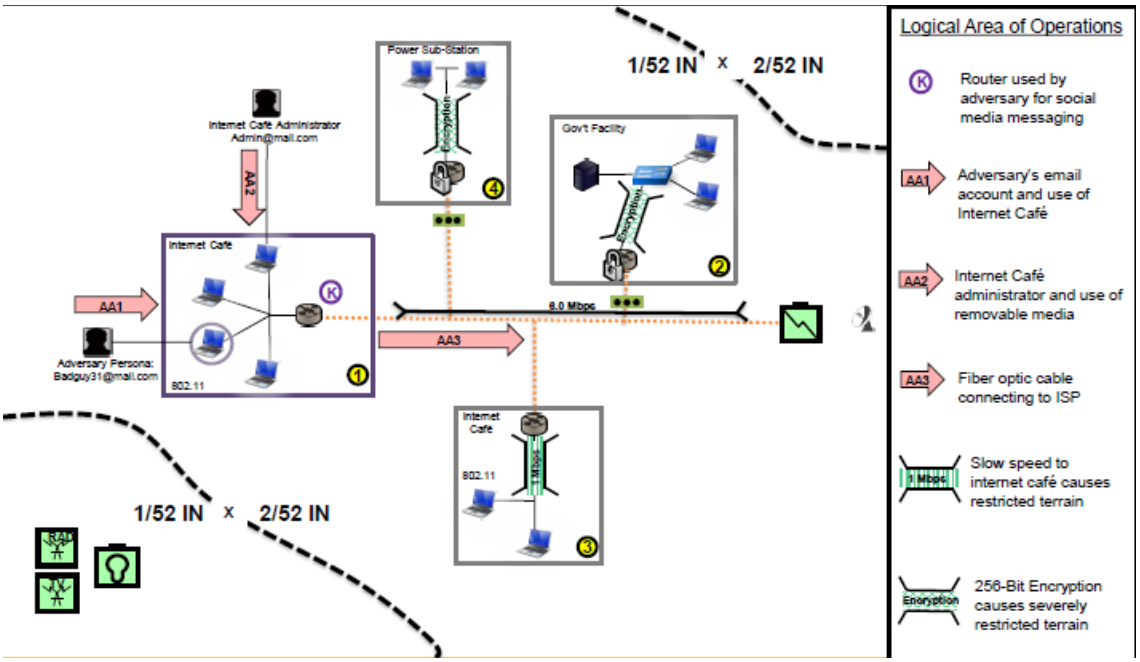


Figure F6. (U//FOUO) Example of Step 2 Continued (Logical Overlay)

IPB Step 3: Determines adversary (regular/irregular/hybrid) force capabilities and the doctrinal principles and TTP adversary forces prefer to employ.

- Action: Develop threat models that identify adversaries in the AO as well as adversary courses of action (COA)

☐ Outputs:

☐ Adversary Order of Battle: includes composition, disposition, strength, combat effectiveness, doctrine & tactics, support & relationships, electronic technical data, capabilities & limitation, current operations, historical data, miscellaneous data (ATP 2-01.3, pp. 5-3 thru 5-21)

- Cyber:
  - ✓ Social networking hierarchy
  - ✓ C2 infrastructure (e.g., C2 nodes and call back domains)
  - ✓ What does the adversary want from our networks?
  - ✓ Do we have an insider threat; is there a green-on-blue or FIS physical access threat?
  - ✓ NAI – May have NAIs specific to your organization for collection but some will be of strategic interest where the S2 can pull threat reporting

☐ Adversary Tactics/Options (ATP 2-01.3, p. 5-22)

- Cyber:
  - ✓ What are the global patterns against similar networks?
  - ✓ Who has intent and capability to penetrate our networks?

- ✓ What are the techniques specific to the actors who have intent and capability?
- ✓ What type of malware is commonly used by actors of interest
- ✓ What are the methods of lateral movement by actors of interest?

☐ Identify Adversary Capabilities (ATP 2-01.3, p. 5-23)

☐ Cyber:

- ✓ Cyber actor(s)' pattern of operations
- ✓ Planning/scanning TTPs
- ✓ Exploitation TTPs
- ✓ Lateral movement of actors
- ✓ Adversary exfiltration
- ✓ Adversary intent (e.g., reconnaissance, espionage, destructive malware)
- ✓ Media production flow (e.g., local, regional, global)
- ✓ Use of network to conduct operations and OPSEC
- ✓ Use of technological weapons
- ✓ Identify unique electronic signatures

Step 3: Evaluate the Adversary

1. Identify Threat/Adversaries Capabilities
2. Update or Create Threat/Adversary Models
   - Convert Threat/Adversary Doctrine or Patterns of Operations Graphics
   - Describe Threat/Adversary Tactics and Options
   - Identify High-Value Targets (HVT)

Threat Capability

Warfighting Functions	*How does the Adversary use the Cyberspace domain to support each Warfighting Function?*
Mission Command	Delegation of authority, synchronization and direction of forces through the cyberspace domain. *Example: Usage of email or a website to administer guidance to subordinate units.*
Movement and Maneuver	Movement of forces (physically or logically) to achieve an advantage over an adversary in the cyberspace domain. *Example: Conducting a Distributed Denial of Service (DDoS) to prevent the adversaries movement of forces.*
Intelligence	Information derived through cyberspace which enables understanding of the adversary, terrain, or civil considerations. *Example: Open source collection of adversary social media accounts.*
Protection	Cyberspace enabled methods to preserve the force to allow the commander to apply maximum combat power. *Example: Adversary's usage of defensive cyberspace operations to prevent geolocation.*
Sustainment	Cyberspace synchronized/coordinated support and services to enable freedom of maneuver, extend reach and endurance. *Example: Databases or cyberspace enabled order processes of an adversary's equipment or mission essential supplies.*
Fire Support	The collective/coordinated use of indirect, cyberspace, missile defense and joint fires through the targeting process. *Example: An adversary's use of offensive cyber operations or adversaries' automated fires systems.*

The adversary/threat will have varying capabilities across all warfighting functions but the cyberspace domain will likely touch all of them.

Figure F7. (U//FOUO) Evaluate the Adversary

☐ Adversary Template (ATP 2-01.3, pp. 5-24 thru 5-28)

☐ Adversary Capabilities Statement (ATP 2-01.3, pp. 5-28 & 5-29)

- Cyber: Conduct a critical factors analysis to determine how to affect the actor's ability to target US interests. Determine the critical capabilities, the critical requirements, and the vulnerabilities.

☐ Identify High-Value Targets (ATP 2-01.3, p. 5-29)

- Cyber: Employ CARVER methods:
  - ✓ Criticality: effect of destruction, denial, disruption, or degradation of a component on the adversary's operations
  - ✓ Accessibility: where does the actor(s) reside (red, grey, or blue space) and how protected is their network
  - ✓ Recuperability: how long will it take the actor to repair, replace, or bypass the damage physical/nonphysical component
  - ✓ Vulnerability: can the actor's security feature be bypassed; can the pattern of operations be exploited
  - ✓ Effects: what are potential secondary and tertiary effects as well as potential collateral damage
  - ✓ Recognizability: what sort of obfuscation techniques (proxy, spoofing, etc.) does the actor employ; what is the reliability of the actor's selectors/observables

IPB Step 4: Identifies and describes threat / adversary COAs that can influence friendly operations.

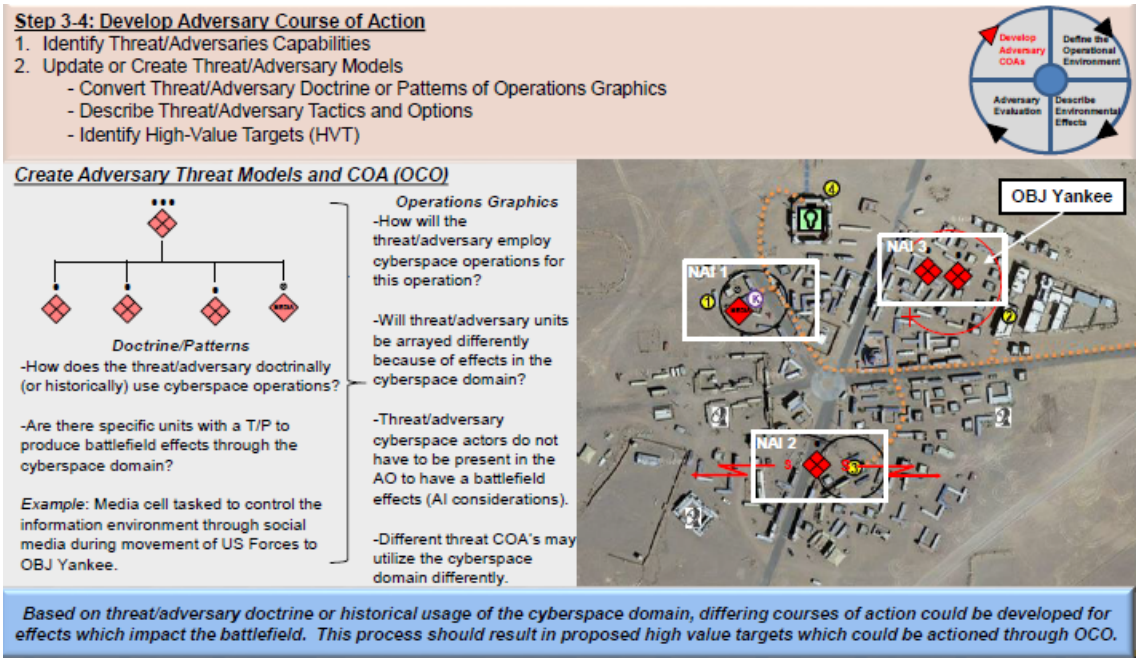


Figure F8. (U//FOUO) Develop Adversary COA

- Action: Develop adversary COAs

  ☐ Cyber: Develop most likely and most dangerous COAs by each Warfighting Function
  ☐ Develop event template and matrix

- Outputs:
  ☐ Refined Adversary COA Statement (ATP 2-01.3, p. 6-13)
  ☐ Enemy Situation Template (ATP 2-01.3, pp. 6-7 thru 6-15)
  ☐ Event Matrix (ATP 2-01.3, p. 6-16)

- ☐ Identify Potential Objectives, Decision Points, NAIs, and TAIs (ATP 2-01.3, p. 6-17)
  - Cyber
    - Refine cyber actor(s) pattern of operations
    - Identify networks that support the adversary's C2 and military operations
- ☐ HVTL and provide input to HPTL
- ☐ Provide input to collection plan
- ☐ Update intelligence estimate
- ☐ Provide input into PIRs
- ☐ Provide input into OPORDs / OPLANs (annexes/appendices)

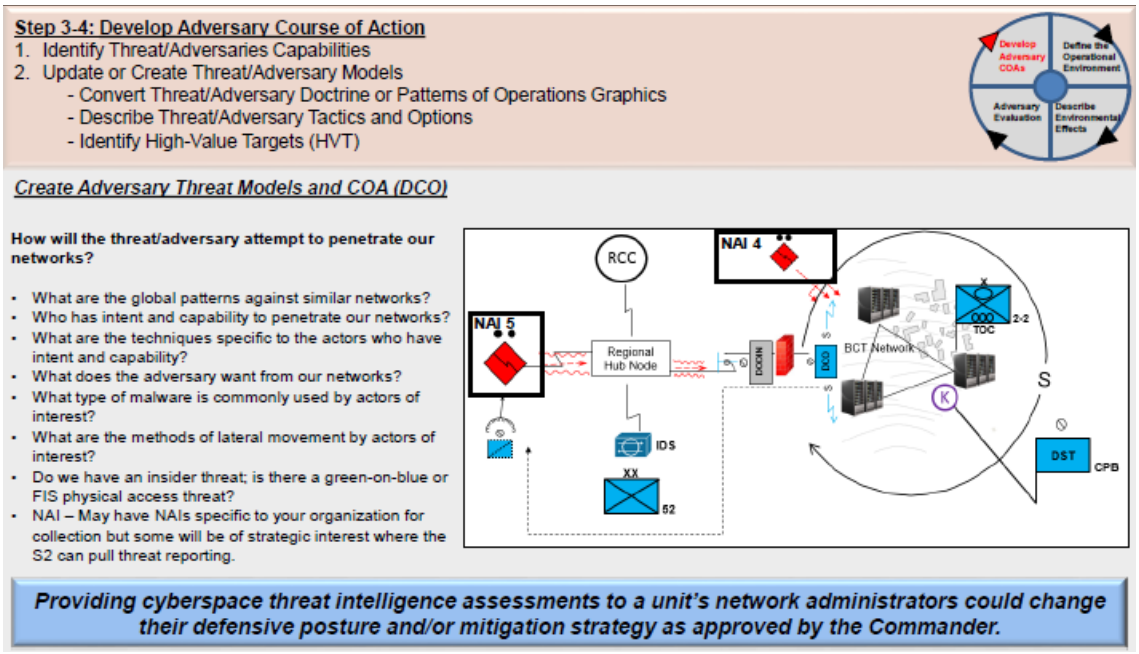
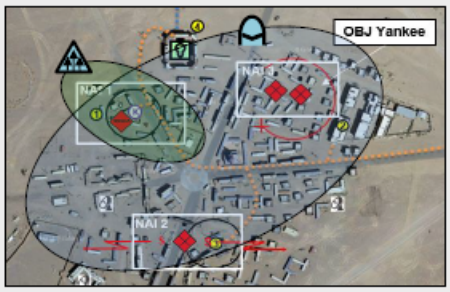
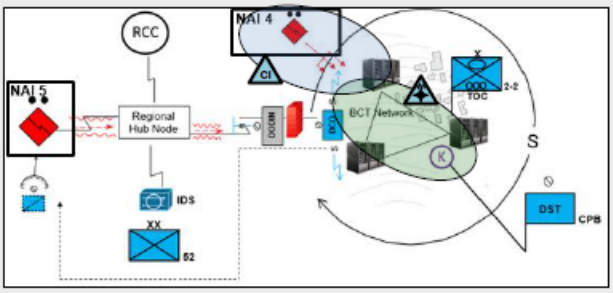


Figure F9. (U//FOUO) Develop Adversary COA Continued

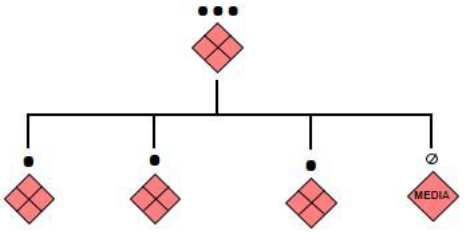




PIR	EEI	SIR	NAI	Collection Asset						Organic Reporting		
				Scouts	HCT	Prophet	CI	OSINT	Shadow	CST	CPT Sensors	S6/User
PIR1: Adversary utilization of the cyberspace domain which impact BCT or host nation operations.	EEI 1.1: What adversary actions indicate a comprise of BCT or host nation networks?	SIR 1.1.1: Report exfiltration of large data quantities from BCT networks.	4, 5		X	X	X				X	X
		SIR 1.1.2: Report protected US or host nation data posted to open forum or social media	4, 5				X	X				
		SIR 1.1.3: Report attempted spear-phishing against BCT networks	4, 5								X	X
	EEI 1.2: What adversary actions indicate malicious CO with the Area of Operations?	SIR 1.2.1: Report adversary utilization of social media to influence the populace.	1					X		X		
		SIR 1.2.2: Report adversary's physical access to known malicious CO locations.	1, 2	x	X	X		X	X	X		
		SIR 1.2.3: Report adversary patterns in malicious network activity.	1, 2							X		

All collection assets can be used to answer PIR related to the cyberspace domain in support of both DCO and OCO.

Figure F10. (U//FOUO) Develop Adversary COA Continued



Doctrine/Patterns

-How does the threat/adversary doctrinally (or historically) use cyberspace operations?

-Are there specific units with a T/P to produce battlefield effects through the cyberspace domain?

Example: Media cell tasked to control the information environment through social media during movement of US Forces to OBJ Yankee.

Operations Graphics

-How will the threat/adversary employ cyberspace operations for this operation?

-Will threat/adversary units be arrayed differently because of effects in the cyberspace domain?

-Threat/adversary cyberspace actors do not have to be present in the AO to have a battlefield effects (AI considerations).

-Different threat COA's may utilize the cyberspace domain differently.

Figure F11. (U//FOUO) Example of Considerations in the Cyberspace Domain