Active Defense
from Telos Corporation

A Framework for Aligning Operational Requirements with Cyber Capabilities in support of GCCs, JTFs and their AORs

> ***"DOD will treat cyberspace as an operational domain to organize, train and equip so that DOD can take full advantage of cyberspaces potential."***
> *("Department of Defense Strategy for Operating in Cyberspace," July 2011*)

> ***"Currently, the approach to cyber defense is based primarily on policy compliance, hardening configurations, and patching vulnerabilities, which are necessary but not sufficient."*** (DoD CIO Testimony to the House Armed Services Subcommittee on Intelligence, Emerging Threats and Capabilities, March 13, 2013)

Cyberspace is the only warfighting domain where defense is weaker than offense and a far inferior foe can cripple or overwhelm a force that enjoys superior resources and numbers. Achieving mission success in a world where information is the lifeblood of military capability requires thought leadership and a new innovative approach in leveraging old and new capabilities.

That requirement can be met by an **active defense approach to cybersecurity** that establishes an operational framework specific to a particular Global Combatant Command (GCC) or Joint Task Force (JTF) and maps technology capabilities to the requirements of their area of responsibility (AOR).

Telos Corporation: Active Defense that Integrates Operational Requirements with Cyber.

Telos Corporation offers a comprehensive security methodology and balanced cyber portfolio that takes advantage of the full spectrum of offensive and defensive variables to win and remain viable in a contested environment.

Our active defense approach creates the conditions to improve your capacity for action to achieve mission assurance. Active defense goes beyond the static perimeter to define adversary intentions and identities in order to better protect critical assets and provide options to facilitate decision-making. Active defense allows defenders to see their defenses/assets as their adversary would, in order to gain an understanding of and the ability to anticipate the enemy's techniques and tactics.

Active defense is a cross-disciplinary approach that establishes resiliency in the cyber domain. By synchronizing architecture, governance and operations with business processes and missions, active defense provides a streamlined system for organizations to operate in a chaotic and contested cyber environment.

Active defense does not replace current directives and instructions, but instead combines the functions of Critical Infrastructure Protection, Force Protection, Information Assurance, Operational Risk Management, Operations Research and Military Science and Art into a complete and more cohesive methodology to achieve greater efficiency and effectiveness.

The Telos active defense approach provides a methodology to provide a streamlined system for organizations to operate in a chaotic and contested cyber environment.

Active defense focuses on establishing the context of the operating environment while respecting the operational design and critical capabilities that enable organizations to function and compete. Key concepts of our active defense framework are:

- Understanding contextual, operational design and critical capabilities;
- Conducting full assessments of both friendly and adversary capabilities and vulnerabilities;
- Developing and employing dynamic prevention and mitigation strategies; and
- Developing adversary capabilities (tactics, techniques and procedures), intentions and vulnerabilities for future operational constructs and decisions

Traditional systems tend to be static and dependent on lagging indicators. Active defense provides effective methodologies and capabilities to begin to operate and make critical operational decisions from *leading* indicators without negating the importance of governance, architecture, design and integration.

Active defense is an approach that works within the dynamic that assumes not everything can be defended equally, and that having established benchmarks for intervention is more important than striving to reach the unobtainable "100 percent security." Instead, active defense centers on operational context and establishing an integrated approach that delivers advantage in the cyber domain.

The Telos Approach

Telos focuses on four components to achieve active defense: 1) understanding and mastery of the customer's operating environment; 2) seasoned professionals that are highly educated,

trained and experienced to operate in high-performing organizations; 3) the ability to rapidly develop and deploy customized capabilities to meet mission requirements; and 4) the ability to visualize critical information in the cyber domain.

Mastery of the Operating Environment

Architecture, governance and operations are currently isolated functions within an organization that tend to compete with one another. The friction between the functions is compounded when the responsibilities for each function are distributed amongst several organizations that are geographically dispersed. The friction is further exacerbated when the changing nature, lethality and motivation of the threat is realized as determined actors seeking to disrupt, deny and exploit access to critical information and systems.

Mastery of the friendly environment requires a deliberate synchronization of the operational architecture (the design in which to achieve success) with the technical architecture (the support system to enable success) that is governed by a process which shapes successful current and future operations. Where governance was previously seen as a bureaucratic process, the Telos approach aligns applicable standards, protocols and directives with the mission requirements of the customer in order to enable operations. Essential to success is the implementation of an operational risk framework that can be synchronized with priorities and missions.

The Telos approach to active defense aligns applicable standards, protocols and directives with the mission requirements of the customer in order to enable operations.

The adversary will never be mastered; however, an aggressive proactive approach that encompasses the principles of both the offense and defense to prevail in a contested environment will start to move organizations into an active defensive posture.

Seasoned Professionals

Warfare, including cyber warfare, is a human endeavor; to achieve resilience requires an investment in intellectual capital. While technology is important, seasoned operators and technicians synchronized to achieve desired effects are crucial to achieving mission assurance. Developing an intellectual and operational framework that supports the overarching mission is critical for success.

Telos is focused on providing the highest caliber operational and technical personnel that can integrate all aspects of Cyber Computer Network Defense/Computer Network Attack/Computer Network Exploitation (CND/CNA/CNE) and synchronize with the overall mission and the other battle-space functions.

Our operations personnel are experienced unconventional and conventional warfare practitioners and come from the special operations, combat arms and intelligence communities. They are proven and skilled operational planners and operational architects that work in tandem with our highly skilled technical personnel. Our technical personnel are top tier civilian and military specialists in computer network defense (CND). And, they have the experience in computer network attack and exploitation (CNA/CNE) to think like the adversary and anticipate his moves.

Together, the operators and technical personnel form a capable team that work toward solving difficult and challenging problems that arise in the cyber domain.

Customized Capabilities

Telos Corporation in conjunction with industry partners has produced a full-spectrum cyber capability that integrates the elements of CND/CNA and CNE into a single platform. The advanced cyber capabilities are designed to maximize all aspects of intelligence, generate a cyber collection and surveillance plan, execute a surveillance plan, and evaluate and exploit the results, as well as provide customized options that are synchronized with the overall mission.

Visualization

Critical to leveraging the potential of cyberspace is the ability to fuse previously unused data and information into actionable intelligence and to present it in a meaningful way. Our teams of operations and technical personnel ensure that the cyber picture is synchronized with the mission and can be presented in parallel with other critical factors that effect and determine the outcome of the mission.

Telos Corporation: Operational Requirements and Tasks for Establishing an Active Defense

Telos Corporation's approach to active defense focuses on defining your specific operational requirements and aligning them with the cybersecurity capabilities and technologies most appropriate for achieving mission success.

The key operational requirements and tasks are as follows:

1. **Establish the operating context for the organizational cyber domain. The main focus is on the adversary and the threat.**
    - 1.1 Prioritize and categorize threats based upon current and future operations within the **geographic layer**
    - 1.2 Prioritize and categorize threats based upon current and future operations within the **physical infrastructure layer**
        - 1.2.1 Prioritize and categorize threat devices and nodes
    - **1.3** Prioritize and categorize threats based upon current and future operations with the **network layer**
        - 1.3.1 Prioritize and categorize threat protocols
    - 1.4 Prioritize and categorize current and future operations with the **threat cyber persona layer**
        - 1.4.1 Prioritize and categorize known and discovered cyber personas

1.5 Establish geographic, physical infrastructure, network and cyber persona relationships to create a prioritized and categorized cyber suspect list

1.5.1 Synchronize results with existing intelligence and information

2 Establish an operational framework for the organizational cyber domain. The main focus is on synchronizing with current and future operations in the other domains and to develop the intellectual capital to create an active defense.

2.1 Establish an operational design for the organizational cyber domain

2.1.1 Develop a recommended commanders vision statement for the organizational cyber domain that is synchronized with current and future operations and addresses:

2.1.1.1 Ends

2.1.1.2 Ways

2.1.1.3 Means

2.1.1.4 Risk

2.1.2 Develop an organizational **operational approach** for active defense

2.1.3 Develop an organizational **mission statement** for active defense

2.1.4 Develop an organizational **Concept of Operations** (CONOPS) for active defense

2.1.5 Develop and recommend Commanders Critical Information Requirements (CCIRS) Friendly Force Information Requirements (FFIRS) and Priority Intelligence Requirements (PIRS)

3 Establish a technical framework for active defense. The main focus is synchronizing current and future cyber capabilities with operational tasks.

3.1 Identify critical governance tasks, constraints and restraints

3.1.1 Integrate the results with task 2.1.1.4 (Risk)

3.2 Identify key system capabilities and limitations within the cyber architecture

3.2.1 Integrate the results with task 2.1.1.3 (Means)

3.3 Identify key information requirements for the operation of the organizational cyber infrastructure.

3.3.1 Integrate with task 2.1.5 (CCIRS) and task 2.1.1.2 (Ways)

3.4 Identify critical capabilities and critical individuals

3.4.1 Integrate with task 2.1.5 (CCIRS)

4 Synchronize the operational framework with the technical framework for active defense. The main focus is "operationalizing" cyber tasks into a standard operational format that can be synchronized with other operational domains and other missions.

- 4.1 Develop the results of task 3.1 (Governance) into an operational risk methodology that is synchronized with other operational domains
- 4.2 Identify and designate mission critical systems, applications and capabilities and develop a decision support matrix that presents options for decision during normal operations and when in a contested environment
- 4.3 Develop a methodology for integrating cyber information requirements into the organization request for information system (RFI)

5 Develop and implement an all source/all capability surveillance plan for critical capabilities and individuals. The main focus is to synchronize traditional surveillance and monitoring capability with other existing capabilities.

- 5.1 Implement the surveillance plan on **critical capabilities**
  - 5.1.1 Establish baseline thresholds on all critical capabilities
  - 5.1.2 Establish intervention/investigation criteria for all critical capabilities
  - 5.1.3 Develop and implement assessment methodologies to establish measures of effectiveness
- 5.2 Implement the surveillance plan on **critical personnel**
  - 5.2.1 Establish baseline thresholds for critical individuals
  - 5.2.2 Establish intervention/investigation criteria for all critical individuals
  - 5.2.3 Develop and implement assessment methodologies to establish measures of effectiveness

6 Implement an "Adversary View" of critical capabilities and Individuals. The main focus is to on demand determine attack surfaces and vulnerabilities of critical capabilities and individuals, as an adversary would see them.

- 6.1 Implement an external-to-internal on-demand vulnerability assessment of critical capabilities and personnel
- 6.2 Implement an operational/technical remediation of vulnerabilities
- 6.3 Implement a targeted surveillance plan of all critical capabilities and individuals until full remediation

7 Develop geographic, infrastructure, network, cyber persona and cyber faction areas and targets of concern. The main focus is to establish priorities for future observation and monitoring.

- 7.1 Prioritize geographic areas and the threats that emanate from them
- 7.2 Prioritize infrastructures and the types of threats that come from them

7.3 Prioritize networks (human and physical) and the threats that come from them

7.4 List and prioritize cyber personas with known intentions to disrupt, degrade, exploit or deny cyber activity

7.5 List and prioritize cyber factions with known intentions to disrupt, degrade, exploit or deny cyber activity

7.6 Synchronize tasks 7.1 thru 7.5 with all others sources of information and intelligence

8 Implement an internal cyber collection plan. The main focus is to gather readily available data to begin to determine adversary identities and intentions.

8.1 Collect attempted intrusion/attack data and correlate with the results of Task 7

8.1.1 Develop cyber surveillance targets

8.1.2 Develop and implement an external surveillance plan

8.2 Synchronize attempted intrusions/attacks with potential effects on other missions and operations

9 Develop and implement a full-spectrum cyber assessment capability for designated individuals or for designated missions. The main focus is to determine individual or collective cyber signatures and to present options for mitigating risk.

9.1 Develop a detailed assessment for designated individuals and missions that details individual or collective cyber signatures

10 Develop and implement a visualization capability that integrates cyber with operations in other domains.

10.1 Develop a visualization capability for depicting **the context of the organization's cyber domain**

10.2 Develop a visualization capability for depicting **CCIRs, PIRs and FFIRs**

10.3 Develop a visualization capability for depicting **critical capabilities and individuals**

10.4 Develop a visualization capability for depicting a **decision support matrix**

10.5 Develop a visualization capability for depicting an **internal surveillance plan** for critical capabilities and individuals

10.6 Develop a visualization capability for depicting an **adversary view** of critical capabilities and individuals

10.7 Develop a visualization capability for depicting **geographic, infrastructure, network, cyber persona and cyber faction areas** and individuals of interest

10.8 Develop a visualization capability for depicting **attempted intrusions and attacks** that are related to current and future missions and operations

10.9 Develop a methodology and display mechanism for **depicting cyber signatures** for designated individuals and missions

About Telos Corporation

Telos Corporation delivers solutions that empower and protect the world's most security-conscious enterprises. We *empower* our customers with secure solutions that leverage mobile communication and real-time collaboration. We *protect* our customers' vital assets, including their critical operational and tactical systems so that they can safely conduct their global missions. Our solutions are employed by defense and civilian agencies of the federal government, the intelligence community, all branches of the armed forces, NATO allies, and commercial enterprises that demand high security.

For more information, please contact:

Telos Corporation
19886 Ashburn Road, Ashburn, Virginia 20147
Toll-free: 1-800-444-9628 | info@telos.com
www.telos.com | @telosnews | facebook.com/teloscorporation