# Cyber Continuity of Operations Planning

## Overview

Increasing resilience against threats of destructive malware requires insight into the current security posture, planning and coordinating key defensive actions, and aligning key defensive resources correctly. This document describes how to apply *Dynamic Representation*[1], *Coordinated Defense,* and *Realignment* resiliency techniques into cyber architectures, techniques, tactics and procedures (TTPs).

## Applying *Dynamic Representation* to Detect and Analyze Adversary Activity

*Dynamic Representation* is the capability to reflect changes in state or behavior and materializes through constructing and maintaining a *dynamic representation* of components, systems, services, mission dependencies, adversary activities, and effects or alternative cyber courses of action. *Dynamic Representation* should first ensure the existence of static representations and then expand upon them so adversary actions, once detected and analyzed, will inform mission situational awareness and response. *Dynamic Representation* implementation approaches include:

- Dynamic Mapping and Profiling: Maintaining current information about resources, their status and their connectivity.
- Dynamic Threat Modelling: Maintaining current information about threat activities and characteristics (e.g., observables, indicators, adversary techniques, tactics, and procedures (TTP)).
- Mission Dependency and Status Visualization: Maintaining current information about the mission on resources, and the status of those resources with respect to threats.

## Priorities for Immediate Action with *Dynamic Representation*

- Construct and maintain a dependency model mapping functions to capabilities, services and systems.
    - Identify and map the high-level associations like process-to-application or system and application-to-service.
    - Use dynamic mapping and profiling tools (e.g., tools referenced in Situational Awareness Reference Architecture Guide at http/ics-isac.org/blog/sara) and dynamic threat modeling tools (e.g., those with real time or dynamic capabilities)
- Perform an impact analysis to determine crown jewels/core services and systems.
    - Understand and prioritize incidents and events in terms of business impact.
    - Determine the organizational and business impacts
- Define processes for updating the assessment of threat susceptibility for core services and systems.
    - Develop and use simulation exercises to test core processes, systems, and services to the point of failure (e.g., chaos monkey type tool).
    - Implement periodic review of cyber resiliency defender TTPs against new and evolving known threats so the defender TTPs will be reflective of the current threat environment.

[1] All italicized words are defined in the *Cyber Resiliency Terms and Concepts* document.

## Applying *Coordinated Defense* to Delay and Degrade Adversary Activity

*Coordinated Defense* is using a coordinated, adaptively managed approach for applying multiple, distinct defense mechanisms at different architectural levels and with different configurations settings to delay, degrade, and deny adversary actions upon critical core resources. *Coordinated Defense* implementation may entail:

- Technical Defense-in-Depth: Using multiple protective mechanisms applied at different architectural layers or locations.
- Coordination and Consistency Analysis: Applying processes, supported by analytic tools, to ensure that defenses are applied and cyber courses-of-action are defined and executed in a coordinated, consistent, and non-disruptive way.
- Adaptive Management: Changing how defense mechanisms are used based on changes in the operational environment as well as changes in the threat environment.
- Course of Action (CoA) Analysis: Maintaining a set of alternative CoAs, with supporting analysis of resource requirements, contingencies for meeting those requirements, and effects of CoAs on current and future mission capabilities.

## Priorities for Immediate Action with *Coordinated Defense*

- Develop a cyber 'Go Bag' with essential procedures and information.
    - Assemble mobile cyber security toolkits that include procedures for establishing, implementing, maintaining, and enabling the continuance of cyber resilient TTPs within a COOP-designated facility (refer to http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901 for an example).
- Develop, test and validate playbooks, roles, responsibilities, and tools.
    - Designate specific cyber roles, associated responsibilities, and the cyber tools that may be deployed to ensure implementation of cyber COOP.
    - Define standard cyber COOP plays for individual or cyber team execution using cyber 'Go Bag' tools and elastic TTPs.
    - Conduct different types of cyber exercises (e.g. mini-table top type exercises) using the cyber 'Go Bag' and playbook.
- Define collaboration processes and acquire tools for cyber defenders and incident responders.
    - Ensure both mobile and stationary cyber COOP processes incorporate communication and coordination dovetailing to promote adequate management of cyber defenses, synergy among all response activities, and reduction of security coverage gaps during recovery activities.

## Applying *Realignment* to Degrade and Delay Adversary Activity

*Realignment* is defining and determining the operational implications and resource needs of alternate and primary mission and cyber defender courses of action. *Realignment* aligns cyber resources with core aspects of mission/business functions and helps reduce the attack surface, thereby degrading and delaying adversary activity. *Realignment* implementation entails:

- Purposing: The mission purposes of functions, services (including connectivity as well as processing), information and systems are identified, to prevent uses that increase risk without any corresponding mission benefit.
- Offloading/Outsourcing: Supportive but non-essential functions are offloaded to a service provider that is better able to support the service.

- Agility/Repurposing: System elements are repurposed to provide services, information, and connectivity to meet new or changing mission needs.
- Customization: Critical components are custom-developed or re-implemented.
- Restriction: Risky functionality or connectivity is removed or replaced with less risky implementations.

## Priorities for Immediate Action with *Realignment*

- Identify mission and business function dependencies on cyber resources.
    - Determine the mission purposes of resources so that uses that increase risk without any corresponding mission benefit can be identified and eliminated.
        - Identify and remove or replace data feeds and connections for which risks outweigh benefits.
    - Consider the interdependencies between and among mission and non-mission business functions and organizations that share critical roles in the delivery of NEF capabilities.
        - Reallocate resources or reassign administrative and management responsibility based on risk to mission and business function.
- Identify non-mission and business function dependencies on or uses of cyber resources.
    - Make use of mission flow analysis, mission dependency analysis, tabletop exercises, and Red Teaming to uncover undocumented mission dependencies.
    - Review and correlate mission and business functions with dependency model mapping and impact analysis activities and results.
    - Identify systems, applications and processes of non-mission critical functions and the resources that support them.
        - Assess those functions against a fluid Cyber COOP implementation strategy to accommodate priority operations and better dependency utilization or elimination.

## Preparing for the Future

With the advent of the internet of things, dependency analysis (which underlies *Dynamic Representation*) will become much harder to discern. This is because components that traditionally did not have cyber elements (e.g., appliances) will now (or in the near future) have such cyber elements opening these components up to potential cyber-attack and increases the mission cyber-attack surface. This in turn increases the complexity of determining dependencies between components because two components that only have direct physical dependencies (e.g., car and fuel pump) may now have indirect cyber dependencies (e.g., cyber compromise of fuel pump could disable it, thus impacting the fueling of the car). This increase in complexity due to incorporating devices with embedded systems into larger ecosystems has the potential for unintended consequences. For example, the incorporation of wireless capabilities into avionics may cause the avionics to be impacted if not properly isolated from passenger use of Wi-Fi.