



Project No.: 0713ECSE-KE

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release; Distribution Unlimited. 13-3513.

©2013 The MITRE Corporation.  
All rights reserved.

**Bedford, MA**

## **Resiliency Techniques for Systems-of-Systems**

### **Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain**

**Deborah Bodeau  
John Brtis  
Richard Graubart  
Jonathan Salwen  
September 2013**

## **Abstract**

This white paper describes how resiliency techniques apply to an acknowledged system-of-systems (SoS). MITRE's cyber resiliency engineering framework is extended, to address a broader range of threats than purely cyber. The extended framework is intended to apply to systems-of-systems that include cyber-physical constituents, and in particular to space systems.

This page intentionally left blank.

# Table of Contents

1	Introduction.....	1
2	Key Concepts and Terminology .....	1
2.1	Systems-of-Systems.....	1
2.2	Considerations for Space Systems.....	2
2.3	Cyber Resiliency.....	2
3	How Resiliency Techniques Can Apply in an Acknowledged SoS .....	8
3.1	Resiliency Techniques in SoS Operations .....	8
3.2	Opportunities and Challenges for Emergent Resiliency.....	9
4	Detailed Analysis .....	12
4.1	Applicability of Specific Cyber Resiliency Techniques.....	12
4.1.1	Adaptive Response.....	12
4.1.2	Analytic Monitoring.....	13
4.1.3	Coordinated Defense.....	14
4.1.4	Deception .....	16
4.1.5	Diversity.....	17
4.1.6	Dynamic Positioning.....	18
4.1.7	Dynamic Representation.....	19
4.1.8	Non-Persistence .....	20
4.1.9	Privilege Restriction.....	21
4.1.10	Realignment .....	21
4.1.11	Redundancy.....	22
4.1.12	Segmentation/Isolation .....	24
4.1.13	Substantiated Integrity .....	25
4.1.14	Unpredictability .....	26
4.2	Summary .....	26
4.3	Synergies and Dependencies among Resiliency Techniques .....	28
4.4	Cyber Resiliency Techniques and Disaggregation .....	29
5	Conclusion .....	31
6	Bibliography .....	32
Appendix A	Abbreviations .....	35
Appendix B	Survivability.....	36

## List of Figures

Figure 1. Cyber Resiliency Engineering Framework .....	3
Figure 2. Resiliency Techniques in Operational Context .....	8

## List of Tables

Table 1. Resiliency Framework for Space SoS: Goals .....	4
Table 2. Resiliency Framework for Space SoS: Objectives .....	4
Table 3. Resiliency Framework for Space SoS: Techniques .....	5
Table 4. Mapping Cyber Resiliency Techniques to Objectives.....	7
Table 5. Opportunities and Challenges for Emergence of Resiliency .....	10
Table 6. Adaptive Response in SoS.....	12
Table 7. Analytic Monitoring in SoS.....	13
Table 8. Coordinated Defense in SoS.....	15
Table 9. Deception in SoS .....	16
Table 10. Diversity in SoS.....	17
Table 11. Dynamic Positioning in SoS.....	18
Table 12. Dynamic Representation in SoS .....	19
Table 13. Non-Persistence in SoS.....	20
Table 14. Privilege Restriction in SoS.....	21
Table 15. Realignment for SoS.....	22
Table 16. Redundancy for SoS .....	23
Table 17. Segmentation/Isolation in SoS.....	24
Table 18. Substantiated Integrity in SoS.....	25
Table 19. Unpredictability for SoS .....	26
Table 20. SoS Applicability of Cyber Resiliency Techniques (Capabilities and Approaches)....	26
Table 21. Relationships among Resiliency Techniques .....	29
Table 22. Disaggregation and Cyber Resiliency Techniques .....	30
Table 23. Mapping of Cyber Resiliency Framework to Principles for Survivable Systems .....	36

This page intentionally left blank.

# 1 Introduction

Resiliency, particularly in the face of advanced cyber threats, is of increasing interest to military and critical infrastructure stakeholders [1] [2]. Resiliency is variously characterized or defined. For space systems, the following definition has been articulated:

“Resilience is the ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions. An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions and threats. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities.” [3] [4]

The cyber aspects of space systems, and the importance of considering cyber resiliency for space systems, are increasingly recognized [5] [6]. Because space systems can be viewed as SoS<sup>1</sup>, the ways cyber – as well as non-cyber – resiliency techniques apply to SoS, and the challenges related to resilience in SoS, are highly relevant.

This white paper describes how resiliency techniques apply to an acknowledged SoS. In the following section, key concepts and definitions are presented, extending MITRE’s cyber resiliency engineering framework<sup>2</sup>. The next section provides an overview of how resiliency techniques could apply in SoS. The final section provides analysis of how each resiliency techniques could apply in an acknowledged SoS and corresponding challenges.

---

<sup>1</sup> A space system typically includes a space segment, a ground segment, communications links, and (transiently) a launch vehicle [28]. While these can be viewed as subsystems of a single system, they can also be viewed as constituents of a system-of-systems (typically a directed SoS; see descriptions of types of SoS below). See, for example, [31] [32]; alternately, the collection of all space systems (or all space systems under the auspices of a single enterprise) can be viewed as a SoS [33].

<sup>2</sup> See [11], which is used in [6]. The DoD Cyber Resiliency Framework [16] uses the same goals (Anticipate, Withstand, Recover, Evolve); the set of methods largely corresponds to the set of techniques.



## 2 Key Concepts and Terminology

This section provides background on systems-of-systems and the resilience framework.

### 2.1 Systems-of-Systems

A *system-of-systems* is “a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities”, where a *system* is “a functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements; that group of elements forming a unified whole” [7]. The Air Force defines a *capability* as:

“A capability is the combined capacity of personnel, materiel, equipment, and information in measured quantities, under specified conditions, that, acting together in a prescribed set of activities can be used to achieve a desired output.” [8]

For purposes of the discussion below, a SoS is made up of *constituent* systems. A unified set of services (e.g., identity management and authentication services), a major application, a network, or a network segment can constitute a system.

The DoD acquires a wide variety of types of System of Systems. The DoD Defense Acquisition Guidebook [9] recognizes the following four SoS types:

- **Virtual SoS** – A virtual SoS lacks a central management authority and a centrally agreed upon purpose for the system-of-systems. Large-scale behavior emerges, and although it may be desirable, this type of SoS must rely upon relatively invisible mechanisms to maintain it.
- **Collaborative SoS** – In a collaborative SoS, the constituent systems interact more or less voluntarily to fulfill agreed upon central purposes. The Internet is a collaborative system. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.
- **Acknowledged SoS** – An acknowledged SoS has recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches. Changes in the systems are based on collaboration between the SoS and the system.<sup>3</sup>
- **Directed SoS** – A directed SoS is one in which the integrated SoS is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The constituent systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose.

Because the constituent systems in an acknowledged SoS retain their independence, agreements are made between or among system owners. These can cover such topics as the use of shared SoS resources (such as test and evaluation (T&E) facilities), the coordination of SoS-related activities (e.g., integration or interoperability T&E), the performance of the SoS or of constituent systems (which can include Service Level Agreements (SLAs)), technical constraints on the SoS itself and its constituents (e.g., interface agreements), funding for SoS activities, and SoS process

---

<sup>3</sup> For more on acknowledged SoS, see [27] [26].

constraints (e.g., the use of specific tools). For purposes of the discussion below, agreements on such topics are referred to as *governance agreements*. Governance agreements can – and should – establish authority and accountability for resolving conflicts among different stakeholders (e.g., different Program Executive Offices (PEOs) or mission owners), as well as accountability for decisions or actions that affect constituent systems other than the one over which a stakeholder has authority.

## 2.2 Considerations for Space Systems

Some of the unique characteristics of space systems make resilience -- and system of systems resilience -- both challenging and important. The operating environment for the space vehicle (or constellation of vehicles) and payloads imposes constraints on power and size, and hence processing and storage [10]. In addition, the space vehicle operates in a limited-connectivity environment, i.e., one in which bandwidth is limited or in which constituent systems or sub-systems periodically operate without connectivity (“disconnected operations”). These characteristics are common to SoS that include tactical or mobile components. Unlike many tactical or mobile systems, however, the operating location of the space vehicle creates challenges for maintainability or sustainability, “identifying in advance the parameters that must be monitored, including the most likely failure modes and their effects on the system.” [10] These challenges become more complex when the threat model must include not only faults, accidents, natural events, and errors, but also deliberate and sustained attacks [5] [6].

## 2.3 Cyber Resiliency

Resiliency, particularly in the face of advanced cyber threats, is of increasing interest to military and critical infrastructure stakeholders [4] [5]. Resiliency is variously characterized or defined. For space systems, the following definition has been articulated:

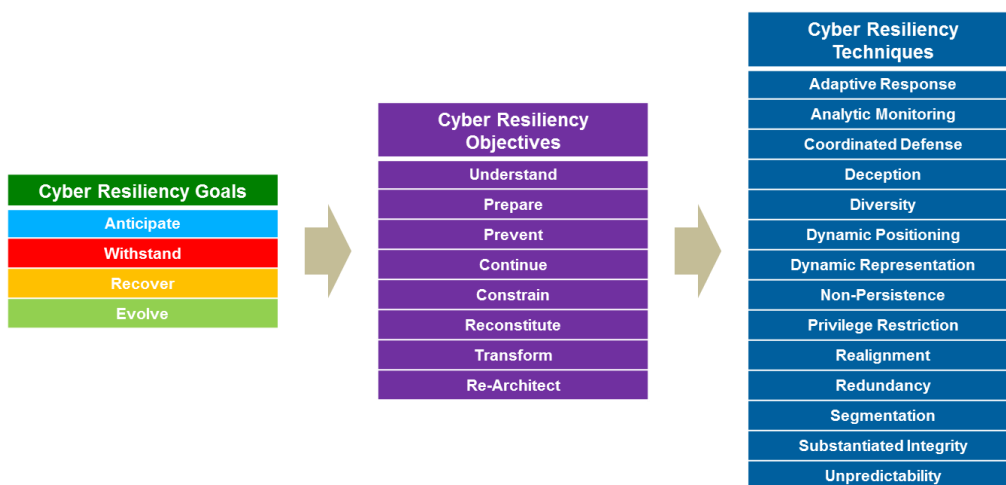
“Resilience is the ability of an architecture to support the functions necessary for mission success in spite of hostile action or adverse conditions. An architecture is "more resilient" if it can provide these functions with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions and threats. Resilience may leverage cross-domain or alternative government, commercial, or international capabilities.” [5] [7]

MITRE’s cyber resilience engineering framework (CREF) [11] draws from frameworks and taxonomies in the disciplines of resilience engineering [12] [13], network resilience [14], fault-tolerant and intrusion tolerant systems, and systems resilience in critical infrastructures<sup>4</sup>. While the CREF focuses on cyber, its derivation enables it to be extended (1) to extend the set of possible threat sources to include natural events and errors as well as adversarial actions; (2) to extend the set of adversarial actions to include non-cyber attack vectors; and (3) to consider cyber-physical as well as purely cyber systems.

As illustrated in Figure 1, the CREF consists of resiliency goals, objectives, and techniques. The framework of cyber resiliency goals, objectives, and techniques is intended to map the cyber resiliency solution space. Overlapping regions on a map (e.g., states, watersheds) are to be expected. In addition, the geography continues to change, as threats evolve and new resilience-related technologies transition from research to operational use.

---

<sup>4</sup> For more information on these frameworks and how the MITRE cyber resiliency engineering framework relates to them, see Appendix B of [11]. For the relationship between the CREF and survivability, see the Appendix to this white paper.



**Figure 1. Cyber Resiliency Engineering Framework**

The framework organizes the cyber resiliency domain into a set of goals, objectives, and techniques. Goals are high-level statements of intended outcomes. They help scope the cyber resiliency domain. Objectives are more specific statements of intended outcomes, to serve as a bridge between techniques and goals. They are expressed so as to facilitate assessment; it's straightforward to develop questions of "how well" or "how quickly" or "with what degree of confidence or trust" can each objective be achieved. They enable different stakeholders to assert their different priorities, based on mission.

Developing assessment-motivated questions leads to identifying sub-objectives, and activities that cyber defenders or systems engineers perform to achieve those sub-objectives. (See Appendix A of [15]. They, like the techniques, are expected to change over time.) These are also useful to articulate the relationship between techniques and goals.

An objective can be identified with a single goal but may support achieving multiple goals. The sub-objectives help show how this many-to-many relationship comes about. For example, the Continue objective primarily supports the Withstand goal. However, one of the sub-objectives of Continue is Ensure that functioning is correct; this also supports Recover. The main example of an objective that supports multiple goals is Understand – it supports all the goals. The Understand adversaries sub-objective supports Anticipate; the Understand status sub-objective supports Withstand and Recover; and the Understand dependencies sub-objective supports Withstand, Recover, and Evolve.

Cyber resiliency techniques are ways to achieve one or more cyber resiliency objectives that are applied to the architecture or design of mission/business functions and the cyber resources that support them. Techniques are selectively applied to the architecture or design of mission/business functions and the cyber resources that support them to achieve objectives; a given technique usually supports multiple objectives but may be unique to a single objective. The expectation is that the set of cyber resiliency techniques will change over time, as research in some of them fails to prove out, as others become standard cybersecurity or COOP practice, and as new research ideas emerge.









The CREF is deliberately incomplete: Objectives and techniques that relate to organizational resilience or business continuity in the face of non-cyber threats (e.g., natural disaster, human error) are not included. The CREF assumes a good foundation of cybersecurity and continuity of

operations (COOP), as described in the security control baselines in NIST SP 800-53 Rev. 4. For resilience against a broader set of threats, and to ensure relevance to space SoS, the CREF is extended as shown in Tables 1-3.

**Table 1. Resiliency Framework for Space SoS: Goals**

Goal	Description	Notes
<b>Anticipate</b>	Maintain a state of informed preparedness in order to forestall compromises of mission function from potential adverse conditions	Adverse conditions include, but are not limited to, adversary attacks. Corresponds to Avoidance in [4].
<b>Withstand</b>	Continue essential mission functions despite adverse conditions	Adverse conditions include, but are not limited to, successful execution of an attack by an adversary. Corresponds to Robustness in [4].
<b>Recover</b>	Restore mission functions during and after the adverse conditions	Adverse conditions include, but are not limited to, successful execution of an attack by an adversary. Corresponds to Reconstitution and aspects of Recovery in [4].
<b>Evolve</b>	Change mission functions and/or supporting capabilities, so as to minimize adverse impacts from actual or predicted adverse conditions	Adverse conditions include, but are not limited to, successful execution of an attack by an adversary. Corresponds to aspects of Recovery in [4].

**Table 2. Resiliency Framework for Space SoS: Objectives**

Objective	Description	Notes	Goals Supported
<b>Understand</b>	Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity	Removed “cyber” modifier for dependencies and resources; “adversity” rather than “adversary activities”	
<b>Prepare</b>	Maintain a set of realistic courses of action that address predicted or anticipated adversity	Removed “cyber” modifier for courses of action (CoAs); “adversity” rather than “cyber attacks”	
<b>Prevent / Avoid</b>	Preclude successful execution of attack or the realization of adverse conditions	Added “Avoid” to the name of the objective; for threats other than an advanced cyber adversary, avoidance may be a realistic objective Removed “on a set of cyber resources”; added “or the realization of adverse conditions”	
<b>Continue</b>	Maximize the duration and viability of essential mission functions during adverse conditions	“Adverse conditions” rather than “an attack”	
<b>Constrain</b>	Limit damage from adverse conditions	“Adverse conditions” rather than “an adversary’s attacks”	
<b>Reconstitute</b>	Redeploy resources to provide as compete a set of mission functionality as possible subsequent to adverse conditions	Removed “cyber” modifier for resources; “adverse conditions” rather than “an attack”	
<b>Transform</b>	Change aspects of organizational behavior in response to prior, current or prospective adverse conditions or attack	Added “adverse conditions”	
<b>Re-architect</b>	Modify architectures for improved resilience	Replaced “cyber resiliency” with “resilience”	

**Table 3. Resiliency Framework for Space SoS: Techniques**

Technique	Description	Notes	Capabilities or Approaches
<b>Adaptive Response</b>	Respond appropriately and dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, in order to limit consequences and avoid destabilization, taking preemptive action where appropriate	Extended to apply to situations other than attack; identifies concern for consequence limitation and stability; includes preemption Corresponds to Adaptive Management & Response in [16]	Dynamic Reconfiguration Dynamic Resource Allocation Dynamic Composability
<b>Analytic Monitoring</b>	Continuously gather, fuse, and analyze data to use threat intelligence, identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage	“Continuous” rather than “on an ongoing basis”; “adverse conditions” rather than “adversary activities”; added “use threat intelligence” Corresponds to Detection/Monitoring in [16]	Monitoring and Damage Assessment Sensor Fusion and Analysis Malware and Forensic Analysis
<b>Coordinated Defense</b>	Coordinate multiple, distinct mechanisms (defense-in-depth) to protect critical resources, across subsystems, layers, systems, and organizations	Emphasis on coordination rather than management; “protect” rather than “defend against adversary activities” Management aspect covered by Adaptive Management & Response in [16]	Defense-in-Depth Coordination and Consistency Analysis Adaptive Management
<b>Deception</b>	Confuse, deceive and mislead the adversary	Removed mention of specific approaches (obfuscation and misdirection) Included in Randomness / Unpredictability / Deception in [16]	Obfuscation Dissimulation / Disinformation Misdirection / Simulation
<b>Diversity</b>	Use a heterogeneous set of technologies, data sources, processing locations, and communications paths to minimize common mode failures (including attacks exploiting common vulnerabilities)	“Minimize common mode failures (including attacks exploiting common vulnerabilities)” rather than “minimize the impact of attacks and force adversaries to attack multiple different types of technologies” Part of Diversity & Redundancy in [16]	Architectural Diversity Design Diversity / Heterogeneity Dynamic or Synthetic Diversity Information Diversity
<b>Dynamic Positioning</b>	Distribute and dynamically relocate functionality and assets	Added “functionality”; removed reference to “processing”; treat sensors as a type of asset Corresponds to Distribution & Moving Target Defense in [16]	Functional Relocation Asset Mobility Distributed Functionality
<b>Dynamic Representation</b>	Support mission situation awareness and response by using dynamic representations of components, systems, services, adversary activities and other adverse situations, and effects of alternative courses of action	Added emphasis on mission situation awareness; included “other adverse conditions”; removed “cyber” modifier of CoA Included in Detection/Monitoring in [16]	Dynamic Mapping and Profiling Dynamic Threat Modeling Mission Dependency and Status Visualization Course of Action (CoA) Analysis

Technique	Description	Notes	Capabilities or Approaches
<b>Non-Persistence</b>	Retain information, services, and connectivity for a limited time, thereby reducing exposure to corruption, modification, or usurpation	Replaced “an adversary’s opportunity to exploit vulnerabilities and establish a persistent foothold” with “exposure to corruption, modification, or usurpation” Corresponds to Reset for Non-Persistence in [16]	Non-Persistent Information Non-Persistent Services Non-Persistent Connectivity
<b>Privilege Restriction</b>	Design to restrict privileges assigned to users and cyber entities, and to set privilege requirements on resources based on criticality	Removed details related to cyber Corresponds to Least Privilege in [16]	Privilege Management Privilege-Based Usage Restrictions
<b>Realignment</b>	Enable resources to be aligned (or realigned) with core mission functions, thus reducing the attack surface, the potential for unintended consequences, and the potential for cascading failures	Added potential for unintended consequences and cascading failures Not included in [16]	Purposing Offloading / Outsourcing Agility / Repurposing
<b>Redundancy</b>	Provide multiple protected instances of critical information and resources, to reduce the consequences of loss	Added “to reduce the consequences of loss” Part of Diversity & Redundancy in [16]	Backup and Restore Surplus Capacity Replication
<b>Segmentation / Separation</b>	Separate (logically or physically) components based on criticality and trustworthiness, to limit the spread of damage	Added “Separation” to the name Removed “from successful exploits” Corresponds to Separation/Isolation in [16]	Modularity / Layering Predefined Segmentation Dynamic Segmentation / Isolation
<b>Substantiated Integrity</b>	Provide mechanisms to ascertain whether critical services, information stores, information streams, and components have been corrupted	Removed “by an adversary” Corresponds to Integrity Checks in [16]	Integrity / Quality Checks Provenance Tracking Behavior Validation
<b>Unpredictability</b>	Make changes, frequently and randomly, to make the attack surface unpredictable	No changes; Unpredictability is useful solely in the face of an adversary Included in Randomness / Unpredictability / Deception in [16]	Unpredictable Behavior

**Table 4. Mapping Cyber Resiliency Techniques to Objectives**

	Understand	Prepare	Prevent	Constrain	Continue	Reconstitute	Transform	Re-Architect
<b>Adaptive Response</b>				X	X	X		
<b>Analytic Monitoring</b>	X	X		X		X		
<b>Coordinated Defense</b>		X	X	X	X	X		
<b>Deception</b>	X		X		X			
<b>Diversity</b>			X		X			X
<b>Dynamic Positioning</b>	X		X		X			X
<b>Dynamic Representation</b>	X	X					X	
<b>Non-Persistence</b>			X	X	X			X
<b>Privilege Restriction</b>			X	X				
<b>Realignment</b>				X			X	
<b>Redundancy</b>					X	X		
<b>Segmentation</b>			X	X				
<b>Substantiated Integrity</b>	X			X	X	X		
<b>Unpredictability</b>	X		X		X			

### 3 How Resiliency Techniques Can Apply in an Acknowledged SoS

This section provides an overview of how resiliency techniques could apply in an acknowledged SoS.

#### 3.1 Resiliency Techniques in SoS Operations

As illustrated in Figure 2, the resiliency techniques focus on providing system-of-systems resilience in support of mission resilience<sup>5</sup>. Some resiliency techniques (Coordinated Defense and Dynamic Representation) provide capabilities that bridge between system/SoS operations and mission operations. The concept of operations (CONOPS) for a SoS depends on the mission(s) (and, potentially, the additional business functions) it supports. However, the overarching goal of resilient mission operations creates a need for resilient operations of the SoS and, to a lesser extent, of constituent systems. Thus, some resiliency techniques (Adaptive Response, Analytic Monitoring, and active forms of Deception) provide capabilities for resilient SoS operations. Finally, the remaining resiliency techniques provide supporting functionality to those that support resilient SoS operations<sup>6</sup>.

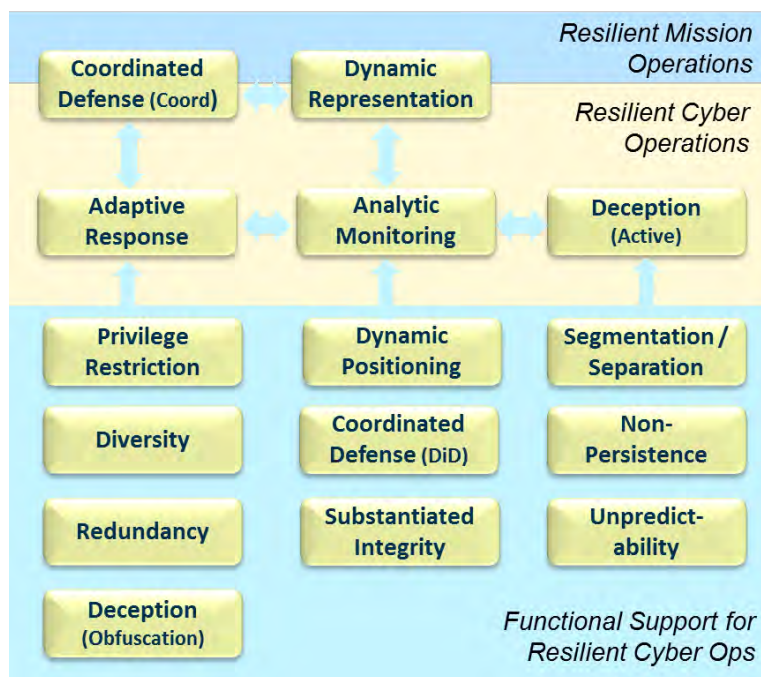


Figure 2. Resiliency Techniques in Operational Context

Resilient SoS operations entails the following processes for using the resiliency techniques:

1. As part of Coordinated Defense, SoS Courses of Action (SCoAs) are defined. A SCoA identifies actions to change how the SoS or selected constituent systems will be used or

<sup>5</sup> Mission resilience techniques that do not involve anticipating, withstanding, or recovering from undesirable changes in the behavior of the SoS or its constituents, or evolving SoS or constituent capabilities, are outside the scope of this paper. For example, mission resilience techniques can include investments in human capital or changes in governance [34].

<sup>6</sup> All the techniques in the bottom blue box can be used by Adaptive Response. Dynamic Positioning and the Defense-in-Depth aspect of Coordinated Defense support Analytic Monitoring as well as the active aspect of Deception. The active aspect of Deception also can use Substantiated Integrity, Segmentation / Separation, Non-Persistence, and Unpredictability.



defended, taking into consideration mission contingencies as well as the capabilities of constituent systems. SCoAs are coordinated across mission owners, cyber defenders at different tiers<sup>7</sup>, and the owners/operators of constituent systems.

2. Analytic Monitoring (possibly informed by Deception and Dynamic Representation) produces a trigger for responsive action. For a SoS, Dynamic Representation provides current situational awareness (SA) of constituent systems and capabilities to support mission SA, relying on data provided by Analytic Monitoring capabilities at the SoS level (in turn relying on Analytic Monitoring capabilities of constituent systems).
3. In Adaptive Response, a SCoA, which can make use of a combination of other techniques, is selected and executed. Depending on how the SoS as a mission resource is managed and defended, together with how the constituent systems are managed and defended, a SCoA could be directed or coordinated from a higher-level tier than the constituent systems (e.g., from a Joint Operations Center (JOC) or a Joint Cyber Center (JCC)<sup>8</sup>), or could consist of activities on constituent systems coordinated either formally or informally.
4. The selected SCoA can involve active Deception, which can make use of a combination of such techniques as Segmentation (for a Deception environment), Non-Persistence, Unpredictability, and Dynamic Positioning.
5. Analytic Monitoring can make use of Dynamic Positioning and the Defense-in-Depth element of Coordinated Defense, either as part of a SCoA or as part of an everyday CONOPS.

## 3.2 Opportunities and Challenges for Emergent Resiliency

Resilience can be an emergent property [17] [18]. By definition systems-of-systems is that they display emergent properties and behaviors. The question arises: In what ways can resilience be an emergent property in SoS?

This question can be made more specific, using the resilience framework. Which resilience techniques (or which capabilities or approaches to applying those techniques) are (or can be) artifacts or products of bringing together constituent systems into an acknowledged SoS? What opportunities emerge for applying techniques at the SoS level? Which techniques must be produced deliberately? In the following, “deliberate efforts” refer to efforts by Program Managers and owners/operators of constituent systems, cyber defenders at all tiers, and mission owners, to reach governance agreements, make common architectural decisions, and ensure operational coordination and cooperation, based on engineering analysis of how the constituent systems interact in the SoS as it evolves over time.

Analysis, presented in detail in the next section and summarized in the table below, indicates that

- Relatively few techniques arise purely as artifacts of bringing together constituent systems into an acknowledged SoS. These are Diversity, Redundancy, and some aspects

---

<sup>7</sup> DoD Computer Network Defense (CND) is organized into three tiers: Tier I (Global), Tier II (Regional/Theater), and Tier III (Local). For a SoS, Tier II is most relevant; however, activities at Tier II must be coordinated with Tiers I and III. See [29].

<sup>8</sup> See [30] for a description of USTRANSCOM’s JCC.

of Segmentation and Substantiated Integrity. Deliberate efforts can make these emergent resilience techniques more effective.

- The acknowledgement of a SoS creates opportunities for applying most techniques at the SoS level. Deliberate efforts are needed to capitalize on SoS-level opportunities. These include Adaptive Response, Analytic Monitoring, Dynamic Positioning, Non-Persistence, Privilege Restriction, some aspects of Segmentation and Substantiated Integrity, and Unpredictability.
- A few techniques are most effective at the SoS level, but require deliberate efforts before they can be applied at all. These are Coordinated Defense, Deception, Dynamic Representation, and Realignment.

**Table 5. Opportunities and Challenges for Emergence of Resiliency**

Technique	Opportunities and Challenges for Emergence
<b>Adaptive Response</b>	<p>Opportunities arise for dynamic reconfiguration, dynamic reallocation, and dynamic composability at the SoS level: The information and control flows among constituent systems can be changed, responsibilities for providing functionality can be reassigned, and constituent systems can be added to provide capabilities in alternate ways.</p> <p>Deliberate efforts are needed to capitalize on these opportunities, identifying new alternatives as they arise, and finding ways to use alternative capabilities in a non-disruptive way.</p>
<b>Analytic Monitoring</b>	<p>Opportunities arise for developing threat intelligence about adversary behavior that spans constituent systems, and for identifying interactions or dependencies among constituent systems that could indicate destabilization or disruption before it affects mission performance.</p> <p>Deliberate efforts are needed to capitalize on these opportunities, i.e., to establish monitoring and analysis at the SoS level, to share and fuse information, and to define roles and responsibilities for malware and forensic analysis.</p>
<b>Coordinated Defense</b>	<p>Coordinated Defense is most effective at the SoS level: The SoS can be defended as a whole, rather than defense being performed on a system-by-system basis, with possible destabilizing effects on the SoS.</p> <p>Deliberate efforts are vital to provide ongoing coordination – to define and execute courses of action that span constituent systems, and that ensure continued mission capabilities in the presence of adverse events.</p>
<b>Deception</b>	<p>Deception is most effective at the SoS level: Deception environments that mirror the SoS as a whole (or sub-networks or enclaves) can provide insight into adversary tactics, techniques, and procedures (TTPs) and strategies.</p> <p>Deliberate efforts – including ongoing investment of time and effort to keep deception environments fresh while providing adequate OPSEC – are vital.</p>
<b>Diversity</b>	<p>Diversity (typically in conjunction with Redundancy) is an artifact of the creation of an acknowledged SoS. Constituent systems are acquired by different organizations, possibly using different SDLC models and/or technical standards, in varying timeframes. Therefore, even when constituent systems share requirements, those requirements will be met in different ways.</p> <p>Deliberate efforts are needed to capitalize on this incidental diversity, rather than for it to be a barrier to interoperability.</p>
<b>Dynamic Positioning</b>	<p>Opportunities arise for distribution of processing, storage, or communications across constituent systems. Opportunities also arise for dynamically relocating capabilities or critical assets from one constituent system to another.</p> <p>Deliberate efforts are needed to capitalize on these opportunities, to provide interoperability and consistent interfaces.</p>

Technique	Opportunities and Challenges for Emergence
<b>Dynamic Representation</b>	Dynamic Representation is most effective at the SoS level: Situation Awareness (SA) of which resources are currently or prospectively mission-critical, as well as the status of those resources, can support mission execution and planning. Deliberate efforts to create a SoS-level (and corresponding mission-level) representation are vital.
<b>Non-Persistence</b>	Opportunities arise for non-persistent services, connectivity, and information: Insofar as needs for these can be met in the SoS in multiple ways, removing and reconstituting capabilities becomes less problematic to users. Deliberate efforts are needed to identify and address governance and operational problems.
<b>Privilege Restriction</b>	Opportunities arise for the use of federated identity and privilege management systems / services, so that privileges can be defined and restricted in a consistent manner across the SoS. Deliberate efforts are needed to agree on federated services and how they will be used.
<b>Realignment</b>	Realignment is most effective at the SoS level: Constituent systems can be defined, and functionality allocated to them, based on such risk factors as mission criticality, information sensitivity, and security and performance characteristics. Deliberate and ongoing efforts are vital, particularly since constituent systems – and the mission uses of constituent systems – change over time.
<b>Redundancy</b>	Redundancy (typically in conjunction with Diversity) is an artifact of the creation of an acknowledged SoS. Constituent systems are acquired by different organizations, in varying timeframes, frequently to provide similar capabilities. In addition, as the SoS evolves over time, connectivity and functional dependencies among constituent systems can accrete. Deliberate efforts are needed to capitalize on this incidental redundancy, and to guard against the possibility that it provides unrecognized avenues for cyber attack.
<b>Segmentation</b>	Some Segmentation can be a result of acknowledging a SoS (e.g., sets of constituent systems limiting their traffic with others based on sensitivity). Opportunities arise for dynamic definition of virtual enclaves based on mission priorities, and for dynamically isolating segments of the SoS in response to indications of adversity. Deliberate efforts are needed to ensure that applications of Segmentation are – and remain – consistent with mission needs and with how the constituent systems are used to meet those needs as they evolve.
<b>Substantiated Integrity</b>	Behavior Validation can emerge at the SoS level: Constituent systems can observe their interactions with each other, and provide warnings of unexpected behavior by a constituent system that could indicate adverse conditions. Deliberate efforts are needed to ensure that mission operators and cyber defenders are notified, rather than having automated responses to unexpected behavior go unrecognized until a failure occurs. Opportunities for other Substantiated Integrity capabilities arise at the SoS level: Data quality (including integrity) can be evaluated and tracked, and provenance determined, to improve the correctness and effectiveness of data-driven decisions. Deliberate efforts are needed to ensure that meta-data is defined and handled consistently.
<b>Unpredictability<sup>9</sup></b>	Opportunities arise for Unpredictability at the SoS level, by taking advantage of redundant and diverse implementations of capabilities. Deliberate efforts are needed to capitalize on such opportunities, so that changes in the configuration or use of the SoS can be made randomly or unpredictably without causing instability or undermining mission capabilities.

<sup>9</sup> Note that Unpredictability as a resilience technique is intended to make an adversary's job harder. While emergent behavior in a SoS can become knowable only by observing the SoS, rather than from analysis of the constituent systems, that is not the meaning of Unpredictability used here.

## 4 Detailed Analysis

This section provides a more detailed analysis of how resiliency techniques could apply in SoS operations. For each technique, capabilities used in – or approaches to – implementing the technique are identified.<sup>10</sup> For each capability or approach, a brief description is given of how it applies to SoS, and what challenges could arise. A summary is provided, together with identification of synergies among cyber resiliency techniques. Finally, the relationship between the cyber resiliency techniques and disaggregation for space systems is discussed.

### 4.1 Applicability of Specific Cyber Resiliency Techniques

#### 4.1.1 Adaptive Response

Adaptive Response techniques enable systems and organizations to *respond appropriately and dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, in order to limit consequences and avoid destabilization, taking preemptive action where appropriate*. More specifically, Adaptive Response involves selecting, executing, and monitoring the effectiveness of the CoA that best changes the attack surface, maintains critical capabilities, and restores functional capabilities. Capabilities that support Adaptive Response include Dynamic Reconfiguration, Dynamic Resource Allocation, Dynamic Composability, and Preemptive Action.<sup>11</sup> In a SoS, these capabilities can be instantiated by component systems, either with operator/administrator intervention or via pre-established automated response to contingencies.

**Table 6. Adaptive Response in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Dynamic Reconfiguration: Make changes to an element or component while it continues operating.</b>	A component system or network segment responds to indications that another component system or network segment on which it relies is unavailable or responding slowly by routing requests or traffic to an alternate.	<p>The component system or network needs to be able to sense service unavailability or degradation, to identify alternative sources of needed functionality / connectivity, and to be authorized to use the alternate.</p> <p>If the alternate uses different protocols or interface standards, traffic or requests must be translated.</p> <p>Alternates need to conform with existing service-level agreements (SLAs), which can deprecate the request or traffic.</p>

<sup>10</sup> More information on these capabilities and approaches can be found in Appendix D of [15].

<sup>11</sup> A preemptive action forestalls or prevents something from happening; that is, it is taken in anticipation of the undesired event or action. Here, preemption is aimed at the effects of potential adversary activities, and is used in the sense of a preemptive strike against a military or cyber adversary. Others use “preemption” more broadly, in the sense of proactive rather than reactive behavior [23]. In cyberspace, some forms of preemptive actions, including proactive actions within organizationally owned systems and in some cases preemptive strikes on adversary-controlled systems, are referred to as active cyber defense. Preemption may not be a valid intended effect, depending on policy, legal, regulatory, or other organizational considerations; uncertainties arise specifically related to active cyber defense [24].

Capability/Approach	Application to SoS	SoS Challenges
	A component system or network segment responds to indications that another component system or network segment, on which it relies, may be compromised by routing requests or traffic to an alternate.	Malware latent on the component system (propagated from the system suspected of being compromised) can be further propagated. The alternate may be overwhelmed by requests or traffic. (This could even be the intended effect of the initial compromise.)
<b>Dynamic Resource Allocation: Change the allocation of resources to tasks or functions without terminating functions or processes.</b>	A component system or network changes the relative priority assigned to a mission task, service request, or traffic to / from a set of participant systems / services.	The component system or network needs to conform with existing SLAs.
<b>Dynamic Composability: Replace software elements with equivalent functionality without disrupting service.</b>	The implementation of a set of services, collectively offered by multiple systems, is altered by swapping out different implementations.	Alternate implementations need to provide equivalent functionality and consistent interfaces. Component systems may have different criteria for replacement, due to governance differences.
<b>Preemptive Action: Destroy, damage, or make unavailable/inaccessible adversary resources.</b>	Resources that an adversary could use to cause mission impacts are destroyed, damaged, or made unavailable.	Policy, legal, regulatory, and/or other organizational considerations such as reputation or relationships.

## 4.1.2 Analytic Monitoring

Analytic Monitoring techniques *continuously gather, fuse, and analyze data to use threat intelligence, identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage.* Capabilities that support Analytic Monitoring include Monitoring and Damage Assessment, Sensor Fusion and Analysis, and Malware and Forensic Analysis.

**Table 7. Analytic Monitoring in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Monitoring and Damage Assessment: Behavior and characteristics of elements are monitored and analyzed to look for indicators of adversary activity, detect and assess damage,<sup>12</sup> and watch for adversary activities during recovery and evolution.</b>	A component system or network segment monitors the behavior of connected systems or networks to maintain a current assessment of their availability, performance, and health.	Component system/network owners may be concerned about the correctness and confidentiality of assessments made by other systems/networks. Incorrect assessments can lead to false claims of breach of SLAs or false accusations of compromise. Unauthorized disclosure of assessments can result in reputation damage.

<sup>12</sup> For cyber systems, damage assessment involves analysis of behavior, data, and system artifacts to determine the presence and extent of damage.

Capability/Approach	Application to SoS	SoS Challenges
	A component system or network segment monitors its own status to find indications of potential adverse conditions and identify potential or actual damage. It shares status information with other component systems and/or network segments.	Concerns about confidentiality of information shared with other systems/networks. Unauthorized disclosure of assessments can result in reputation damage.
<b>Sensor Fusion and Analysis: Monitoring data and preliminary analysis results from different elements are fused and analyzed, together with externally provided threat intelligence, to look for indicators of adversary activity that span elements; to identify attack trends; and (in conjunction with Malware and Forensic Analysis) to develop threat intelligence.</b>	Performance and security monitoring data from multiple systems and network segments is shared with, fused by, and analyzed by a regional, sector-wide, national, or multinational operations center.	Data interoperability standards are needed. Component system/network owners may have different policies about information sharing, particularly with respect to vulnerability and damage data. Big data analytics could reveal patterns of usage that could be exploited by an adversary, or by a partner seeking a competitive advantage.
<b>Malware and Forensic Analysis: Malware and other artifacts left behind by adversary activities are analyzed to develop observables, indicators, and adversary tactics, techniques, and procedures (TTPs).</b>	Malware and other data from suspected or confirmed intrusions are shared with, and analyzed by, a cyber threat analysis cell or center (CTAC). Indicators and signatures developed by the CTAC are shared with component systems and networks.	Component system/network owners may have different policies about sharing contextual information, the absence of which could decrease the utility of CTAC analysis.

### 4.1.3 Coordinated Defense

Coordinated Defense techniques *coordinate multiple, distinct mechanisms to protect critical resources, across subsystems, layers, systems, and organizations*. A key approach is Technical Defense-in-Depth, while capabilities that support Coordinated Defense include Coordination and Consistency Analysis, and Adaptive Management.<sup>13</sup>

<sup>13</sup> As the inclusion of Adaptive Management as a Coordinated Defense capability suggests, Coordinated Defense and Adaptive Response are closely related. However, Adaptive Response is oriented toward making changes in response to indications that an attack is underway, and may use mechanisms that are not conventionally viewed as defensive (e.g., Dynamic Composability, Dynamic Reallocation). Coordinated Defense has more to do with using defensive mechanisms effectively, in a considered and coordinated way. It therefore has a strong planning element (defining, coordinating, and exercising cyber courses of action). While Adaptive Response can include execution of a cyber course of action, it can also include taking actions that have not been planned or coordinated in advance.

**Table 8. Coordinated Defense in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<p><b>Technical Defense-in-Depth: Make use of multiple protective mechanisms, applied at different architectural layers or locations.</b></p>	<p>Component systems and network segments employ multiple and distinct protective mechanisms.</p>	<p>Increased cost of development and testing. Increased complexity of management, training, and maintenance.</p>
	<p>The set of protective mechanisms varies across component systems and network segments.</p>	<p>Increased cost to ensure and test interoperability. Increased complexity of management, training, and maintenance; experience on one system does not necessarily apply to another. Need for data interoperability standards for data related to protection mechanisms.</p>
<p><b>Coordination and Consistency Analysis: Apply 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.</b></p>	<p>Operators, administrators, and managers of component systems coordinate to ensure that defenses are defined and implemented consistently across component systems and networks.</p>	<p>Governance: How can policy conflicts be resolved? Increased cost (time and effort) of coordination.</p>
	<p>Cyber courses of action are defined jointly by operators, administrators, and managers of component systems; cyber defenders at different tiers; and mission owners.</p>	<p>Governance: How can equities be respected, particularly as mission needs change over time? Increased cost (time and effort) of coordination.</p>
	<p>Changes (e.g., addition of capabilities, changes in configuration, software updates, hardware refreshes) to component systems and network segments are analyzed to ensure that interoperability is preserved, and that a disruption (e.g., attack, accident) that involves one defensive mechanism or one component system or network segment does not negate, degrade, or destabilize another.</p>	<p>Increased cost (time, effort, specialized expertise) to analyze and test changes. Insufficient knowledge of how other component systems will respond to changes in a component system, due to unidentified functional or mission dependencies. Need for exercises that include disruptions.</p>
<p><b>Adaptive Management: Change how defensive mechanisms are used based on changes in the operational environment as well as changes in the threat environment.</b></p>	<p>Component systems and network segments change how defensive mechanisms are used (e.g., making configuration changes, turning on some mechanisms while turning off others, deciding when and how to update or patch software) based on changes in the operational environment (e.g., changes in mission/business needs or priorities), while maintaining consistency.</p>	<p>Need for exercises and visualization capabilities, to understand the relationship between (1) changes to component systems and network segments and (2) the effects of changes on mission capabilities.</p>

#### 4.1.4 Deception

Deception techniques confuse, deceive, or mislead the adversary. Capabilities include Obfuscation, Dissimulation and Disinformation, Misdirection, and Simulation.

**Table 9. Deception in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Obfuscation: Hide or otherwise obfuscate information from the adversary.</b>	Component systems and network segments employ encryption and data hiding mechanisms.	Synchronization and key management. Encrypting network traffic can impede monitoring and analysis.
	Programs and missions employ operations security in a coordinated way.	Need to provide cross-organizational or cross-mission guidance on what constitutes critical information. Need to ensure that information needed to support mission functions and/or cybersecurity operations is shared.
	Component systems perform repackaging or data transformations to obscure data or hide its provenance.	Mechanisms for recovering and tracking provenance of repackaged data will be needed to ensure authenticity and accountability.
<b>Dissimulation/Disinformation: Provide deliberately confusing responses to adversary requests.</b>	Component systems respond to (what are believed to be) adversary queries with deliberately confusing or erroneous information.	Mechanisms are needed to ensure correct responses to anomalous but authentic queries. Disinformation can confuse component systems or cause them to operate incorrectly.
<b>Misdirection/Simulation: Maintain deception resources or environments and direct adversary activities there.</b>	Deception environments (e.g., honeypots, honeynets) are included on component systems or networks.	Deception environments should be managed and analyzed by a CTAC. Coordination with owners/managers/administrators of component systems and networks is needed to ensure that the deception environment appears realistic and current, without revealing actual sensitive information, particularly about other component systems. Traffic from a component system can be erroneously diverted to a deception environment, causing it to be confused or to operate incorrectly.



## 4.1.5 Diversity

Diversity techniques *use a heterogeneous set of technologies, data sources, processing locations, and communications paths to minimize common mode failures (including attacks exploiting common vulnerabilities)*. Approaches include Architectural Diversity/Heterogeneity, Design Diversity/Heterogeneity, Dynamic or Synthetic Diversity, and Information Diversity.

**Table 10. Diversity in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Architectural Diversity/Heterogeneity:</b> Use multiple sets of technical standards, different technologies, and different architectural patterns.	Component systems and network segments conform to differing sets of technical standards, use different product suites, or follow different architectural patterns.	Interface standards, particularly standards for transforming message and data formats, must be defined and used consistently.  Note that architectural diversity/heterogeneity is often an unintended consequence of systems being acquired at different times, by different organizations, and/or to meet different mission needs.
	Different networks or network segments rely on different technologies (e.g., wired, wireless, radio frequency, satellite communication), and provide different communications paths.	Interface standards must be defined and used consistently. Component systems must be capable of interfacing with multiple networks.
<b>Design Diversity/Heterogeneity:</b> Use different designs to meet the same requirements or provide equivalent functionality.	For key components, multiple designs and implementations are developed independently.	Increased cost of development and testing. Increased complexity of management, training, and maintenance.
<b>Dynamic or Synthetic Diversity:</b> Transform implementations so that for no specific instance is the implementation completely predictable.	For key software elements (particularly those common to multiple component systems or network segments), implementations are transformed so that multiple variants are used; variants are dynamically created when software is instantiated/activated.	Increased cost of development and testing. Governance: Who determines which software elements should be subject to such techniques as instruction set randomization, address space randomization, and data space randomization?
<b>Information Diversity:</b> Provide information from different sources or transform information in	Different sources provide the same or equivalent information.	Mechanisms are needed to identify and track the provenance of information. Governance: Who decides how to handle alternate information? Different component systems can treat information of a given provenance differently, leading to inconsistencies. Mission CONOPS must take the provenance (and thus the trustworthiness, validity, and/or quality) of information into consideration.

## 4.1.6 Dynamic Positioning

Dynamic Positioning techniques *distribute and dynamically relocate functionality and assets*, thus changing the attack surface. Capabilities include Functional Relocation, Asset Mobility, and Distributed Functionality.

**Table 11. Dynamic Positioning in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Functional Relocation: The location that provides functionality is changed dynamically, to change the attack surface.</b>	Functionality (e.g., as provided by an executing process) is relocated from one system (or system component, in the case of a distributed system) or one network (or network segment) to another. For functionality provided by software, relocation typically leverages virtualization.	Component systems or networks that provide internal relocation of functionality provided or exposed to other components must provide mechanisms to make that relocation transparent to external components.
<b>Asset Mobility: Physical assets (e.g., platforms or vehicles, mobile computing devices) are physically relocated.</b>	Asset mobility applies primarily to assets within component systems. However, some component systems or network segments—particularly those identified with a mobile platform or vehicle—can be physically relocated as a whole.	Physical relocation can result in breaks in communications with or transient unavailability of capabilities provided by the assets. Asset interfaces, particularly management interfaces, must be designed and implemented to handle communications gaps and changes in communications paths. Mission threads must include alternatives for contingencies involving physical relocation.
	Information assets (e.g., data stores) associated with one platform or computing device (e.g., server, storage area network ) are transferred/relocated to another. This transfer can be internal to a component system, or can cross systems.	Mechanisms are needed to make the transfer transparent to external components. Latency or gaps in coverage must be addressed, typically by using some form of Replication.
<b>Distributed Functionality: Functionality (e.g., processing, storage, communications) is distributed across multiple elements.</b>	Functionality related to executing a mission thread spans components in a SoS (the set of component systems and networks is referred to as a mission segment in [19]), with different tasks assigned to different components.	Need to avoid single points of failure in mission threads. (This can involve redundant or replicated functionality in different component systems, or defining alternate mission threads that provide equivalent mission functionality. That is, in a SoS, Distributed Functionality is more effective when combined with Redundancy.)

## 4.1.7 Dynamic Representation

Dynamic Representation techniques *support mission situation awareness (SA) and response by using dynamic representations of components, systems, services, adversary activities and other adverse situations, and effects of alternative courses of action (including cyber courses of action)*. Capabilities include Dynamic Mapping and Profiling, Dynamic Threat Modeling, Mission Dependency and Status Visualization, and CoA Analysis.<sup>14</sup>

**Table 12. Dynamic Representation in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Dynamic Mapping and Profiling: Maintain current information about resources, their status, and their connectivity.</b>	Component systems and networks maintain current asset inventories and resource maps, which include patch status for software and firmware and configuration data about configurable elements. Relevant information is shared with other component systems/networks, or with an SA entity such as a Joint Cyber Center or with mission operators (e.g., via a Joint Operations Center [JOC]).	Component systems and networks can differ in terms of requirements for configuration, patching, and reporting. The results produced by different inventory, mapping, or scanning tools can differ in format and content (particularly level of detail). Information sharing can be problematic in tactical environments or other environments in which bandwidth or connectivity to component systems is limited.
<b>Dynamic Threat Modeling: Maintain current information about threat activities and characteristics (e.g., observables, indicators, TTPs).</b>	Component systems and networks capture threat information, analyze it locally, and share the results with other component systems/networks, with an SA entity, or with mission operators.	Lack of standards for capturing and sharing threat information. Note that for cyber threats, Structured Thread Information eXpression (STIX) [20] and Trusted Automated Exchange of Indicator Information provide standards; however, this is not the case for other types of threats. The relevance of threats identified by one component system to another, or to a specific mission, can be difficult to determine. Governance: Mission and system owners can have different risk tolerances, which influence what they perceive to be a threat.
<b>Mission Dependency and Status Visualization: Maintain current information about mission dependencies on resources, and the status of those resources with respect to threats.</b>	Mission operators (or those who support them, e.g., in a JOC) maintain a current visualization of the resources needed to execute current and future mission tasks, and of the status of those resources with respect to threats. This involves understanding mission dependencies on component systems and network segments, and often on elements within component systems.	Lack of standard approaches to identifying and visualizing mission dependencies. Within individual systems, mission dependencies are often captured in continuity of operations documentation. However, such documentation is typically static, quickly outdated, and poorly validated through exercises.

<sup>14</sup> As described in [25], cyber SA includes Network Awareness, Threat Awareness, and Mission Awareness. Dynamic Representation techniques extend cyber SA to include support for mission SA and response. Dynamic Mapping and Profiling capabilities provide Network Awareness; Dynamic Threat Modeling capabilities provide Threat Awareness; and Mission Dependency and Status Visualization capabilities provide Mission Awareness. Dynamic Representation supports mission response via CoA Analysis capabilities.

Capability/Approach	Application to SoS	SoS Challenges
<b>CoA Analysis: Maintain 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.</b>	Mission operators (or those who support them, e.g., in a JOC) identify and analyze the effects of alternative CoAs on mission effectiveness, taking into consideration effects on component systems and networks.	Lack of standard approaches to identifying and analyzing the effects of CoAs.

#### 4.1.8 Non-Persistence

Non-persistence techniques *retain information, services, and connectivity for a limited time, thereby reducing an adversary's opportunity to exploit vulnerabilities and establish a persistent foothold*. Capabilities include Non-Persistent Information, Non-Persistent Services, and Non-Persistent Connectivity.

**Table 13. Non-Persistence in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Non-Persistent Information: Information is refreshed to a known trusted state and deleted when no longer needed.</b>	<p>Except for archival storage of authoritative versions, information is removed from component systems and network devices when not in use; information is retrieved from authoritative sources (and refreshed by or combined with new information from sensors or users) only upon demand. A component system may be the source of all authoritative information, or authoritative information may be distributed across multiple component systems.</p> <p>Note that some Data Loss Prevention solutions have non-persistence effects, by making copies of information unusable or inaccessible after a specified time.</p>	<p>Requires analysis to determine what information needs to be archived. Note that in tactical environments (or other environments with low-bandwidth communications), an archiving strategy is required, to determine what information must be transmitted to the archive and how quickly, what information can be retained locally until high-bandwidth connectivity is available, and what information can be discarded.</p> <p>Default functionality in many components (e.g., routers, applications such as email) must be configured to conform with the archiving strategy; note that many applications retain multiple copies of data, increasing storage requirements as well as data exposure.</p> <p>Requires assured connectivity with archival storage to retrieve authoritative information. Therefore, component systems may need to maintain internal archives. Note that maintaining component-internal copies of information raises problems wotj data quality and lack of synchronization / consistency across SoS, as well as increasing risks of data compromise.</p> <p>Requires that component systems be able to locate authoritative information.</p>
<b>Non-Persistent Services: Services are refreshed periodically and/or terminated after completion of a request.</b>	Services (within a component system or network segment) are periodically refreshed, and/or are terminated after completion of a request and re-instantiated upon a new request.	Potential delays.

Capability/Approach	Application to SoS	SoS Challenges
<b>Non-Persistent Connectivity: Connections are terminated after completion of a request or after a period of non-use.</b>	Connections between component systems, or between applications or services running on component services, are terminated after completion of a request or after a specified period of non-use, and re-instantiated upon a new request.	Potential delays.

#### 4.1.9 Privilege Restriction

Privilege Restriction techniques *restrict privileges assigned to users and cyber entities, and set privilege requirements on resources based on criticality*. Capabilities include Privilege Management and Privilege-Based Usage Restrictions.

**Table 14. Privilege Restriction in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Privilege Management: Define, assign, and maintain privileges associated with end users and cyber entities (e.g., systems, services, devices), based on established trust criteria, consistent with principles of least privilege.</b>	Define, assign, and maintain privileges associated with end users and cyber entities in a consistent way across component systems.	Need mechanisms for identity resolution and/or resolution of other access- or privilege-related attributes across multiple systems; the use of multiple identifiers can complicate privilege management. In many circumstances, federated identity and privilege management systems can be used to provide needed functionality; however, these may not be useful in tactical environments (or other environments in which bandwidth or connectivity to such systems is limited). Governance: Because different mission and system owners can have different risk tolerances, trust criteria can differ across component systems. How will differences be identified and resolved? Agility: How can least privilege be enforced, given the possibility that mission needs will change? Can risk-adaptable access control mechanisms be used?
<b>Privilege-Based Usage Restrictions: Define, assign, maintain, and apply usage restrictions on cyber resources based on mission criticality and other attributes (e.g., data sensitivity).</b>	Define, assign, maintain, and apply usage restrictions on cyber resources based on mission criticality and other attributes in a consistent way across component systems.	Need to define criteria for usage restrictions that can be applied across component systems. Potential lack of agility/flexibility; the mission criticality of a resource can change dynamically.

#### 4.1.10 Realignment

Realignment techniques *enable resources to be aligned (or realigned) with core mission functions, thus reducing the attack surface, the potential for unintended consequences, and the potential for cascading failures*. Approaches include Purposing, Offloading/Outsourcing, and Agility/Repurposing.

**Table 15. Realignment for SoS**

Capability/Approach	Application to SoS	SoS Challenges
<p><b>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.</b></p>	<p>The mission purposes of functions, services (including connectivity as well as processing), information, and systems are identified, so they can be protected accordingly.</p>	<p>In an architecture with shared services or other shared resources, the mission purposes may not be known—or knowable—prior to actual mission use. In such cases, Segmentation, together with virtualization and Privilege Restriction mechanisms, can be used to define virtual systems or enclaves with different allowable purposes and corresponding protection profiles. Virtual systems or enclaves can be defined based on partnership relationships, with some enclaves shared with external mission partners and others restricted to organization-internal users.</p>
	<p>Resources are dedicated to specific missions or mission functions.</p>	<p>See above. In addition, dedication of resources can restrict agility/repurposing. Thus, dedication should be applied very selectively.</p>
<p><b>Offloading/Outsourcing: Supportive but non-essential functions are offloaded to a service provider that is better able to support the functions.</b></p>	<p>Supportive but non-essential functions are allocated to specific component systems, rather than performed by component systems that are mission-essential. Connectivity with or use of such non-essential component systems can be terminated in case of attack or other disruption.</p>	<p>Some functions that are supportive of one component system may in fact be mission-essential to another; these include many communications, discovery, and security services. Exercises as well as analysis may be needed to identify other functions that, while supportive, are mission-essential. System owners may want to claim their systems are (or, to decrease protection requirements, are not) mission-essential.</p>
<p><b>Agility/Repurposing: System elements are repurposed to provide services, information, and connectivity to meet new or changing mission needs.</b></p>	<p>Services and information provided by component systems, and connectivity provided by component networks or network segments, are repurposed to meet new or changing mission needs.</p>	<p>Mechanisms will be needed to support discovery of repurposed resources. Data transformation or service request translation mechanisms may be needed.</p>

#### 4.1.11 Redundancy

Redundancy techniques *provide multiple protected instances of critical information and resources, to reduce the consequences of loss*. Capabilities include Backup and Restore, Surplus Capacity, and Replication.

**Table 16. Redundancy for SoS**

Capability/Approach	Application to SoS	SoS Challenges
<p><b>Backup and Restore: Functionality is maintained to back up information and software (including configuration data) in a way that protects its confidentiality, integrity, and authenticity, and to restore it in case of disruption or destruction.</b></p>	<p>Component systems and networks or network segments can provide internal Backup and Restore capabilities for themselves, without coordination with other component systems. Backup and Restore capabilities should be combined with Substantiated Integrity, so that the functionality and data are restored to a known good state.</p> <p>One component system or network segment providing a service to others in the SoS can serve as a backup for another. This can be combined with Architectural Diversity to decrease the likelihood that compromise of the primary system/network segment will propagate to the backup. (Alternately, this can involve Replication, which is described below.)</p>	<p>Potential gaps in service when a component system or network segment is unavailable.</p> <p>Similar to the challenges for Dynamic Reconfiguration: Other systems need to be able to discover where to find the service, establish connectivity, and be authorized. If the backup uses different protocols or interface standards, traffic or requests must be translated. The backup may need to conform with existing SLAs, which can deprecate the request or traffic. The backup may need to be reconfigured to handle the responsibility for providing the service. In addition, mechanisms are needed to restore the failed system or segment, to notify other systems when it is restored, and to restore the system that had served as backup to its prior configuration. This can include expunging from the backup system mission and supporting data needed to provide the backup service. Data aggregation can increase the sensitivity of a component system unacceptably: If component X backs up component Y, the aggregated set of information on component X that is more than it is authorized to process.</p>
<p><b>Surplus Capacity: Extra capacity for information storage, processing, or communications is maintained.</b></p>	<p>Component systems, networks, or network segments can include extra capacity, unused during normal operations.</p>	<p>Increased cost.</p>
<p><b>Replication: Information and/or functionality is replicated (reproduced exactly) in multiple locations.</b></p>	<p>Software, hardware, and/or data can be replicated across multiple component systems.</p>	<p>Consistency of replicates needs to be maintained. This can be problematic in tactical environments or other environments in which bandwidth or connectivity to component systems is limited.</p>

#### 4.1.12 Segmentation/Isolation

Segmentation / Isolation techniques *separate components, subsystems, and systems (logically or physically) based on criticality and trustworthiness, to limit the spread of damage*. Approaches include Predefined Segmentation and Dynamic Segmentation/Isolation.

**Table 17. Segmentation/Isolation in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<p><b>Predefined Segmentation: Define enclaves, segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated.</b></p>	<p>Enclaves, consisting of component systems and network segments, are defined based on criticality and trustworthiness. Encryption can be used to separate virtual enclaves (where the services share hardware/communications media with other virtual enclaves). Cross-domain solutions or other boundary defense mechanisms can be used at enclave boundaries.</p> <p>A predefined enclave can be isolated from other systems and networks by reconfiguring its boundary defense mechanisms or by physically cutting communications. This can protect the enclave from attacks from other component systems, or vice versa.</p>	<p>Key management for cryptographically based segmentation.</p> <p>Separation of virtual enclaves may not be as strong as desired. For example, attacks on hypervisors can enable attacks to cross virtual machine-based enclave boundaries. Physical attacks on communications media can deny service across multiple enclaves.</p> <p>Mission needs may cause enclave boundaries to be redefined, or may require that access to an enclave for which a high level of trust in users be extended to mission partners.</p> <p>As noted above, separation of virtual enclaves may not be as strong as desired. Physical isolation is increasingly problematic, as devices are enabled with wireless communications.</p> <p>The performance or behavior of other component systems can be degraded, due to the unavailability of services provided by the now-isolated enclave.</p> <p>Procedures are needed for restoring the isolated enclave to the SoS; Substantiated Integrity mechanisms may be needed to ensure that the component systems and network segments are in a known good state before they are reconnected to other component systems.</p>
<p><b>Dynamic Segmentation/Isolation: Change the definition of enclaves or protected segments, or isolate resources, while minimizing operational disruption.</b></p>	<p>Enclave definitions may be created and enforced dynamically. Component systems, network segments, or networks can be isolated from others by reconfiguration or physical changes.</p>	<p>Key management for cryptographically based segmentation.</p> <p>The performance or behavior of other component systems can be degraded, due to the unavailability of services provided by the now-isolated resources.</p> <p>Procedures are needed for restoring the isolated resources to the SoS; Substantiated Integrity mechanisms may be needed to ensure that the resources are in a known good state before they are reconnected to other component systems.</p>



### 4.1.13 Substantiated Integrity

Substantiated Integrity techniques *provide mechanisms to ascertain whether critical services, information stores, information streams, and components have been corrupted*. Approaches include Integrity/Quality Checks, Provenance Tracking, and Behavior Validation.

**Table 18. Substantiated Integrity in SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Integrity/Quality Checks: Apply and validate checks of the integrity or quality of information or devices.</b>	Component systems and network segments apply integrity values (e.g., cryptographic checksums) to information they share. This information can include gold copies of software, validated versions of archived data, and messages transiting the network. Corrupted data can be quarantined for further analysis.	Consistent mechanisms across the SoS. Key management for cryptographic checksums. Gold copies of software may not include recent patches; validated data may not be up-to-date.
	Component systems and network segments perform quality checks (e.g., range-of-value checks) on information they handle. Anomalous or suspect data can be quarantined for further analysis.	Consistency of checks across the SoS. Anomalous data can be correct and mission-critical. If a component system suppresses anomalous information, mission impacts could result.
	Anti-tamper (AT) technologies are applied to selected common component devices.	Additional costs for AT. Consistent practices across the SoS.
<b>Provenance Tracking: Identify and track the provenance of data, software, and/or hardware elements.</b>	Component systems identify and track the provenance of data they handle, and provide provenance metadata to other component systems. Digital signatures can provide a limited mechanism for provenance.	Consistent mechanisms across the SoS. Additional overhead to assign, maintain, transmit, and store provenance metadata.
	Supply chain risk management (SCRM) practices are applied to selected technologies or common elements (e.g., devices).	Additional costs for SCRM. Consistent practices across the SoS.
<b>Behavior Validation: Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).</b>	Component systems and/or network segments can apply mechanisms (e.g., Byzantine quorum, reputation) to observe the behavior of a service offered by a component and collectively determine whether that component is likely to have been compromised or is otherwise less trustworthy.	Anomalous behavior can be mission-appropriate, given unusual or unforeseen circumstances.
	Component systems can rely on mechanisms for formal or algorithmic validation of specified behaviors or properties (e.g., formal verification of key software or hardware).	No standards for sharing, and no CONOPS for using, information about which elements of component systems are most trustworthy.

#### 4.1.14 Unpredictability

Unpredictability techniques *make changes, frequently and randomly, to make the attack surface unpredictable*. These changes, which may draw upon Diversity, Non-Persistence, and Dynamic Positioning techniques, make it more difficult for an adversary to predict behavior, which (as with Coordinated Defense) increases the chance of adversary actions being detected or tradecraft revealed.

**Table 19. Unpredictability for SoS**

Capability/Approach	Application to SoS	SoS Challenges
<b>Unpredictable Behavior: Changes are made to reduce an adversary's ability to predict future behavior.</b>	Unpredictability, using Diversity, Non-Persistence, and/or Dynamic Positioning techniques, is applied internally to component systems and network segments within a system-of-systems.	The services or capabilities that components expose to one another in a SoS need to be predictable. See also the challenges for Diversity, Non-Persistence, and Dynamic Positioning.

## 4.2 Summary

Table 20 presents a summary of the foregoing analysis, using the following key:

- **Internal:** The capability or approach, while possibly depending on information from or about another constituent system, is applied within a given constituent system; hence potentially implemented by individual programs.
- **Paired:** The capability or approach involves pairwise interactions between constituent systems; hence entails at a minimum agreements between programs.
- **Coordinated:** The capability or approach involves coordination among multiple constituent systems, or between constituent systems and a higher-level entity (e.g., a regional cyber defense center).
- **Effect:** The capability or approach emerges as an effect of bringing together constituent systems.
- **Opportunity:** The acknowledgement of a SoS creates opportunities for providing the capability or applying the approach at the SoS level; however, deliberate efforts are needed to capitalize on SoS-level opportunities.

**Table 20. SoS Applicability of Cyber Resiliency Techniques (Capabilities and Approaches)**

Technique	Capability or Approach	SoS Applicability
<b>Adaptive Response</b>	Dynamic Reconfiguration	Internal
	Dynamic Resource Reallocation	Internal
	Dynamic Composability	Internal
	Preemptive Action	Opportunity
<b>Analytic Monitoring</b>	Monitoring	Internal and Coordinated; can be Paired
	Damage Assessment	Internal and Coordinated; can be Paired
	Sensor Fusion and Analysis	Internal and Coordinated
	Malware and Forensic Analysis	Coordinated
<b>Coordinated Defense</b>	Technical Defense-in-Depth	Internal

Technique	Capability or Approach	SoS Applicability
	Coordination and Consistency Analysis	Opportunity
	Adaptive Management	Internal
<b>Deception</b>	Masking	Internal
	Repackaging	Internal
	Dissimulation / Disinformation	Internal; can be Paired
	Misdirection / Simulation	Opportunity

Technique	Capability or Approach	SoS Applicability
<b>Diversity</b>	Architectural Diversity / Heterogeneity	Effect
	Design Diversity / Heterogeneity	Internal and Coordinated
	Dynamic or Synthetic Diversity	Internal
	Path Diversity	Effect
	Information Diversity	Effect
<b>Dynamic Positioning</b>	Functional Relocation	Internal; some Opportunity for Paired
	Asset Mobility	Opportunity
	Distributed Functionality	Sometimes Paired; Opportunity
<b>Dynamic Representation</b>	Dynamic Mapping and Profiling	Opportunity
	Dynamic Threat Modeling	Opportunity
	Mission Dependency and Status Visualization	Opportunity
	CoA Analysis	Opportunity
<b>Non-Persistence</b>	Non-Persistent Information	Internal
	Non-Persistent Services	Internal and Paired
	Non-Persistent Connectivity	Internal and Paired; Opportunity
<b>Privilege Restriction</b>	Privilege Management	Opportunity
	Privilege-Based Usage Restriction	Opportunity
	Dynamic Privileges	Internal
<b>Realignment</b>	Purposing	Opportunity
	Offloading / Outsourcing	Opportunity
	Customization	Opportunity
	Restriction	Opportunity
	Agility / Repurposing	Opportunity
<b>Redundancy</b>	Backup and Restore	Internal and Paired
	Surplus Capacity	Internal and Paired; Opportunity
	Replication	Internal and Paired; Opportunity
<b>Segmentation / Separation</b>	Modularity / Layering	Internal
	Predefined Segmentation	Paired; Opportunity
	Dynamic Segmentation / Isolation	Paired; Opportunity
<b>Substantiated Integrity</b>	Integrity / Quality Checks	Internal; Opportunity
	Provenance Tracking	Internal and Paired; Opportunity
	Behavior Validation	Internal and Paired; Opportunity
<b>Unpredictability</b>	Unpredictable Behavior	Internal

### 4.3 Synergies and Dependencies among Resiliency Techniques

Resiliency techniques are often more effective in combination. In some cases, one technique will depend on another. On the other hand, one approach to implementing a resiliency technique can sometimes interfere with or undermine the effectiveness of an approach to implementing another technique, due to dependencies among mechanisms. Table 21 identifies synergies, dependencies, and conflicts at a high level. See Figure 2 (in Section 3) for a higher-level visual representation.

**Table 21. Relationships among Resiliency Techniques**

Technique A	Technique B	Adaptive Response	Analytic Monitoring	Coordinated Defense	Deception	Diversity	Dynamic Positioning	Dynamic Representation	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability
Adaptive Response	-	D	S	U	U, S	U	U	U, S	U		U	U	U, S	U	U
Analytic Monitoring	S	-	S	U, S	U	U, S	S								
Coordinated Defense		U	-	U	U		U		U		U	U	U		
Deception	S	S	S	-		U		U					U		U
Diversity	U, S	C, S	C, S		-		C	U, S	C	S	U, S				S
Dynamic Positioning	S	S		S		-		U							U, S
Dynamic Representation	S	U	S				-	S		S					
Non-Persistence	U, S			S	U, S	S	U	-							S
Privilege Restriction	S		S							-	S			U	
Realignment							U		U	-		U			
Redundancy					U, S							-		U	
Segmentation	U, S		S	S						S			-	U	
Substantiated Integrity	S								S		S	S	S	-	
Unpredictability	C, S	C	C	S	U	U, S		U							-

Key:

- S indicates that the technique in the row (Technique A) supports the one in the column (Technique B). Technique B is made more effective by Technique A.
- D indicates that Technique A depends on Technique B. Technique B will be ineffective if not used in conjunction with Technique A.
- U indicates that Technique A can make use of Technique B. Technique A can be implemented effectively in the absence of Technique B; however, more options become available if Technique B is also used.
- C indicates that Technique A can conflict with Technique B. Some or all implementations of Technique A could undermine the effectiveness of Technique B.

#### 4.4 Cyber Resiliency Techniques and Disaggregation

The recent Air Force Space Command paper on resiliency and disaggregation [21] defines space disaggregation as “the dispersion of space-based missions, functions or sensors across multiple systems spanning one or more orbital plane, platform, host or domain” and states that “Disaggregating space architectures is one strategy to improve resiliency, offering a means to trade cost, schedule, performance, and risk to increase flexibility and capability survivability.” The paper identifies five approaches to achieving disaggregation: Fractionation, Functional Disaggregation, Hosted Payloads, Multi-Orbit Disaggregation, and Multi-Domain Disaggregation. The last two approaches are inherently non-cyber.

The Fractionation, Functional Disaggregation, and Hosted Payloads approaches could introduce potential new cyber attack vectors, including exploitation of inconsistencies in privileges or configurations, exploitation of inconsistencies or use of timing attacks on components providing disaggregated functionality, and attacks on co-resident payloads via shared infrastructures. As shown in Table 22, these approaches apply some cyber resiliency techniques, enable the application of others, and require the application of still others to reduce risks associated with new attack vectors.

**Table 22. Disaggregation and Cyber Resiliency Techniques**

Approach	Cyber Resiliency Techniques
<b>Fractionation:</b> decomposition of a system into modules which interact wirelessly to deliver the capability of the original monolithic system	<ul style="list-style-type: none"> <li>• Applies Segmentation / Separation</li> <li>• Requires Coordinated Defense, to ensure that protections are layered and are used consistently</li> <li>• Facilitates the application of Privilege Restriction</li> </ul>
<b>Functional Disaggregation:</b> dispersion of sensors or distinct sub-missions onto separate platforms that were previously hosted on a single system	<ul style="list-style-type: none"> <li>• Applies Realignment in conjunction with Segmentation / Separation and Dynamic Positioning (Distributed Functionality)</li> <li>• Could apply Redundancy, if multiple copies of sensors or sub-missions are deployed; Redundancy could then enable Dynamic Positioning (Functional Relocation, Asset Mobility) to be applied, if tasking can be re-assigned</li> <li>• Requires Segmentation / Separation in conjunction with Privilege Restriction, to ensure that an attack on one platform will not compromise other platforms</li> <li>• Requires Coordinated Defense, to ensure that protections are used consistently</li> </ul>
<b>Hosted Payloads:</b> similar to functional disaggregation, take advantage of a primary payload that would typically be fielded even without the secondary, hosted payload	<ul style="list-style-type: none"> <li>• Requires Segmentation / Separation in conjunction with Privilege Restriction, to ensure that an attack on one payload will not compromise other co-resident payloads</li> <li>• Requires Coordinated Defense, to ensure that protections are used consistently</li> <li>• Applies Realignment in conjunction with Segmentation / Separation (non-cyber)</li> </ul>
<b>Multi-Orbit Disaggregation:</b> take advantage of multiple orbital planes to increase resiliency and complicate an adversary's targeting calculus	<ul style="list-style-type: none"> <li>• Applies a combination of Redundancy and Diversity (non-cyber)</li> <li>• Can potentially apply Dynamic Positioning (non-cyber)</li> </ul>
<b>Multi-Domain Disaggregation:</b> take advantage of systems in more than just the space domain	<ul style="list-style-type: none"> <li>• Applies Realignment in conjunction with the combination of Redundancy and Diversity (non-cyber)</li> <li>• Can potentially apply Dynamic Positioning (non-cyber)</li> </ul>

## 5 Conclusion

This paper has extended the definitions of goals, objectives, and techniques in the cyber resiliency engineering framework to 1) extend the set of possible threat sources to include natural events and errors as well as adversarial actions; 2) extend the set of adversarial actions to include non-cyber attack vectors; and 3) consider cyber-physical as well as purely cyber systems. The applicability of the techniques to system-of-systems resilience was analyzed. The analysis includes identification of interdependencies among techniques, as well as articulation of the extent to which, and how, the techniques apply in the SoS context. Challenges were identified, as were opportunities for emergent resilience.

Challenges largely relate to governance. Examples include who has decision authority, who has primary or shared responsibility for implementation, how coordination will be ensured, and how costs will be allocated or shared among constituent systems. In addition, technical problems arise related to interoperability and the time-phasing of implementations of cyber resiliency solutions.

Resilience is emergent at the mission / SoS level for some forms of Diversity and Redundancy. The potential to apply techniques at the SoS level is greatest for Dynamic Positioning, Dynamic Representation, Privilege Restriction, and Realignment. The potential to apply some approaches arises for Adaptive Response, Coordinated Defense, Deception, Segmentation / Separation, and Substantiated Integrity. Unpredictability is relevant within constituent systems, rather than at the SoS level.

## 6 Bibliography

- [1] DoD Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013. [Online]. Available: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>.
- [2] Cyber Physical Systems Virtual Organization, "National Symposium on Moving Target Research," 11 June 2012. [Online]. Available: <http://cps-vo.org/group/mtrs/program>.
- [3] ASD, "Memorandum for DoD Executive Agent for Space: Space Resilience Definition and Evaluation Criteria (U)," October 11, 2011.
- [4] ASD, *Fact Sheet: Resilience of Space Capabilities (attachment to Memorandum: Space Resilience Definition and Evaluation Criteria)*, 2011.
- [5] F. C. Belz, "Space Segment Information Assurance Guidance for Mission Success," Aerospace Report No. TOR-2011(8591)-22, 2011.
- [6] F. C. Belz, "Space Mission Resilience to Cyber Attacks (Aerospace Report No. TOR-2012(8960)-7)," The Aerospace Corporation, 2012.
- [7] OSD, "Systems Engineering Guide for Systems of Systems, Version 1.0," August 2008. [Online]. Available: <http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf>.
- [8] Air Force, "AFI 10-604, Capabilities-Based Planning," 10 May 2006. [Online]. Available: [http://static.e-publishing.af.mil/production/1/af\\_a3\\_5/publication/afi10-604/afi10-604.pdf](http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-604/afi10-604.pdf).
- [9] Defense Acquisition University, "Defense Acquisition Guidebook," 29 July 2011. [Online]. Available: <http://www.dote.osd.mil/docs/dote-temp-guidebook/DEFENSE-ACQUISITION-GUIDEBOOK-07-29-2011.pdf>.
- [10] J. Andary, "What Is Unique about Space Systems?," *INCOSE Insight*, December 2008.
- [11] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework," September 2011. [Online]. Available: [http://www.mitre.org/work/tech\\_papers/2012/11\\_4436/11\\_4436.pdf](http://www.mitre.org/work/tech_papers/2012/11_4436/11_4436.pdf).
- [12] A. M. Madni, *Designing for Resilience, ISTI Lecture Notes on Advanced Topics in Systems Engineering*, 2007.
- [13] A. M. Madni and S. Jackson, "Towards a Conceptual Framework for Resilience Engineering," *IEEE Systems Journal*, Vol. 3, No. 2, June 2009.
- [14] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," 17 March 2010. [Online]. Available: <http://www.ittc.ku.edu/resilinet/papers/Sterbenz-Hutchison-Cetinkaya-Jabbar-Rohrer-Scholler-Smith-2010.pdf>. [Accessed 23 May 2011].
- [15] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR 12-3795)," May 2013. [Online]. Available: [http://www.mitre.org/work/tech\\_papers/2013/12\\_3795/12\\_3795.pdf](http://www.mitre.org/work/tech_papers/2013/12_3795/12_3795.pdf).
- [16] L. Boehm, *Assuring Mission Execution through Resilient Cyber Architectures, presentation at the 3rd Annual Secure and Resilient Cyber Architectures Workshop*,



- 2013.
- [17] S. Sheard and A. Mostashari, "A Framework for System Resilience Discussions (18th Annual International Symposium of INCOSE)," 15 June 2008. [Online]. Available: [http://www.stevens.edu/csr/fileadmin/csr/Publications/Sheard\\_SystemsResilienceDiscussions.pdf](http://www.stevens.edu/csr/fileadmin/csr/Publications/Sheard_SystemsResilienceDiscussions.pdf).
  - [18] CERT Program, "CERT® Resilience Management Model, Version 1.0: Improving Operational Resilience Processes," May 2010. [Online]. Available: <http://www.cert.org/archive/pdf/10tr012.pdf>. [Accessed 26 October 2011].
  - [19] NIST, "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>.
  - [20] The MITRE Corporation, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)," 2012. [Online]. Available: <http://measurablesecurity.mitre.org/docs/STIX-Whitepaper.pdf>.
  - [21] Air Force Space Command, "Resiliency and Disaggregated Space Architectures: White Paper," 21 August 2013. [Online]. Available: <http://www.afspc.af.mil/shared/media/document/AFD-130821-034.pdf>.
  - [22] M. G. Richards, A. M. Ross, D. E. Hastings and D. H. Rhodes, "Empirical Validation of Design Principles for Survivable System Architecture," in *Proceedings of the 2nd Annual IEEE Systems Conference*, Montreal, Quebec, Canada, 2008.
  - [23] S. Marra, S. Hassell, C. Eck, J. (. Moody, S. R. Martin, G. Ganga, K. Harward, E. Rickard, J. Sandoval and J. Brown, "Cyber Resiliency Metrics for Discussion," 14 June 2013. [Online]. Available: [http://bbn.com/resources/pdf/whitepaper\\_CyberResiliencyMetricsMASTERv4.pdf](http://bbn.com/resources/pdf/whitepaper_CyberResiliencyMetricsMASTERv4.pdf).
  - [24] I. Lachow, "Active Cyber Defense: A Framework for Policymakers," February 2013. [Online]. Available: [http://www.cnas.org/files/documents/publications/CNAS\\_ActiveCyberDefense\\_Lachow\\_0.pdf](http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf).
  - [25] The MITRE Corporation, "Situation Awareness," Cybersecurity: Strengthening Cyber Defense, 2013. [Online]. Available: <http://www.mitre.org/work/cybersecurity/focus/awareness.html>.
  - [26] The MITRE Corporation, "Systems Engineering Guide: The Evolution of Systems Engineering," 11 November 2011. [Online]. Available: [http://www.mitre.org/work/systems\\_engineering/guide/evolution\\_systems.html](http://www.mitre.org/work/systems_engineering/guide/evolution_systems.html).
  - [27] J. S. Dahmann, G. J. Rebovich and J. A. Lane, "Systems Engineering for Capabilities," Crosstalk, November 2008. [Online]. Available: <http://www.crosstalkonline.org/storage/issue-archives/2008/200811/200811-Dahmann.pdf>.
  - [28] M. Richards, "'Complexity Has Bred Fragility': How Systems Engineering Can Enhance the Survivability of Space Systems," *INCOSE Insight*, December 2008.
  - [29] DoD, "Cyber Incident Handling Program, CJCSM 6510.01B," 10 July 2012. [Online]. Available: [http://www.dtic.mil/cjcs\\_directives/cdata/unlimit/m651001.pdf](http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf).

- [30] A. King, "Joint Cyber Center: command and control in the USTRANSCOM cyber domain," 18 March 2013. [Online]. Available: <http://www.transcom.mil/news/read.cfm?id=8933>.
- [31] K. B. Bhasin and J. L. Hayden, "Architecting communication network of networks for Space System of Systems," in *IEEE International Conference on System of Systems Engineering (SoSE '08)*, 2008.
- [32] M. Jamshidi, "Introduction to system of systems," in *Systems of Systems Engineering: Principles and Applications*, Boca Raton, FL, CRC Press, 2009, pp. 1-37.
- [33] K. B. Bhasin and J. L. Hayden, "Communication and Navigation Networks in Space System of Systems," in *System of Systems Engineering: Innovations for the Twenty-First Century*, John Wiley & Sons, 2011.
- [34] C. Peake, A. Underbrink and A. Potter, "Cyber Mission Resilience: Mission Assurance in the Cyber Ecosystem," September/October 2012. [Online]. Available: <http://www.crosstalkonline.org/storage/issue-archives/2012/201209/201209-Peake.pdf>.

## Appendix A    Abbreviations

AF	Air Force
AFSPC	Air Force Space Command
AIAA	American Institute of Aeronautics and Astronautics
ANSI	American National Standards Institute
APT	Advanced Persistent Threat
ASD	Assistant Secretary of Defense
AT	Anti-Tamper
CND	Computer Network Defense
CoA	Course of Action
CONOPS	Concept of Operations
COOP	Continuity of Operations
CREF	Cyber Resiliency Engineering Framework
CTAC	Cyber Threat Analysis Cell (or Center)
DoD	Department of Defense
IEEE	Institute of Electrical and Electronics Engineers
JCC	Joint Cyber Center
JOC	Joint Operations Center
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NSTAC	National Security Telecommunications Advisory Committee
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
PEO	Program Executive Office
SA	Situational Awareness
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SCoA	SoS CoA

SoS	System of Systems
STIX	Structured Thread Information eXpression
T&E	Test and Evaluation
TTPs	Tactic, Techniques, and Procedures

## Appendix B Survivability

The following table identifies relationships between principles for survivable systems architecture [22] and the resiliency goals, objectives, and techniques. The mapping to techniques is not one-to-one, primarily because the threat models are different, but also because the resiliency techniques assume systems engineering principles that support basic continuity of operations (COOP) and cyber security against non-advanced threats. Many of the principles for survivable systems architecture correspond primarily to a single resiliency technique (indicated by **X**), but include aspects of one or more other techniques (indicated by x). For some survivability principles, there is no clear corresponding technique. Note that no survivability principle corresponds to Analytic Monitoring, and that Dynamic Representation corresponds to Preemption only insofar as a near-real-time representation enable pre-emptive action.

**Table 23. Mapping of Cyber Resiliency Framework to Principles for Survivable Systems**

Resiliency	Goals				Objectives							Techniques														
	Anticipate	Withstand	Recover	Evolve	Understand	Prepare	Prevent	Continue	Constrain	Reconstitute	Transform	Re-Architect	Adaptive Response	Analytic Monitoring	Coordinated Defense	Deception	Diversity	Dynamic Positioning	Dynamic Representation	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability
<b>Survivability</b>																										
<b>Susceptibility Reduction</b>																										
Prevention: suppress a future or potential disturbance <sup>15</sup>	X						<b>X</b>																			
Mobility: relocate to avoid detection by an external change agent	X						X											<b>X</b>								X
Concealment: reduce the visibility of a system from an external change agent	X						X									<b>X</b>										

<sup>15</sup> While Prevent is a cyber resiliency objective, it is achieved primarily by using conventional information system security controls effectively.

Resiliency	Goals				Objectives							Techniques															
	Anticipate	Withstand	Recover	Evolve	Understand	Prepare	Prevent	Continue	Constrain	Reconstitute	Transform	Re-Architect	Adaptive Response	Analytic Monitoring	Coordinated Defense	Deception	Diversity	Dynamic Positioning	Dynamic Representation	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability	
<b>Survivability</b>																											
Deterrence: dissuade a rational external change agent from committing a disturbance <sup>16</sup>	X					X							X		X												X
Preemption: suppress an immediate disturbance	X					X							<b>X</b>														
Avoidance: maneuver away from disturbance	X					X						X					<b>X</b>										X
<b>Vulnerability Reduction</b>																											
Hardness: resist deformation		X				X									<b>X</b>						X	X		X			
Redundancy: duplicate system functions to increase reliability		X					X																<b>X</b>				
Margin: allow extra capacity to maintain value delivery despite losses		X					X																<b>X</b>				
Heterogeneity: vary system elements to mitigate homogeneous disturbances		X						X									<b>X</b>										
Distribution: separate critical system elements to mitigate local disturbances		X						X										X						<b>X</b>	X		
Failure Mode Reduction: eliminate system hazards through intrinsic design				X	X		<b>X</b>													X	<b>X</b>						
Fail-Safe: prevent or delay degradation via physics of incipient failure <sup>17</sup>		X			X									X											X		
Evolution: alter system components to reduce disturbance effectiveness				X							X	<b>X</b>									X						

<sup>16</sup> Deterrence is an examples of an intended effect on the adversary; the survivability framework does not provide a comprehensive treatment of effects on the adversary. The resiliency framework is oriented to benefits to the mission or the defender. While Deception and Unpredictability can be viewed as deterrent, deterrence is a secondary effect of those techniques. Preemption, with the goal of deterrence, is one approach to providing Adaptive Response.

<sup>17</sup> The fail-safe principle as defined involves the use of physical properties, and thus does not apply to the cyber domain. However, the principle can be extended to mean “design so that failure does not leave the system in an unsafe or insecure state.” If this is the definition, then such techniques as Coordinated Defense and Substantiated Integrity apply.

Resiliency	Goals				Objectives							Techniques														
	Anticipate	Withstand	Recover	Evolve	Understand	Prepare	Prevent	Continue	Constrain	Reconstitute	Transform	Re-Architect	Adaptive Response	Analytic Monitoring	Coordinated Defense	Deception	Diversity	Dynamic Positioning	Dynamic Representation	Non-Persistence	Privilege Restriction	Realignment	Redundancy	Segmentation	Substantiated Integrity	Unpredictability
<b>Survivability</b>																										
Containment: isolation or minimization of the propagation of failure		X							X															X		
Replacement: substitute system elements to improve value delivery				X								X							X							
Repair: restore system to improve value delivery		X								X				X										X	X	