Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 28 (2014) 838 – 847

Procedia Computer Science

Conference on Systems Engineering Research (CSER 2014)

Eds.: Azad M. Madni, University of Southern California; Barry Boehm, University of Southern California; Michael Sievers, Jet Propulsion Laboratory; Marilee Wheaton, The Aerospace Corporation
Redondo Beach, CA, March 21-22, 2014

Cyber Resiliency Engineering

Overview of the Architectural Assessment Process

Deborah J. Bodeau[a], Richard D. Graubart[b], and Ellen R. Laderman[c] *

a, b, c *The MITRE Corporation 202 Burlington Road Bedford MA 01730, USA*

Abstract

Missions, business functions, organizations, and nations are increasingly dependent on cyberspace where attacks are no longer limited to simple discrete events such as the spread of a virus or a denial-of-service attack. Therefore, architecture and systems engineering must assume systems or components have been compromised and missions and business functions must continue to operate despite compromises. A growing number of technologies and architectural practices can be used to improve resilience to cyber threats. However, these improvements come with costs as well as benefits. Cyber resiliency assessments are intended to identify where, how, and when cyber resiliency techniques can be applied to improve architectural resiliency in a cost-effective way.

Keywords: cyber resiliency engineering, cyber resiliency assessment, architectural assessment process

*Deborah J. Bodeau Tel.: 1-781-271-8436; fax: 1-781-271-8953; E-mail address: dbodeau@mitre.org
Richard D. Graubart Tel.: 1-781-271-7976; fax: 1-781-271-8953; E-mail address: rdg@mitre.org
Ellen R. Laderman Tel.: 1-781-271-4940; fax: 1-781-271-3957; E-mail address: laderman@mitre.org

doi:10.1016/j.procs.2014.03.100

1. Introduction

With the growing capability, expertise and intent of advanced cyber adversaries, it is no longer realistic to assume that one can successfully keep all adversaries out of a system infrastructure. Therefore, architecture and systems engineering must be based on the assumption that systems or components have been or can be compromised, and that missions and business functions must continue to operate in the presence of compromise [1]. Cyber resiliency assessments [2] are intended to identify where, how, and when cyber resiliency techniques can be applied to improve architectural resiliency against advanced cyber threats. The Cyber Resiliency Engineering Framework [3], as illustrated in Figure 1 and described in more detail in the Appendix, provides a way to understand goals and objectives based on this assumption of compromise, and the techniques (as defined in Table 5 below) that can be applied to improve mission resilience against advanced cyber threats.

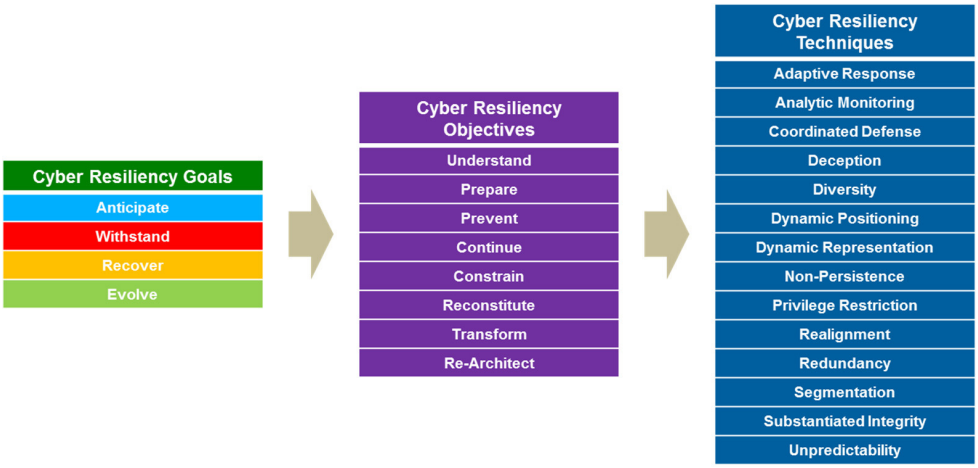

Figure 1. Cyber Resiliency Engineering Framework

However, due to a variety of political, operational, economic and technical (POET) factors, it is not feasible for organizations to use all resiliency techniques, or the growing set of technologies that implement aspects of the techniques. (For a detailed survey of technologies, as well as discussion of POET factors, see [2].) It is also not feasible to apply any resiliency technique pervasively, because implementations of cyber resiliency techniques vary in maturity across different architectural layers, and because some implementations are intended to be used only in strategically chosen locations in a system, common infrastructure, or System of Systems (SoS). Thus, a structured approach to identifying possible improvements is needed. The following three steps are used to assess the cyber resiliency of a system or architecture: (1) determine the scope of, and prepare for, the assessment, (2) assess the architecture, and (3) develop specific recommendations.

If the approach is applied to an operational or as-is architecture, the emphasis may be on “low-hanging fruit” or opportunities for near-term and high-leverage improvements, using a few cyber resiliency techniques. A set of general recommendations provides a starting point for identifying such opportunities. If the approach is applied to a notional or to-be architecture, the assessment may look at the full set of cyber resiliency techniques, and at ensuring that possible solutions in the mid- and long-term can be integrated into the architecture.

2. Determine the Scope and Plan for the Assessment

Planning an assessment involves determining the purpose and scope of an assessment and identifying key stakeholders and sources of information.

The purpose of an assessment is defined by the questions it is intended to answer and the decisions it is intended to support. These should initially be expressed in stakeholder terms rather than resiliency terms; they can then be

translated into the cyber resiliency framework terminology. Depending on the purpose, the assessment can produce qualitative assessment values for objectives, sub-objectives, and techniques, or can identify existing capabilities for achieving objectives and sub-objectives, and potential improvements based on applying relevant techniques.

The scope of a cyber resiliency architectural assessment consists of both the architecture to be assessed, including a description of the missions and/or business processes when appropriate, and the cyber resiliency objectives and techniques to be considered. The scope is also determined in part by the architectural layers included in the architecture. Finally, the scope depends on whether the architecture is as-is or to-be. For an as-is architecture, the scope may be limited to near-term improvements, emphasizing effective use of existing security capabilities to anticipate, withstand, and recover from attacks. For a to-be architecture, the scope can include ways the architecture can be defined to evolve over time, to leverage techniques that are currently being researched or prototyped.

The determination of which techniques to include in the scope is strongly influenced by POET considerations. Table 1 provides representative examples of reasons for excluding techniques from consideration or restricting specific techniques to be considered in developing recommendations.

Table 1. Representative Reasons for Restricting Consideration of Cyber Resiliency Techniques

Technique	**Representative Reasons for Restricting Consideration**
Adaptive Response	Liability concerns (e.g., responses that violate Service Level Agreements (SLA), cause collateral damage)
Analytic Monitoring	Policy concerns related to collecting, aggregating, and retaining data
Coordinated Defense	Governance and Concept of Operations (CONOPS) issues (e.g., overlapping or incompletely defined roles and responsibilities, no clear responsibility for defining cyber courses of action)
Deception	Legal, regulatory, contractual, or policy restrictions; Concern for reputation
Diversity	Policy or programmatic restrictions (e.g., organizational commitment to a specific product or product suite); Life-cycle cost of developing or acquiring, operating, and maintaining multiple distinct instances
Dynamic Positioning	Technical limitations due to policy or programmatic restrictions (e.g., organizational commitment to a specific product or product suite)
Dynamic Representation	Governance issues / information sharing constraints in the context of SoS
Non-Persistence	Technical limitations that prevent refresh functions from meeting Quality of Service requirements
Privilege Restriction	Governance and CONOPS issues (e.g., operational impetus to share roles)
Realignment	Organizational and cultural impacts (e.g., eliminating functions staff are used to, morale of relocating staff)
Redundancy	Costs of maintaining multiple, up to date and secure instantiations of data and services
Segmentation	Cost and schedule impacts of re-architecting; cost of additional routers, firewalls
Substantiated Integrity	Cost and schedule impacts
Unpredictability	Operational and cultural issues (e.g., adverse impact on planned activities or staff expectations)

Stakeholders' needs drive which resiliency techniques are needed. Different stakeholders have different needs and perspectives. Interviews with the various stakeholders are needed to obtain a complete view of their needs. Table 2 identifies possible stakeholders and Subject Matter Experts (SMEs) who might be interviewed.

Table 2. Possible Stakeholders and Subject Matter Experts to Interview

Role	Information to Obtain
Mission Owner	Mission priorities – what tasks are mission-essential, mission-critical, or supportive; relative priority of near-term vs. long-term mission capabilities. Information usually derived from requirements and in Mission Impact Analysis or Business Impact Analysis.
Cyber Defender: Tactical or line-level management, operational or mid-level management, and strategic or enterprise-level management	How – and how well – the architecture enables cyber defenders to fulfill their responsibilities. (See Appendix A of reference 2 for a detailed mapping of cyber defender activities to cyber resiliency objectives and sub-objectives.)
Program Manager	Relative priorities of cyber resources and cyber resiliency goals and objectives, based on the missions the program supports, the relative priorities of near-term vs. long-term capabilities for those missions, and the criticality of cyber resources to those missions.
IT/ICT Provider (e.g., Datacenter Manager)	Relative importance of different capabilities or services.
Architect / Systems Engineer	Current and future architecture. POET considerations, particularly technical constraints.

Table 3 identifies possible source documents for a cyber resiliency assessment. The source documents consulted depend on the scope of the assessment, and on the life-cycle stage.

Table 3. Possible Source Documents

Source Document	Relevance
Mission Impact Analysis or Business Impact Analysis	Identifies mission (or business process) concerns and priorities. Identifies mission-essential and mission-critical resources. Provides basis for contingency plans.
Contingency Plans (e.g., Business Continuity Plans or Continuity of Operations Plans)	Describes how cyber resources and operational processes are used to ensure mission / business continuity under stress.
Architecture documentation	Describes the architectures of the mission / business segment, SoS, common infrastructure, set of shared services, system, and/or components.
Standard Operating Procedures (SOPs) for system or network administration, and for handling computer incidents	Describes how cyber resources are used to enforce policies and meet SLAs. Describes operational processes for responding to incidents.
Computer Network Defense plans, Cyber Courses of Actions (CCoA) or cyber playbooks	Describes processes, procedures, and cyber resources used in those processes for cyber defense.

3. Perform the Assessment

Performing the assessment involves assigning qualitative values ranging from very low to very high, with supporting rationale. This section provides general value scales that can be used for all cyber resiliency techniques. For some assessments, a more detailed set of definitions may be needed. Tables defining values for cyber resiliency techniques can be constructed, using the general structure in Section 3.1 below.

Documenting the rationale for the assignment of a value is a crucial part of the assessment. The rationale can identify inherent architectural vulnerabilities to attacks by advanced adversaries; gaps in technologies, SOPs, or CCoAs; and/or policy or governance issues. The rationale therefore provides the foundation for developing recommendations.

3.1. Architecture Flexibility or Capability

For any architecture, an assessment can determine how flexible or capable the architecture is with respect to the incorporation and effective application of a resiliency technique. Table 4 provides a scale of relative flexibility as a function of architectural traits.

Table 4. Definitions of Level for Flexibility

Level	Components, Technology, and Process to Implement Resiliency	Integration of Additional Technology or Components as they become available
Very High	Explicitly integrates a strategic set; has mechanisms to assess effectiveness	Explicitly provides flexibility
High	Explicitly includes	Some flexibility
Medium	Accommodates or includes	Some flexibility
Low	Does not preclude	Limited flexibility
Very Low	Precludes	Severely limited

For each of the resiliency techniques, the differences between these levels are described in terms of technique-specific factors. These differentiating factors are identified as in Table 5.

Table 5. Key Differentiators Between Levels for Cyber Resiliency Techniques

Cyber Resiliency Technique	Key Differentiators Between Levels
Adaptive Response: take actions in response to indications that an attack is underway based on attack characteristics	Breadth: How many different responsive actions does the architecture support? Depth: At how many architectural layers can responsive actions be taken? Dynamism: How quickly can response actions be taken? Integration: How well are resiliency technologies integrated into response?
Analytic Monitoring: gather and analyze data on an ongoing, coordinated basis, to identify potential vulnerabilities, adversary activities, and damage	Sensor locations: At how many locations is monitoring performed? Sensor coordination: How well can sensor coverage and analysis be coordinated? Sensor dynamism: How quickly can sensors be recalibrated? Analysis timeliness: How quickly can analysis data be performed? Scope: What is the scope of analysis?
Coordinated Defense: manage adaptively and in a coordinated way multiple, distinct mechanisms to defend critical resources against adversary activities	Breadth: How many defensive techniques are applied at a given architectural layer? Depth: At how many architectural layers is a given defensive technique applied? Internal consistency / coordination: How consistently and with how much coordination are cyber defenses, and supporting security controls managed in a given administrative span of control? External consistency / coordination: How consistently and with how much coordination are cyber defenses managed across different administrative spans of control?
Deception: use obfuscation and misdirection (e.g., disinformation) to confuse an adversary	Sophistication of dissimulation: How sophisticated are the mechanisms (e.g., encryption)? Sophistication of simulation: How sophisticated are the mechanisms (e.g., honeynets)? Integration: How well are deception mechanisms integrated with other mechanisms?
Diversity: use a heterogeneous set of technologies (e.g., hardware, software, firmware, protocols) and data sources to minimize the impact of attacks and force adversaries to attack multiple different types of technologies	Depth: Diversity provided/supported at how many architectural layers? Breadth: At how many locations in the architecture is diversity provided or supported? Degree: How many instances / alternatives are accommodated within the architectural layers? Dynamism: How quickly can new implementations be integrated into the system? Integration: How well is diversity integrated with other practices?
Dynamic Positioning: use distributed processing and dynamic relocation of critical assets and sensors	Asset positioning: How extensively is a moving target defense strategy applied to critical assets? Sensor positioning: How extensively can sensors be moved / reassigned / reconfigured? Dynamism: How quickly can dynamic positioning take effect?
Dynamic Representation: maintain dynamic representations of components, systems, services, mission dependencies, adversary activities, and effects of cyber actions	Breadth: How many aspects are included in representations? Timeliness: How quickly / how often are representations updated?
Non-Persistence: retain information, services, and connectivity for a limited time	Depth of non-persistence: At how many architectural layers is non-persistence supported? Frequency of non-persistence: How frequently is the data, service, or system refreshed?
Privilege Restriction: restrict privileges required to use cyber resources, and privileges assigned to users and cyber entities, based on the type and degree of criticality and trust respectively, to minimize potential impact of adversary activities	Depth of privilege restriction: At how many layers is privilege restriction applied? Breadth of privilege restriction: How broadly or narrowly is least privilege applied? Criticality: To what degree is criticality analysis linked to least privilege? Coordination/consistency: How consistently are privileges defined and assigned? In a SoS, how well are policies and practices coordinated?
Realignment: align cyber resources with core aspects of mission/business functions, thus reducing the attack surface	Depth of realignment: At how many layers is realignment applied? Degree of analysis: How detailed is analysis/determination of core mission functions? Formalization of realignment: How formal/structured are realignment processes?
Redundancy: maintain multiple protected instances of critical resources (information and services)	Breadth of redundancy: How many duplicate copies of a given resource exist? Where? Depth of redundancy: At how many layers is redundancy provided? Validation: How consistent and independent are duplicate copies? Integration: How well is redundancy integrated with other techniques?

Cyber Resiliency Technique	Key Differentiators Between Levels
Segmentation: separate (logically or physically) components based on pedigree and/or criticality, to limit the damage from successful exploits	Strength of separation: How effective is the separation? Depth of segmentation: At how many layers is segmentation provided? Responsiveness of isolation: How quickly and effectively can segmentation be used to isolate cyber resources in light of an attack?
Substantiated Integrity: ascertain that critical services, information stores, information streams, and components have not been corrupted by an adversary	Depth of integrity: At how many layers is unpredictability applied? Strength of integrity mechanisms: How strong or effective are the substantiated integrity mechanisms (e.g., prevent changes to data/system, detect changes, increase sources of data to reduce probability of changes that will impact mission)?
Unpredictability: make changes frequently and randomly	Depth of unpredictability: At how many layers is unpredictability applied? Intentionality of unpredictability: Is unpredictability planned, happenstance, or a combination?

3.2. Implementation

For notional architectures, the assessment is based on specifications and plans. Regardless of how detailed such documents are they still focus on something that is not yet real. In contrast, "as-is" architectures are realized in operational environments and can be assessed with regards to the commitment to using a resiliency technique, the comprehensiveness of the implementation, and the effectiveness of the implementation. Note that implementation includes not only inclusion of technical mechanisms, but also how the practice is used operationally. Table 6 provides a general definition of levels of implementation.

Table 6. Levels of Implementation

Level	Commitment	Comprehensiveness	Effectiveness
Very High	In addition to the commitment at High Level: Investment / architectural evolution plans include expected future mechanisms / capabilities	All specific technologies or approaches available are applied	Effectiveness validated by penetration testing, exercises, and metrics tracking
High	In addition to the commitment at Medium Level: Resources are allocated to the use of the technique (life-cycle costs, Level of Effort (LOE), training) and investment / architectural evolution plans include the technique	Most specific technologies or approaches available are applied	Effectiveness validated by penetration testing and limited exercises
Medium	Policies and contractual agreements accommodate some use of the technique Some uses of the technique are represented in operations (CONOPS, SOPs, TTPs) Limited resources are allocated to the use of the technique (life-cycle costs, LOE, training)	Some specific technologies or approaches are applied	Effectiveness validated by testing
Low	Plans exist for modifying policies and contractual agreements to accommodate some use of the technique	Some specific technologies or approaches are planned	Effectiveness to be validated by testing
Very Low	No plans to address POET considerations to enable or facilitate use of the technique	Techniques or approaches are incidental rather than planned	Effectiveness is not evaluated

4. Develop Recommendations

The goal of an assessment is to provide recommendations. This section provides general recommendations to serve as a starting point. Issues that architects and systems engineers should take into consideration when developing or applying recommendations are also discussed.

Table 7 provides general recommendations or engineering principles for applying resiliency techniques. These can serve as a starting point. When differentiating factors for resiliency techniques are assessed, more specific recommendations can be developed.

Table 7. General Recommendations for Applying Cyber Resiliency Techniques

Technique	General Recommendations
Adaptive Response	Maintain an up-to-date and consistent cyber playbook (set of SOPs, CCoAs, and configuration guides) - Exercise to validate
	Integrate automated decision response mechanisms carefully, to avoid destabilization
	Support human interaction and understandable user interfaces
	Exercise caution in using fully automated dynamic mechanisms
Analytic Monitoring	Combine monitoring and analysis across sub-systems (e.g., IDS, anti-malware, CMRS)
	Identify and address monitoring issues related to transience of other cyber resources
	Analyze and address trade-off between encryption and monitoring
Coordinated Defense	Apply defense in depth, moving away from a "hard outside, soft chewy center"
	Coordinate SOPs, particularly for performance management and configuration management, with mission threads
	Coordinate the development of CCoAs with administrator SOPs, across multiple administrative domains, taking into consideration mission threads, for missions that rely on resources covered by the CCoAs
Deception	Work out policy, governance, and CONOPS issues related to active deception prior to defining a deception architecture
	Consider the scope of deception (e.g., focused on internal systems, supply chain, DMZ, or external data repositories and servers) in architectural decisions
Diversity	Make effective use of incidental diversity
	Incorporate (rather than try to expunge) diverse components, products, and services acquired at different times and/or by different organizations
	Accommodate diversity in end-user devices (particularly for "bring your own device")
	Invest in targeted diversity for critical assets carefully
	Communications: identify and maintain alternative communications paths
	Software: take advantage of organization-owned mission applications
	Information: identify and maintain multiple sources of critical mission data
	Hardware: apply Anti-Tamper(AT), Supply Chain Risk Management and design diversity
Dynamic Positioning	Use existing technologies to distribute assets in ways that take resiliency into account
	Ensure consistent protection
	Integrate with backup, isolation, and rollback
Dynamic Representation	Ensure existence of and then build on static representations of components, systems, services mission dependencies and adversary actions
	Use existing tools to maintain a current and realistic representation: Use Continuous Monitoring and intrusion detection tools to represent security posture; use performance monitoring and functional mapping tools to represent mission dependencies
	Coordinate with contingency planning activities, so that plans, CCoAs, and SOPs can support non-adversarial as well as adversarial disruptions
Non-Persistence	Leverage virtualization to make services non-persistent
	Minimize "immortal" services and connections as part of system and network administrator SOPs - Terminate unused ports and protocols
Privilege Restriction	Apply best practice for least privilege, separation of duties, and role-based access control
	Identify critical resources and lock down their use
Realignment	Analyze mission/business processes to identify non-essential resources
	Plan to separate or offload non-essential resources
Redundancy	Apply good practice standards for redundancy in the context of contingency planning
	Ensure current patch/configuration status of redundant firmware and software resources
	Ensure protection of all instances of critical resources regardless of location
Segmentation	Define and separate enclaves based on sensitivity, criticality, and trust
	Employ logical isolation mechanisms (e.g., routers, firewalls, controlled interfaces) to isolate enclaves and subnets
	Ensure isolation of Internet from intranet
	Isolate organization's cyber security operations center (CSOC) from rest of organization
Substantiated Integrity	Apply existing software integrity and network address validation mechanisms effectively
	Apply AT to critical hardware, firmware, and software components
Unpredictability	Include unpredictable changes that are transparent to mission/business process users in day-to-day operations

4.1. Additional Considerations

Adoption and effective use of a cyber resiliency technique entails addressing a variety of challenges that can be framed in POET terms. See Appendix E of [2].

Another consideration is the maturity of the resiliency technique. Not all resilience techniques are at the same level of maturity and usage. Techniques such as Privilege Restriction, Redundancy, Segmentation, and Analytic Monitoring include elements that are in common practice today. At the other extreme, techniques such as Adaptive Response, Deception, Diversity, Realignment and Unpredictability are rarely applied in current practice. See Appendix D and Appendix F of [2].

When a technology supports cyber resiliency, it is important to consider how effectively it is used to provide resiliency. For example, virtualization can be an effective means of supporting Non-Persistence, Diversity, Adaptive Response, Dynamic Positioning and Segmentation strategies. The use of virtualization is growing, but that does not mean that simply including virtualization technology in an architecture makes the architecture more resilient. Most uses of virtualization are intended to improve performance, and have little or no relevance to resiliency against advanced cyber threats.

While the trend toward using data centers to host mission/business applications is largely driven by cost, data centers can provide increased resiliency, leveraging virtualization and cloud computing infrastructures. Cyber resiliency techniques apply differently to different classes of resources in data centers. Segmentation techniques to create separate enclaves for different classes of resources are highly applicable to data center/cloud environments. It is important to look at the implementation to see how it supports or limits cyber resiliency.

5. Conclusion

Cyber resiliency is a relatively new concept, and engineering principles for cyber resiliency are emerging. (For more information, see the Reports of the 2nd and 3rd Annual Secure and Resilient Cyber Architectures Workshop [4,5].) The recommendations developed from an architectural assessment of cyber resiliency must be meaningful and feasible within the constraints of the political, operational, economic, and technical factors that apply. The architectural resiliency assessment process summarized in this white paper, and described in more detail in reference 2, is designed to be adaptable, so that only the most relevant aspects of cyber resiliency are considered. The process – like the Cyber Resiliency Engineering Framework – is also designed to be extensible, to accommodate new cyber resiliency technologies and principles as they are developed and proven.

Appendix A. Cyber Resiliency Engineering Framework

This appendix provides background on the Cyber Resiliency Engineering Framework, which can be used to structure analysis during an assessment. The framework was derived from frameworks and ontologies in a variety of related engineering disciplines, including resilience engineering [6,7], system resilience in critical infrastructure sectors[8], network resilience [9,10], survivability [11], dependability [12], and cybersecurity [13]. The framework organizes the cyber resiliency domain into a set of goals, objectives, and techniques. Goals are high-level statements of intended outcomes. Objectives are more specific statements of intended outcomes, expressed so as to facilitate assessment.

Cyber resiliency techniques are technical, operational, or governance approaches to achieving cyber resiliency objectives. These techniques are selectively applied to architectures or to the design of mission/business functions and the cyber resources that support them, to achieve cyber resiliency objectives. Table 8 identifies enabling techniques for the objectives (and, to aid understanding, more specific sub-objectives).

Table 8. Cyber Resiliency Objectives and Sub-Objectives Enabled by Techniques

Objective	Sub-Objective	Techniques
Understand: *maintain useful representations of mission/business cyber dependencies, and of the status of cyber resources with respect to possible adversary activities*	Understand adversaries	Analytic Monitoring Deception
	Understand mission or business function dependencies on cyber resources *and*	Dynamic Representation Realignment
	Understand the functional dependencies among cyber resources	Coordinated Defense Privilege Restriction
	Understand the status of resources with respect to adversary activities	Adaptive Response Analytic Monitoring Dynamic Positioning Dynamic Representation Substantiated Integrity
Prepare: *maintain a set of realistic cyber courses of action that address predicted or anticipated cyber attacks*	Create and maintain cyber courses of action	Coordinated Defense
	Maintain resources to accomplish above actions	Coordinated Defense
	Validate the realism of cyber courses of action	Coordinated Defense Dynamic Representation
Prevent: *preclude successful execution of an attack on a set of cyber resources*	Harden resources based on adversary capabilities	Coordinated Defense
	Deflect adversary actions	Deception
	Dissuade / deter adversaries by increasing the adversary's costs	Diversity Privilege Restriction Segmentation Unpredictability
	Dissuade / deter adversaries by increasing the adversary's risks	Analytic Monitoring Deception
	Deter attacks by limiting the adversary's benefits	Deception Non-Persistence
Continue: *maximize the duration and viability of essential mission/business functions during an attack*	Maintain functioning	Adaptive Response Diversity Coordinated Defense
	Ensure that functioning is correct	Substantiated Integrity
	Extend the surface an adversary must attack to be successful	Privilege Restriction Non-Persistence Unpredictability
Constrain: *limit damage from an adversary's attacks*	Isolate resources to preclude or limit adversary access	Segmentation
	Move resources to preclude adversary access	Dynamic Positioning Realignment
	Change or remove resources to limit or preclude adversary access	Non-Persistence Privilege Restriction Adaptive Response
Reconstitute: *redeploy cyber resources to provide mission / business functionality after a successful attack*	Maintain deployable / redeployable resources	Redundancy
	Restore functionality	Adaptive Response Coordinated Defense
	Validate functionality	Substantiated Integrity
Transform: *change behavior in response to prior or predicted adversary attacks*	Identify unnecessary dependencies	Realignment
	Adapt systems and mission / business processes to mitigate risks	Realignment
Re-Architect: *modify architectures for improved resiliency*	Address predicted long-term changes in adversary capabilities, intent, and/or targeting	Supporting
	Apply cyber resiliency practices cost-effectively	Supporting
	Incorporate emerging technologies	Supporting

Cyber resiliency techniques can be applied at different domains (layers in a notional layered architecture), as indicated in Table 9. Effective application of cyber resiliency techniques to different layers leverages approaches from the broader disciplines of fault-tolerant computing, network resilience, and system resilience using redundancy for backup, failover, and recovery.

Table 9. Application Domains for Cyber Resiliency Techniques

Application Domain / Layer with examples	Related Resilience Approaches
Hardware/firmware (e.g., FPGA, MPSoC, processors, embedded firmware)	Fault-tolerant hardware
Networking/communications (e.g., Communications media, networking protocols)	Network resilience, especially using redundancy
System/network component (e.g., Firewalls, servers, thin-clients)	Fault-tolerant design
Operating system (e.g., General-purpose OS, Real Time OS)	Fault-tolerant design
Cloud, virtualization, and/or middleware infrastructure (e.g., VMM, hypervisor, SOA infrastructure / shared services)	Fault-tolerant design; middleware for predictable and load-balanced service
Mission / business function application / service (e.g., Tailored DBMS, workflow management software; specialized mission applications)	Fault-tolerant design
Software (e.g., Software running on system/network components (including OS, cloud, virtualization, middleware, DBMSs, applications, services))	Fault-tolerant design
Information streams / feeds (e.g., RSS feeds, Twitter, instant messaging / chat, video feeds)	Network resilience, especially using redundancy
Systems (e.g., Integrated sets of the foregoing, within a single administrative or management span of control.)	System resilience using redundancy for backup, failover, and restore
Systems-of-systems (e.g., sets of systems under multiple spans of control, which interoperate to support a given mission or set of missions.)	System resilience using redundancy for backup, failover, and restore; network resilience using redundancy for alternate communications paths

References

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. Bodeau, D, Graubart, R. Cyber Resiliency Assessment: Enabling Architectural Improvement. The MITRE Corporation; 2012. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf.
3. Bodeau, D, Graubart, R. Cyber Resiliency Engineering Framework. The MITRE Corporation; 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf.
4. The MITRE Corporation (ed.). Second Secure and Resilient Cyber Architectures Workshop. The MITRE Corporation. December 2012. [Online.] https://registerdev1.mitre.org/sr/2012/2012_resiliency_workshop_report.pdf.
5. McQuaid, M, Alicea, CE, Heinbockel, W, Bodeau, D, Graubart, R. Third Secure and Resilient Cyber Architectures Workshop. The MITRE Corporation. December 2013. [Online.] http://www.mitre.org/sites/default/files/publications/13-4210.pdf.
6. Madni, AM, Jackson, S. Towards a Conceptual Framework for Resilience Engineering. *IEEE Systems Journal*, Vol. 3, No. 2. June 2009.
7. Madni, AM. Designing for Resilience. s.l. : *ISTI Lecture Notes on Advanced Topics in Systems Engineering*. 2007.
8. INCOSE. Resilient Systems Working Group. [Online] May 20, 2010. http://www.incose.org/practice/techactivities/wg/rswg/.
9. ReSIST. Resilience for Survivability in IST: Summary. [Online] 2007. http://www.resist-noe.org/DOC/ReSIST_Summary.pdf.
10. ReSIST. Resilience ontology: final. [Online] December 2008. http://www.resist-noe.org/Publications/Deliverables/D34-Resilience_Ontology_Final.pdf.
11. Richards, MG, Ross, AM, Hastings, DE, Rhodes, DH. Empirical Validation of Design Principles for Survivable System Architecture. In: *Proceedings of the 2nd Annual IEEE Systems Conference*, Montreal, Quebec, Canada, 2008.
12. IFIP. WG 10.4 on Dependable Computing and Fault Tolerance. [Online] February 15, 2011. http://www.dependability.org/wg10.4/.
13. Avizienis, A, Laprie, JC, Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*. January-March 2004, Vol. 1, 1.