DOCUMENT NUMBER MTR110237

MITRE TECHNICAL REPORT

MITRE

Cyber Resiliency Engineering Framework

Deborah J. Bodeau & Richard Graubart

September 2011

Dept. No.: G020
Project No.: 05MSR160-JT

Bedford, MA

Approved By:

//Jeffrey Picciotto, Project Leader//	30 December 2011
Name and Title of Approval Signature	Date

Abstract

Missions, business functions, organizations, and nations are increasingly dependent on cyberspace. The need for cyber resiliency – for information and communications systems and those who depend on them to be resilient in the face of persistent, stealthy, and sophisticated attacks focused on cyber resources – is increasingly recognized. While resilience is sometimes described as an emergent property, resilience in the face of cyber threats must be engineered. Cyber resiliency engineering is the sub-discipline of mission assurance engineering which considers (i) the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and (ii) the trade-offs associated with different strategies for applying those practices. This paper presents an initial framework for cyber resiliency engineering. The framework identifies

- Cyber resiliency goals, objectives, and practices;
- The threat model for cyber resiliency;
- Architectural layers or domains to which cyber resiliency practices could be applied; and
- Aspects of cost to consider as part of the trade-off analysis for alternative strategies and implementations.

This framework provides a way to structure discussions and analyses of cyber resiliency goals, objectives, practices, and costs. It also serves to motivate and characterize cyber resiliency metrics. The framework is intended to evolve as the discipline of cyber resiliency engineering matures. To provide feedback or participate in discussions of how to apply or improve the framework, please contact

Deborah Bodeau	Richard Graubart	Jeffrey Picciotto	Rosalie McQuaid
dbodeau@mitre.org	rdg@mitre.org	jp@mitre.org	rmcquaid@mitre.org
781-271-8436	781-271-7976	781-271-3714	781-271-7676

This page intentionally left blank.

Executive Summary

Missions, business functions, organizations, critical infrastructures, and nations are increasingly dependent on cyberspace. The need for cyber resiliency – for information and communications systems and those who depend on them to be resilient in the face of persistent, stealthy, and sophisticated attacks focused on cyber resources – is increasingly recognized. The relatively new discipline of cyber resiliency engineering has been defined to meet the challenge of how to evolve architectures, cyber resources, and operational processes to provide cost-effective cyber resiliency.

Cyber resiliency engineering is a part of mission assurance engineering, and is informed by a variety of disciplines, including information system security engineering, resilience engineering, survivability, dependability, fault tolerance, and business continuity and contingency planning. Cyber resiliency engineering considers (i) the ways in which an evolving set of architectural resilience practices contribute to the resilience of a set of cyber resources in light of the cyber threat, and (ii) the engineering trade-offs associated with those practices. Examples of sets of cyber resources include mission or business segments, common infrastructures, shared services, systems-of-systems, networks, systems, and data repositories.

This paper presents an initial framework for cyber resiliency engineering. The framework identifies cyber resiliency goals, objectives, and practices; the threat model for cyber resiliency; architectural layers or domains to which cyber resiliency practices could be applied; and aspects of cost to consider as part of the trade-off analysis for alternative strategies and implementations. The framework is intended to evolve as the discipline of cyber resiliency engineering matures.

Cyber resiliency goals are

- Anticipate: maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks,
- Withstand: continue essential mission/business functions despite successful execution of an attack by an adversary,
- Recover: restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary, and
- Evolve: to change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks.

Reaching these goals requires achieving cyber resiliency objectives: understand, prepare, prevent, constrain, continue, reconstitute, transform, and re-architect. Cyber resiliency objectives are applied to systems, architectures, and mission/business functions synergistically to improve resiliency. These in turn are supported by a set of cyber resiliency practices. The set of resilience practices considered by cyber resiliency engineering is evolving, as research and investigation provide possible solutions and as experience applying the practices to architectures, systems, and operational processes is gained. The set of resilience practices considered in this framework are adaptive response, privilege restriction, deception, diversity, substantiated integrity, coordinated defense, analytic monitoring, non-persistence, dynamic positioning, redundancy, segmentation, unpredictability, dynamic representation, and realignment. Each practice has operational as well as technical aspects.

Cyber resiliency engineering supports a wide range of stakeholders, including

- Mission commanders (or business function heads), who need to know how well they can perform their missions (or business functions).
- Cyber defenders (e.g., Computer Network Defense staff; staff in a Security Operations Center or a Cyber Security Operations Center), who need to achieve cyber resiliency goals in their operational environments.
- Providers and operators of information and communications technologies and services (e.g., the manager of a fixed-site facility that provides computing resources to multiple missions or users, the provider of a common infrastructure or set of shared services), who need to ensure adequate cyber resiliency for their offerings.
- Program managers (as informed by systems engineers and architects), who need to make decisions related to cost-benefit trade-offs of cyber resiliency investments and decisions related to programmatic risk management.
- Architects and systems engineers, who need to decide which cyber resiliency practices to apply, where, how, and in what timeframe.
- Test and exercise planners, who need to decide how to represent threats to cyber resiliency in their efforts.

The framework presented in this paper provides a way to structure discussions and analyses of cyber resiliency goals, objectives, practices, and costs. It also serves to motivate and characterize cyber resiliency metrics. The framework is intended to evolve as the discipline of cyber resiliency engineering matures. To provide feedback or participate in discussions of how to apply or improve the framework, please contact

Deborah Bodeau	Richard Graubart	Jeffrey Picciotto	Rosalie McQuaid
dbodeau@mitre.org	rdg@mitre.org	jp@mitre.org	rmcquaid@mitre.org
781-271-8436	781-271-7976	781-271-3714	781-271-7676

Table of Contents

List of Figures and Tables

This page intentionally left blank.

1 Introduction

The need for cyber resiliency – for information and communications systems and the missions and business functions which depend on them to be resilient in the face of persistent, stealthy, and sophisticated attacks focused on cyber resources – is increasingly recognized. While resilience is sometimes described as an emergent property, resilience in the face of cyber threats must be engineered. Cyber resiliency engineering is the sub-discipline of mission assurance engineering which considers (i) the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and (ii) the trade-offs associated with different strategies for applying those practices. This paper presents an initial framework for cyber resiliency engineering. The framework identifies

- Cyber resiliency goals, objectives, and practices;
- The threat model for cyber resiliency;
- Architectural layers or domains to which cyber resiliency practices could be applied; and
- Aspects of cost to consider as part of the trade-off analysis for alternative strategies and implementations.

The framework is intended to evolve as the discipline of cyber resiliency engineering matures.

Cyber resiliency engineering is a relatively new discipline, building on a variety of systems engineering disciplines to address the question:

> How can information systems, systems-of-systems, and the mission or business processes they support, be engineered to provide resilience in the presence of advanced cyber threats?

That is, cyber resiliency engineering considers (i) the ways in which an evolving set of architectural resilience practices contribute to the resilience of a set of cyber resources (e.g., a mission or business segment[1], a common infrastructure, a set of shared services, a system-of-systems) in light of the cyber threat, and (ii) the engineering trade-offs associated with those practices. Key resilience practices are discussed in Section 4, and are based on those articulated in (Goldman, 2010).

Engineering trade-offs take into account the costs of the different strategies for applying resiliency practices, as well as potential benefits beyond improved resilience (e.g., improved management or accountability). Engineering trade-offs typically involve the use of metrics[2] (Trade-off Strategies in Engineering Design, 1991), and treat cost and other decision factors as multi-dimensional. Thus, the framework is constructed to facilitate the definition and characterization of metrics.

A wide range of stakeholders need to make decisions related to cyber resiliency, including:

[1] A mission/business segment is the set of cyber resources – including information systems, common infrastructures (e.g., networks), shared services (e.g., Web services), and data stores – used to execute a mission or business process. An information system is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." (NIST, 2011) A system-of-systems consists of "multiple independent information systems (possibly distributed across a widespread geographic area) supporting a set of common missions and/or business functions." (NIST, 2010)

[2] In this document, a metric is the result or product of an assessment process, and can be quantitative, qualitative, or semi-quantitative (Risk Steering Committee, 2010). A quantitative metric can be a measure (i.e., the result of counting or otherwise quantifying an attribute (INCOSE, 1998)), or can be computed from multiple measures.

- Mission commanders (or business function heads), who need to know how well they can perform their missions (or business functions).
- Cyber defenders (e.g., CND staff; staff in a Security Operations Center or a Cyber Security Operations Center), who need to make decisions about how to achieve cyber resiliency goals in their operational environments.
- IT/ICT providers and operators (e.g., the manager of a fixed-site facility that provides computing resources to multiple missions or users, the provider of a common infrastructure or set of shared services), who need to determine how to ensure adequate cyber resiliency for their offerings.
- Program managers (as informed by systems engineers and architects), who need to make decisions related to cost-benefit trade-offs of cyber resiliency investments and decisions related to programmatic risk management.
- Architects and systems engineers, who need to decide which cyber resiliency practices to apply, where, how, and in what timeframe.
- Test and exercise planners, who need to decide how to represent threats to cyber resiliency in their efforts.

This document presents an initial framework for cyber resiliency engineering, and situates cyber resiliency engineering among other systems engineering sub-disciplines. Section 2 provides background on how cyber resiliency can be characterized. Section 3 situates cyber resiliency engineering in the context of related disciplines; additional information can be found in Appendix B. Section 4 presents the cyber resiliency engineering framework. The framework can be used to frame discussions of cyber resiliency among disparate stakeholders, and to motivate and characterize cyber resiliency metrics.

Cyber resiliency metrics and the process for assessing architectural resiliency will be presented in future documents. The cyber resiliency engineering framework provides a way to motivate and characterize cyber resiliency metrics. When an organization uses metrics, the question arises of whether the metrics focus on a small subset of the problem domain or cover the problem domain comprehensively. The cyber resiliency engineering framework enables an organization to select a set of cyber resiliency metrics that adequately cover their cyber resiliency domain.

2 Cyber Resiliency: Characterization as Work in Progress

The concept of resilience – the ability to "bounce back" from an adverse event – has been extended from material science and the psychological domain to such domains as ecology, systems engineering (Jackson, 2009), organizational behavior, and homeland security (HSSIA, 2009). The term "resilience" (or resiliency[3]) has been variously modified, to provide such phrases as cyber resilience, cyber resiliency, and mission resilience. The following paragraphs provide background on the growing and varied uses of the term "resilience," briefly discuss the cyber threat and cyber security, and present working definitions of cyber resiliency and related terms.

2.1 Characterizing Resilience

As illustrated in Table 1 below, "resilience" is increasingly applied, with varying definitions, to the Nation, critical infrastructures, organizations, networks, and systems. Common aspects include preparing for, preventing, or otherwise resisting an adverse event; absorbing, withstanding, or maintaining essential functions in the face of the event; recovering from the event; and adapting to (changing processes, systems, or training based on) the event, its consequences, and its implications for the future. Different definitions emphasize or organize these aspects in varying ways, depending largely on what needs to be resilient.

Table 1. Definitions of Resilience Differ, Depending on Scope

Scope	Definition
Nation	"The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption" (White House, 2010) "The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies" (White House, 2011) (cited in (Preparedness, Response, and Resilience Task Force, 2011)).
Critical Infrastructure	"Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event." (NIAC, 2010)
Defense Critical Infrastructure	"The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change." (DoD, 2008)
Cyberspace	"The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption." (Risk Steering Committee, 2010) "Cyberspace resilience is much more than networks. . . It is the flexibility, adaptability, and trustworthiness among the human, the physical, and the information domain. … Cyberspace resilience is the ability to operate through cyber conflict and recover quickly to a trusted environment." (Bargar, 2009)
Space	"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." (DoD, 2011)
Organization (Operational Resilience)	"The ability of the organization to achieve its mission even under degraded circumstances" "The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk." (CERT Program, 2010)

[3] "Resilience" and "resiliency" are synonyms with a long history of use. (Napoli, 2007) In this paper, "resiliency" is used to help differentiate the emerging discipline of *cyber* resiliency engineering from the discipline of *resilience engineering*.

Scope	Definition
Organization (Contingency Planning)	"The ability to quickly adapt and recover from any known or unknown changes to the environment. Resiliency is not a process, but rather an end-state for organizations. The goal of a resilient organization is to continue mission essential functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions." (NIST, 2010)
Mission	Ensuring that "critical mission processes continue to operate regardless of any threats that exist" (Cole, et al., 2009) "Mission resilience is a multi-tiered, life-cycle-focused methodology for understanding, anticipating, mitigating and minimizing the effects of any material disruption." (accenture, 2008)
Architecture	"The ability of a whole architecture to provide functional capabilities necessary for mission success despite environmental adversity or hostile action." (Schulte, 2011)
Network	"The ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation." (Sterbenz, et al., 2006)
System	"The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs." (NIST, 2011) "Resilience is designed to have systems self-heal with no intervention from humans. In the cyber context, a resilient cyber system must continue to operate as intended, even if compromised (for example, if unauthorized access is achieved)." (TASC, 2011) "System resilience is defined as the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks." (Haimes, et al., 2008) (Haimes, 2009)
Control System	"A resilient control system can be defined as one that maintains state awareness at an accepted level of operational normalcy in response to anomalies, including threats of a malicious and unexpected nature." (Rieger, et al., 2009)

Resilience is variously defined or characterized by different engineering disciplines, as discussed in Section 3. These characterizations, together with the definitions and characterizations identified in this section, were taken into consideration in the working definition of cyber resiliency.

In the cyber domain, resilience concepts must be adapted to take into consideration cyber threats, initial characterizations of cyber resiliency, and the relationship between cyber resiliency and both cyber security and computer network defense (CND). As noted above, "resilience" typically assumes an adverse event (for which the duration of its effects may be unspecified, but which typically is itself narrowly bounded in time). When advanced cyber threats are considered, no single event may be identifiable. Adversary actions can be part of a long-term campaign (Krekel, 2009) (Space Daily Staff, 2011).

2.1.1 Cyber Threats

A clear model of the threat is crucial to defining resilience goals.[4] Cyber threats are variously characterized – for example, in terms of behavior and in terms of adversary characteristics. Adversary *characteristics* can be categorized as capabilities, intent, and targeting (Bodeau, et al., 2010).

The cyber kill chain is a way to describe the *behavior* or activities of a stealthy, persistent adversary who uses malware to gain a foothold in an organization's or mission's systems and then uses that foothold to achieve objectives. The components of the cyber kill chain (Cloppert, 2009) (Croom, 2010) are

[4] "A systematic [threat] taxonomy is necessary for guiding research and development efforts and for assessing systems under development for their resilience against the whole threat spectrum." (CIANCNF, 2010)

- Reconnaissance: Obtaining information to conduct the attack.
- Weaponization: Placing the payload in a delivery vehicle (e.g., a hyperlink to a malware-tainted site in a phishing email, malware in an attachment to a targeted email).
- Delivery: Sending the attack vehicle to the potential victim.
- Exploitation/installation: Exploiting system vulnerabilities to install malware on the victim system. This is identified as the pivotal point in the cyber kill chain. (Cloppert, 2009)
- Command and control: Directing the victim system to take actions (e.g., to download additional malware, to perform more advanced reconnaissance within the enterprise information infrastructure, to propagate malware to other systems).
- Actions to achieve adversary objectives: Depending on the adversary's objectives, these may include exfiltrating data, corrupting mission or organizational data or replacing it with deceptive data, and degrading or denying the functionality of cyber resources.
- Maintenance: Taking actions to ensure future access (e.g., changing the profile of adversary-installed malware, modifying logs).

2.1.2 Evolving Characterizations of Cyber Resiliency

In 2010, Goldman identified objectives for resilient architectures and corresponding properties or characteristics, as well as strategies for achieving resilience (Goldman, 2010). Resilience concepts from health (DARPA, 2010) (Edwards, 2011) and ecology (DHS, 2011) (ENISA, 2010) have been applied to cyberspace. Multiple characterizations of cyber resiliency strategies and architectures have emerged from the research community, as shown in Table 2.

Table 2. Cyber Resiliency as Characterized by the Research Community

Source	Characterization
DoD Cyber S&T Priority Steering Council (King, 2011)	A resilient infrastructure will withstand cyber attacks, and sustain or recover critical functions. Resilient architectures are characterized by • Resiliency for operational systems • Mechanisms to compose resilient systems from brittle components • Integration of sensing, detection, response, and recovery mechanisms • Secure modularization and virtualization of nodes and networks • Resiliency-specific modeling and simulation
DARPA **(Shrobe, 2011)**	Cyber-mission resilience is supported by resilient clouds technology: • Mission-aware networking • Optimizing mission & resources • Innate distributed defense • Shared situational awareness, trust modeling, and diagnosis • Manageable and taskable diversity These are supported by CRASH technologies: innate immunity, adaptive immunity, and manageable diversity.
CyberCARD workshop (CyberCARD, 2011) (Eltoweissy, 2011)	Four elements of a cyber resiliency R&D strategy: • Trustworthy socio-cyber-physical (SCP) systems and infrastructures; • Pervasive monitoring and analysis; • Cooperative autonomous defense; and • Attack-resilient operations, including the ability to "fight through" attack to achieve mission objectives
MITRE (Swarup, 2009)	Enable structured cyber assets to tolerate some component compromises

2.1.3 Cyber Resiliency and Cyber Security

Cyber security (or cybersecurity) is defined as "the ability to protect or defend the use of cyberspace from cyber attacks" (CNSS, 2010) or "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (Merriam-Webster, 2011). These definitions contrast with definitions of information security[5], by emphasizing the concern with cyber attack and with cyberspace. It must be noted, however, that many discussions of cyber security typically leave the terms "cyber attack" and "cyberspace" undefined.[6]

Cyber resiliency can be viewed as part of cyber security, particularly at the national level: "Our Nation's cybersecurity strategy is twofold: (1) improve our resilience to cyber incidents and (2) reduce the cyber threat." (NSC, undated) However, cyber security is generally construed more broadly, to include trust (White House, 2009) or safety (OCS, 2009).

Cyber resiliency can also be viewed as integral to computer network defense or cyber operations. The strategy the office of the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance (CIIA) (ASD(CIIA), 2009) includes two goals which motivate the CND Architecture. (Bingham, 2011) These are

- "Anticipate and prevent successful attacks on data and networks" and
- "Prepare for and operate through cyber degradation or attack."

Key to anticipating and preventing successful attacks are understanding the (cyber) battlespace by knowing the adversary, knowing the network, and understanding cyber effects; preventing and delaying attackers from getting into the network; and preventing attackers from establishing a foothold or acting. Key to preparing are enabling cyber event response; exercising under realistic scenarios; identifying critical cyber assets; and improving continuity planning. Key to operating through are responding to cyber events; sustaining mission-critical functions under degradation; and reconstituting critical cyber assets. (Bingham, 2011)

The Booz | Allen | Hamilton maturity model for cyber operations (Booz | Allen | Hamilton, 2011) identifies four key functions, with supporting activities:

- Anticipation, supported by threat identification and analysis, systemic vulnerability assessment, contingency planning, and training and exercises;
- Awareness, supported by continuous scanning and monitoring, indications and warnings, and intrusion detection and prevention;
- Action, supported by impact analysis and incident response; and
- After-action, supported by forensics and analysis as well as post-incident analysis and adoption.

[5] Information security can be defined as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (NIST, 2011)

[6] The Cyberspace Operations Lexicon defines "cyber attack" as "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves – for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability." (JCS, 2009)

These functions are event-driven, following the "pre-event / post-event" approach which underpins most contingency planning models. The maturity model is intended to support the evolution of a secure cyber ecosystem (DHS, 2011).

2.2 Working Definitions

The definitions and characterizations of resilience cited above emphasize different aspects of the cyber resiliency problem domain, while omitting or glossing others (e.g., by focusing solely on systems or solely on organizations, by omitting anticipation, by implicitly assuming a single-event threat model). The working definitions presented in this section are intended to cover the full problem domain, serve as a starting point for discussion and further refinement by the larger community of potential stakeholders, be consistent with existing definitions, broad enough to cover the problem domain, and able to be tailored to more specific environments. For purposes of this document, the following definitions are used:

Cyberspace is

> "The collection of information and communications technology (ICT) infrastructures, applications, and devices on which the organization, enterprise, or mission depends, typically including the Internet, telecommunications networks, computer systems, personal devices, and (when networked with other ICT) embedded sensors, processors, and controllers." (Bodeau, et al., 2010)

This definition is designed to be consistent with a variety of existing characterizations (NDIA, 2009) (DoD, 2006) (ITGI and ISACA, 2006) (NIST, 2004) (CMMI Team, 2007). In particular, cyberspace can include the networked components of an organization's physical security system (badge readers, access logging system, etc.).

Cyber resources are

> "Separately manageable resources in cyberspace, including information in electronic form, as well as information systems, systems-of-systems, infrastructures, shared services, and devices."

This definition is provided to simplify the definition of cyber resiliency. It emphasizes that information must be considered a resource, as well as hardware and software. Different views of cyberspace could result in identifying resources differently; this definition uses the ability to manage a resource as the key factor.

A *cyber attack* is

> "An attack on cyber resources. The attack is typically, but not necessarily, carried out by cyber means. The attack may be intended to adversely affect the cyber resources, or to adversely affect the missions, business functions, organizations, or populations that depend on those resources."

This definition is designed to be consistent with a variety of existing characterizations (O'Shea, 2003), (JCS, 2009), (Beidleman, 2009), (CNSS, 2010), (Roscini, 2010).

Cyber resiliency is

> **"The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities[7] in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function."**

"Adverse conditions" and "stresses" include not only the faults, errors, surges in demand, and failures of supporting infrastructures (e.g., power loss due to natural disaster) considered in contingency planning, but also adversary activities that have not risen to the level of an attack (e.g., reconnaissance).

This definition of cyber resiliency deliberately accommodates two complementary (overlapping but not identical) interpretations, which emphasize different parts of the definition: cyber resiliency as resiliency of the set of cyber resources on which a mission, business process, or organization depends; and cyber resiliency as resiliency of the mission, business process, or organization in the face of cyber threats. Thus, cyber resiliency has an operational aspect as well as a technical one.

This definition is designed to be consistent with existing characterizations of resilience (see Tables 1 and 2 above, as well as Appendix B), and in particular to provide a foundation for a cyber resiliency engineering framework consistent with a resilience engineering framework (Madni, et al., 2009). It accommodates application at all tiers of the Risk Management Hierarchy defined in (NIST, 2011), but is particularly appropriate to the mission/business tier. It also accommodates missions and business functions that transcend organizational boundaries, and reflects the growing body of work on cyber resiliency at the national level (DHS, 2011).

Cyber resiliency engineering is

> **"The sub-discipline of mission assurance engineering which considers (i) the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and (ii) the trade-offs associated with different strategies for applying those practices."**

See Section 3.3 for further discussion of mission assurance engineering. As discussed in Section 4, resilience practices have operational as well as technical aspects. Thus, cyber resiliency engineering, like mission assurance engineering and resilience engineering, encompasses process engineering as well as architectural definition and systems engineering. Cyber resiliency engineering can be

- Used to define or refine resilient architectures;
- Integrated with the engineering process for systems (including common infrastructures and shared services), systems-of-systems, mission/business segments to ensure that resilience concerns are addressed; and
- Applied in operational environments to improve operational resilience.

[7] A capability is the ability to perform some action (or "the ability to execute a course of action" (DoD, 2011)), and is frequently identified with the set of resources used in the performance of that action.

3 Situating Cyber Resiliency Engineering

This section situates cyber resiliency engineering as informed by resilience engineering, as building on and extending information systems security engineering, and as part of Mission Assurance Engineering (MAE). The relationship between cyber resiliency engineering and other systems engineering disciplines is illustrated in Figure 1 and discussed in Appendix B, with attention to how resilience can be assessed or measured, the relationship between resilience and risk, and research which might be relevant to cyber resiliency.

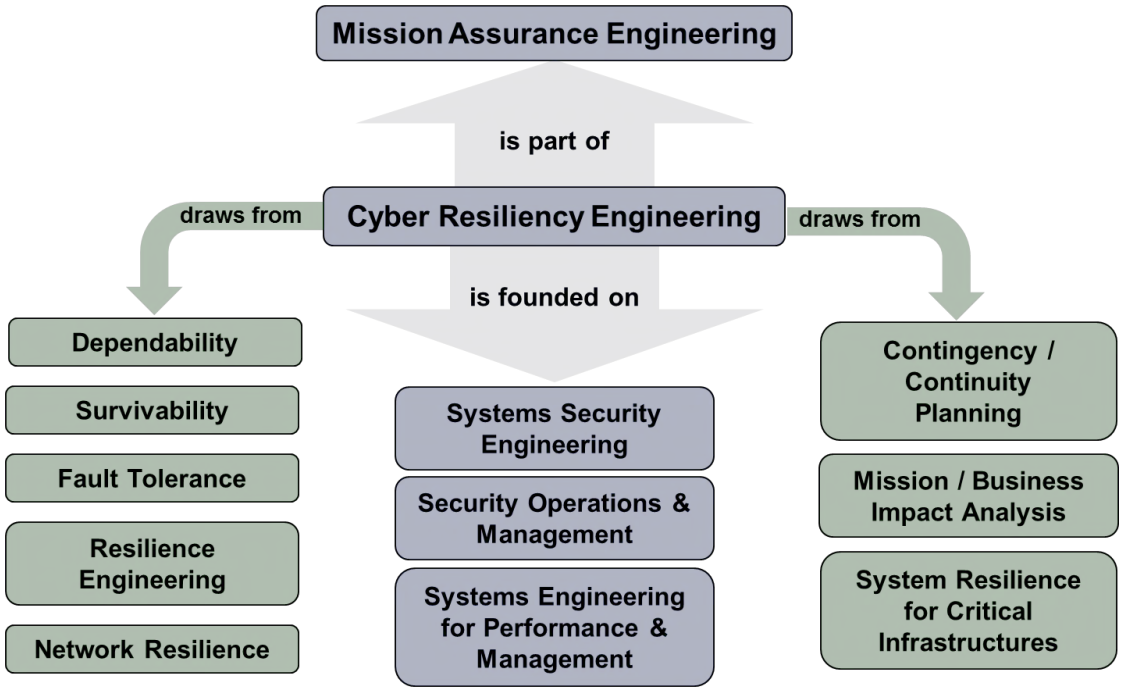

Figure 1. Cyber Resiliency Engineering in Context

3.1 Resilience Engineering

Cyber resiliency engineering could be characterized as resilience engineering focused on cyber threats. Certainly, the cyber resiliency engineering framework presented in Section 4 is informed by frameworks and heuristics developed by resilience engineers. However, the cyber resiliency engineering framework focuses on architectural strategies and practices, emphasizing technical systems; socio-technical aspects are treated as supporting rather than central.

Madni defines four aspects of resilience which can be interpreted with respect to the cyber threat ((Madni, 2007), quoted in (Madni, et al., 2009)):

- Avoid (anticipation)[8]
- Withstand (absorption)

[8] "Resilience involves anticipation. This includes the consideration of how and why a particular risk assessment may be limited, having the resources and abilities to anticipate and remove challenges, knowing the state of defenses now and where they may be in the future, and knowing what challenges may surprise. Taking a prospective view assumes that challenges to system performance will occur, and actively seeks out the range and details of these threats." (Nemeth, 2008)

- Recover from (restoration)
- Adapt to (reconfiguration)

Based on an extensive literature review, Madni defines a conceptual framework for resilience engineering. In that framework, system attributes are affected by disruptions, which can be natural or man-made; external or systemic; single-agent or multi-agent; and short-lived or enduring. For cyber resiliency, disruptions are typically man-made, but can involve deliberate exploitation of transient vulnerabilities resulting from natural disaster; disruptions can be systemic (i.e., the result of actions within the system) when malicious insiders are involved, but are more typically externally created; prudence suggests assuming multiple agents and enduring disruption.

3.2 Information Systems Security Engineering

Information systems security engineering applies generally accepted engineering principles and practices throughout the system life-cycle to achieve the information security goals of confidentiality, integrity, and availability[9]. Some security engineering principles are specific to resilience (Stoneburner, et al., 2004):

- "Principle 16. Implement layered security (Ensure no single point of vulnerability).
- Principle 17. Design and operate an IT system to limit damage and to be resilient in response.
- Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- Principle 19. Limit or contain vulnerabilities.
- Principle 20. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
- Principle 21. Use boundary mechanisms to separate computing systems and network infrastructures.
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability."

Cyber resiliency engineering differs from information systems security engineering (ISSE) in its threat model: Cyber resiliency engineering focuses on persistent, stealthy, and sophisticated adversaries who seek to undermine current or future mission or business functions. Such adversaries can exploit events caused by threat sources (e.g., natural disasters, structural failures) and can take actions difficult to distinguish from threat events (e.g., user error) considered by ISSE. The threat model for cyber resiliency engineering is described in Section 4.2.

Cyber resiliency involves more than achieving the information security goal of availability, even with its more specific threat model. Cyber resiliency includes not only protecting critical

[9] Accountability – the ability to construct a clear account of what happened (e.g., what actions were taken, what events occurred, what resources were involved, what the effects of the actions or events were on those resources) and who was accountable (e.g., individuals, organizations, systems, software components, hardware components) – is sometimes cited as a fourth security goal.

resources from degradation or denial of service prior to or during an attack, but also ensuring their integrity, recovering or reconstructing mission functionality, and evolving to be better prepared for new threats. Cyber resiliency goals are described in Section 4.1.1. (The relationship between resiliency and accountability is an area for further investigation.)

Cyber resiliency engineering assumes that sound information systems security engineering is performed. Without risk-appropriate security controls in systems, services, and networks, the cyber resiliency practices described in Section 4.1.3 can be circumvented or bypassed. In addition, some of those practices (e.g., analytic monitoring) use the functionality or information provided by security controls.

3.3 Mission Assurance Engineering

Mission assurance engineering (MAE) can be defined as enterprise systems engineering to provide mission assurance in the presence of advanced threats (see Section 4.2 below). MAE extends established practices in information systems security engineering and enterprise systems security engineering to focus directly on the advanced persistent threat. MAE includes the emerging discipline of cyber resiliency engineering, which addresses the mission/business process tier in the NIST Risk Management Hierarchy. MAE includes several sub-disciplines: cyber-aware enterprise transformation strategies (Bodeau, et al., 2010), cyber resiliency engineering, system/acquisition mission assurance engineering, and information systems security engineering. Figure 2 illustrates the relationships between cyber resiliency engineering and other mission assurance engineering disciplines.

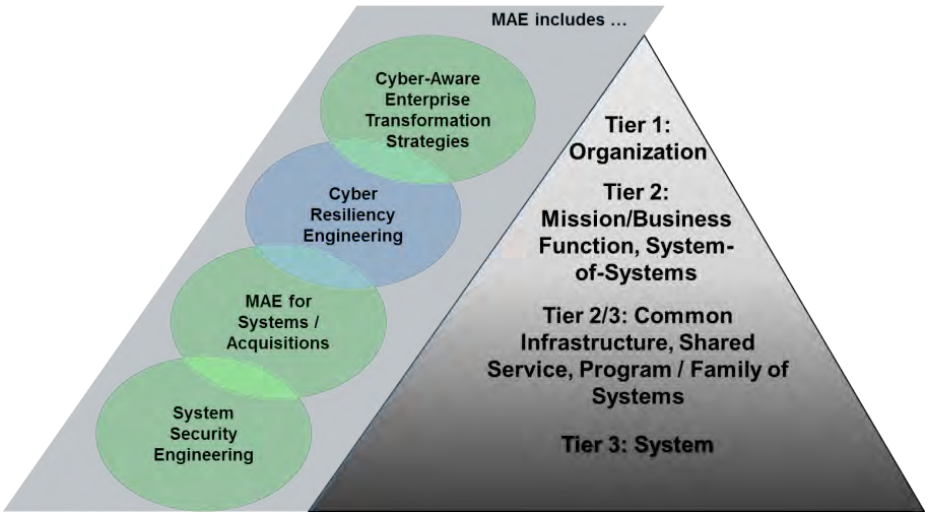

Figure 2. Mission Assurance Engineering Sub-Disciplines and the Risk Management Hierarchy[10]

As discussed in (Goldman, 2010), cyber resiliency engineering focuses on applying architectural practices and mechanisms to improve cyber resiliency. Cyber resiliency engineering builds on information systems security engineering; it assumes (and sometimes provides additional motivation for) security controls that enable systems to meet the security policy objectives of confidentiality, integrity, and availability. Cyber resiliency engineering also builds on – and

[10] Note that Tier 2/3 does not appear in the multi-tiered approach to risk management in NIST SP 800-39 (NIST, 2011); however, many acquisition programs involve families of systems or services rather than individual systems.

overlaps with – system/acquisition MAE,[11] since cyber resiliency practices (as discussed in and described in more detail in Section 4.1.3 below) can be applied to systems and to families of systems.

However, the analysis of the effectiveness of, and trade-offs involving, these practices must be performed at Tier 2, the mission/business function tier. A mission or business segment[12] can and should have a resilience architecture – a pattern of resilience practices and mechanisms, in the context of functional and infrastructure patterns which are typically described using diagrams and identified standards. Thus, cyber resiliency engineering focuses on the mission/business function tier.

Cyber resiliency engineering is informed by the organization's culture, mission priorities and risk tolerance, and risk framing. (See (NIST, 2011) for further discussion.) In particular, cyber resiliency engineering is informed by the set of threats that the organization seeks to address. Cyber resiliency engineering overlaps with MAE at the organizational tier, in that it informs as well as is informed by the organization's investment and risk management strategies.

[11] "Systems engineering for mission assurance is the art of engineering into systems: (1) the capabilities for operators to be aware of different and changing adversarial strategies as well as environmental and system conditions, (2) options and alternatives to accomplish a mission under different circumstances, (3) tools to assess and balance advantages and risks of available response options and alternatives, and (4) the ability to transition to a selected option while simultaneously continuing the mission. Systems engineering for mission assurance extends throughout the entire traditional acquisition life cycle, from concept development through deployment and beyond, to include supply chain considerations and field operations." (MITRE, 2011)

[12] A mission/business segment consists of "elements of organizations describing mission areas, common/shared business services, and organization-wide services" (NIST, 2011). Thus, a mission/business segment can be identified with a set of systems which collectively support a mission/business process.

4 Cyber Resiliency Engineering Framework

The cyber resiliency engineering framework being developed under the RAMBO initiative consists of four major components:

- Elements of cyber resiliency:
  - What are the goals and objectives of cyber resiliency? That is, how can the definition of cyber resiliency be expanded to be useful for investment planning or change management?
  - What practices[13] (also referred to as techniques, strategies, or approaches) can be applied to meet those goals and objectives?
- Threat model: What threats are cyber resiliency practices intended to address?
- Applicability domains: Where – to which architectural layers or to which sets of cyber resources – are cyber resiliency practices, measures (controls, mechanisms, procedures), and solutions (specific products or implementations) applied?
- Aspects of cost: What types of costs (and non-resiliency-specific benefits) are associated with the use of a cyber resiliency practice, mechanism, or specific product or implementation?

As illustrated in Figure 3, these framework components enable cyber resiliency engineering to be informed by three distinct but related disciplines: resilience engineering, cyber security, and mission assurance engineering.

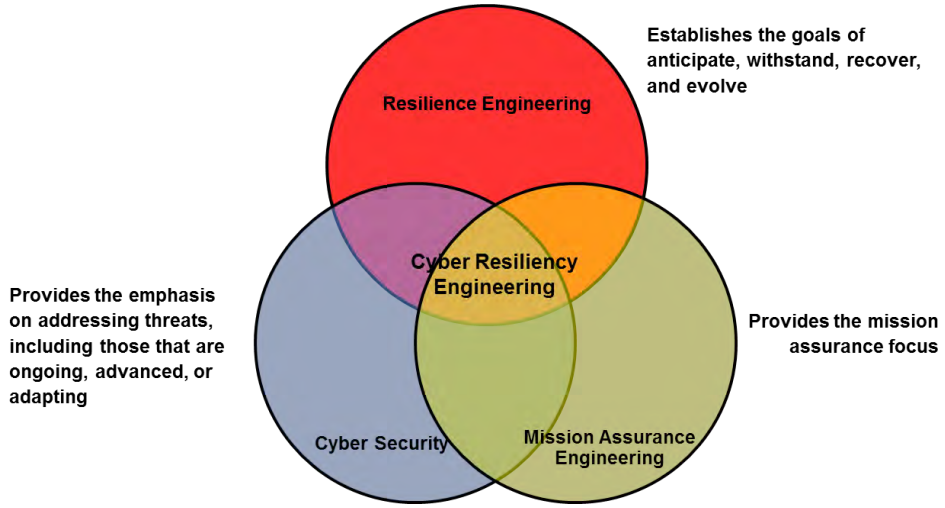

Figure 3. Key Sources for the Cyber Resiliency Engineering Framework

The cyber resiliency engineering framework draws the goals of anticipate, withstand, recover from, and evolve from resilience engineering. The emphasis on addressing threats, including advanced and ongoing and adapting threats from cyber security, is drawn from cyber security. The mission focus in the definitions of goals and objectives is drawn from mission assurance engineering. The recognition that practices are applied in different ways and to different degrees

[13] As noted in Section 2.3, cyber resiliency engineering encompasses processes for integrating resilience into operations and for managing technological solutions as well as for integrating those solutions into an architecture. Thus, a cyber resiliency practice needs to be relevant not only to systems engineering and architectures, but also to operations.

at different architectural layers, and that multiple aspects of cost must be considered, are drawn from all three disciplines. The components of the cyber resiliency engineering framework are discussed in more detail below.

4.1 Elements of Cyber Resiliency

This section defines cyber resiliency goals, objectives, and practices.

- Goals are high-level statements of intended outcomes.
- Objectives are more specific statements of intended outcomes, expressed so as to facilitate assessment; an objective can be identified with a single goal but may support achieving multiple goals.
- Practices 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. Practices are selectively applied to the architecture or design of mission/business functions and the cyber resources that support them to achieve objectives; a given practice usually supports multiple objectives but may be unique to a single objective.

These elements of cyber resiliency, and the relationships among them, provide a partial and informal ontology[14] of cyber resiliency. This partial ontology is intended to aid in understanding how different cyber resiliency practices contribute to achieving cyber resiliency goals. It is also intended to enable cyber resiliency metrics to be characterized in terms of the types of questions the metrics can be used to answer.

The elements of cyber resiliency consist of four goals (Anticipate, Withstand, Recover, and Evolve), eight objectives (Understand, Prepare, Prevent, Continue, Constrain, Reconstitute, Transform, and Re-architect), and an extensible set of (currently fourteen) practices (Adaptive Response, Privilege Restriction, Deception, Diversity, Substantiated Integrity, Coordinated Defense, Analytic Monitoring, Non-persistence, Dynamic Positioning, Redundancy, Segmentation, Unpredictability, Dynamic Representation, and Realignment) that are intended to maximize cyber resiliency. The various goals, objectives and practices do not stand in isolation. For example, unpredictability (a practice) can play a key role in achieving effective deception (another practice).

This section also provides a mapping between goals and objectives, and between objectives and practices. Thus, it shows which objectives support which goals, and which practices support which objectives.

4.1.1 Cyber Resiliency Goals

As noted above, cyber resiliency is defined as enabling the nation, organization, mission or business owner, or resource provider to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions or stresses due to cyber threats. Thus, cyber resiliency practices address four goals:

[14] This ontology is informal, i.e., it is intended to facilitate discussion and analysis by humans rather than to support automated knowledge management. This ontology is partial; it does not attempt to cover the complete cyber resiliency problems space, which could include concepts and terms related to adversaries, adversary activities, and related disciplines and the techniques and mechanisms specific to those disciplines that could contribute to cyber resiliency (e.g., generally accepted security measures, dependability techniques and mechanisms). Research is underway to develop a more complete and less informal resilience ontology (ENISA, 2011).

- Anticipate
- Withstand
- Recover
- Evolve

A key feature of this part of the cyber resiliency framework, as contrasted with resilience frameworks which assume a precipitating adverse event, is the assumption that all four goals must be addressed simultaneously. For example, even while withstanding or recovering from a cyber attack, the mission or business owner or the resource provider must anticipate other attacks. Even while anticipating, withstanding, or recovering from attacks, mission/business segments or the mission or business processes that rely on them are constantly evolving, to address changing (ENISA, 2011)operational and technical environments. And part of anticipation is withstanding stresses within some bounded range.

These four goals are consistent with those defined by (Madni, et al., 2009); however, evolution is a more extensive aspect than adaptation. Hollnagel's four cornerstones of resilience engineering are anticipation, monitoring, response, and learning (Hollnagel, 2009); evolution corresponds to learning, while withstand and recover correspond to response, and monitoring is treated as a technique needed by all aspects. These first three goals are consistent with the three phases (preparation, service delivery, and recovery) identified by ENISA (ENISA, 2011). While monitoring could be identified as a goal (see also (Sterbenz, et al., 2011), where "diagnose" and "detect" are distinct resilience processes related to monitoring), for cyber resiliency monitoring is more usefully characterized as a practice which plays different roles depending on which cyber resiliency goals are considered.

4.1.1.1 Anticipate

For cyber resiliency, to anticipate is to *maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks*[15]. Reaching this goal involves meeting three objectives:

- Predict
- Prevent
- Prepare

To predict attacks, organizational capabilities are needed to obtain and analyze threat intelligence. Threat information is derived from organizationally sanctioned sources (Bodeau, et al., 2010), from monitoring the mission environment (human behavior and physical facilities as well as information systems) for evidence or indications of adversary activity, and from detection of adverse or anomalous events. Cyber threat analytics include threat modeling based on threat information, consequence modeling, and assessment (Bodeau, et al., 2010).

[15] The term "attack" is used to refer to adversary activities intended to cause damage, primarily to compromise a mission/business function (i.e., to impair or impede execution of that mission or business function, for example by denying functionality or service or by corrupting mission-essential information), but also to undermine future mission/business functions (e.g., by exfiltrating information). The term "activity" is used to include a broader range of behaviors, and specifically includes intelligence gathering (e.g., probing) and insertion (e.g., inserting malware into systems or trapdoors into commercial components, putting an agent in place as an insider); such activities may lay the foundation for attacks, or may result in the adversary being deterred from future attacks.

To the extent possible, attacks should be prevented from executing. Prevention includes basic security hygiene and hardening to reduce the attack surface. Prevention also includes changes to system components and/or to mission processes to make the attack surface harder to understand or predict and (using a chess analogy) to counter anticipated future moves.

Preparation involves developing alternative cyber courses of action[16] (CCoAs), and obtaining and positioning the resources needed to execute those CCoAs. Preparation can also include exercises and training to ensure that the CCoAs can be executed (ASD(CIIA), 2009).

4.1.1.2 Withstand

For cyber resiliency, to withstand is to *continue essential mission/business functions despite successful execution of an attack by an adversary*. Reaching this goal involves meeting two objectives:

- "Fight through" an attack or maintain essential functionality in the presence of adversary actions
- Contain or defeat adversary actions

The assumption underpinning this resiliency goal is that operations must continue, in a degraded or alternative mode, until the attack is well enough addressed that recovery becomes possible. The primary focus is thus on maintaining minimal essential capabilities. If the adversary is successful in the early stages of the cyber kill chain, a cyber attack can disrupt mission operations, making key resources unavailable or unreliable. The mission must then "fight through" the cyber attack (Pal, et al., 2010) (Eltoweissy, 2011), while cyber defenders seek to contain or defeat adversary activity.

Fighting through a cyber attack involves maintaining essential mission functions, by selecting and executing a cyber course of action. The mission environment must be monitored to determine the CCoA's effectiveness (and changes in its effectiveness, as the adversary adapts); evidence or indications of changes in adversary TTPs; and evidence or indications of complementary adversary activity. The selected CCoA may need to be adapted, or even abandoned in favor of a different CCoA.

Containing or defeating adversary actions enables cyber defenders to focus their efforts on a limited set of cyber resources while leaving other resources free for mission use, in addition to laying the foundation for recovery.

4.1.1.3 Recover

For cyber resiliency, to recover is to *restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary*. Meeting this goal involves achieving three objectives:

- Determine damages
- Restore capabilities
- Determine reliability

[16] A cyber course of action is a set of activities by cyber defenders (e.g., CND staff; staff in a Security Operations Center or a Cyber Security Operations Center) and, as needed, other cyber staff (e.g., staff in a Cyber Operations Center, system administrators, network operators) and mission staff to confirmed, suspected, or predicted cyber attacks. (Note that this definition is broader than the one presented in (Alphatech, Inc., 2004), which restricts cyber-CoAs to system administrator actions.)

When adversary activities are sufficiently contained or defeated, the process of recovering from the attack can begin. Recovery includes determining the damages, restoring capabilities, and determining the degree of confidence that can be accorded the restored capabilities.

Determination of damages involves forensic analysis of malware used in the attack, as well as analysis of the records produced by monitoring, logging, and auditing to identify cyber resources that were affected by the attack. Depending on the adversary activities found through this analysis, damage determination can also involve coordination and information sharing with external organizations (e.g., if the attack used the affected systems as a launching point for attacks on those organizations). Damage determination can also include searching for copies of stolen or exfiltrated data.

Restoration can take the form of backward recovery, rolling back to a known acceptable state. This can entail loss of data for the period between when the acceptable state was captured and when recovery occurred. Alternately, restoration can recreate capabilities, establishing a new baseline.

Cyber resources – e.g., systems, information stores, networks, shared services – have an associated degree of reliability (e.g., correctness, currency, and completeness of information; availability of communications; confidence that a process such as a search or a computation will complete in a given time). With the exception of documented requirements and service level agreements (SLAs), the reliability of a cyber resource is generally undefined or poorly articulated; however, end users typically have a sense of which resources are more reliable. The reliance that mission/business process users and/or cyber defenders can have in the restored resources may be different from their pre-attack reliance.

4.1.1.4 Evolve

For cyber resiliency, to evolve is to *change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks*. This goal must be achieved in the context of environmental changes. Meeting this goal involves achieving two objectives:

- Transform existing processes and behavior
- Re-architect

Environmental changes include changes to the threat environment, the system environment, and the technology environment. Changes in the threat environment are reflected in updates to the threat model, and include changes in the identity, capabilities, intent, or targeting of adversaries as well as changes in adversary tradecraft and TTPs. Changes in the system environment include changes in mission definition, priorities, workflows; architectural or configuration changes in systems; and changes in the user population (e.g., training, exercises, new communities of users). Changes in the technology environment include new discoveries of vulnerabilities inherent in a technology or specific to a product or class of products; changes in how a technology is deployed or used; the introduction of a new technology; and the phase-out of an established technology.

4.1.2 Cyber Resiliency Objectives

Eight cyber resiliency objectives are defined to enable the cyber resiliency goals to be met. Figure 4 illustrates the goals supported by each objective. Because the cyber threat changes, many actions to improve resilience (to achieve an objective, to meet a goal) will be effective only for a limited time. Thus, the effectiveness of resilience practices and solutions must be

monitored. The structure of goals and objectives provides a conceptual foundation for such monitoring.

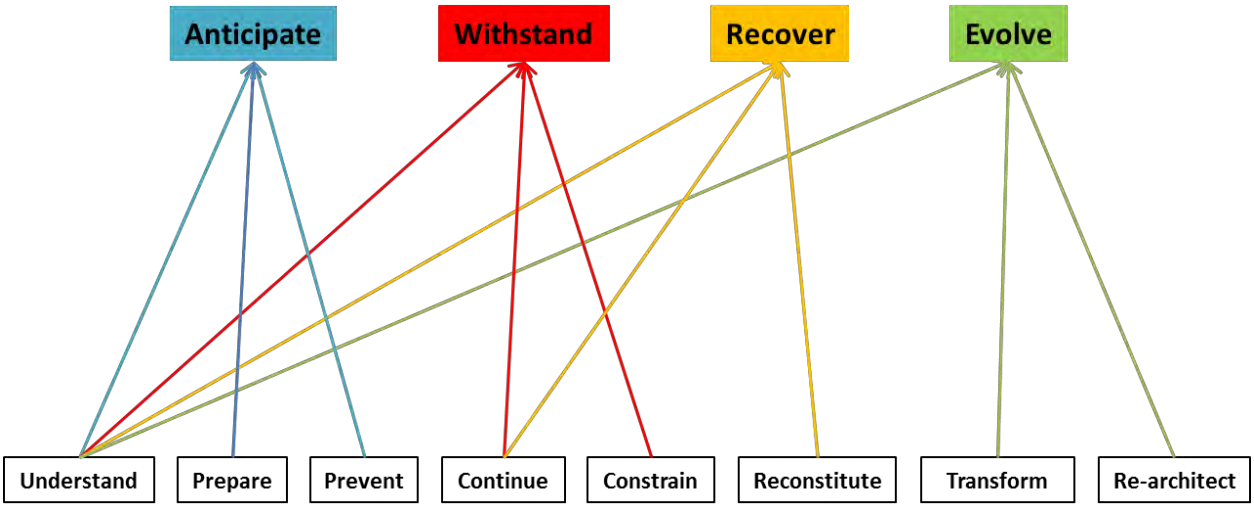

Figure 4. Cyber Resiliency Goals and Objectives

4.1.2.1 Understand

The *Understand* objective is to *maintain useful representations of adversaries, mission or business function dependencies on cyber resources, and the status of those resources with respect to adversary activities*. A useful representation of adversaries identifies adversary characteristics (e.g., capabilities, intent, targeting), includes potential and actual adversary activities, identifies conditions that an adversary might exploit to launch a successful attack, and incorporates knowledge of adversary tradecraft as feasible. A useful representation of the status of cyber resources enables detection of changes which indicate that an attack may be underway, identification of resources affected by an attack, damage assessment, and assessment of resource reliability.

Representations of adversaries and dependencies clearly support Anticipate, enabling prediction of adversary activities as well as CCoA development. Representations of cyber resource status support Withstand, since identifying resources affected by an attack facilitates selecting the most appropriate CCoA, as well as Recover, by facilitating damage assessment and reliability assessment. Finally, representations of dependencies support Evolve, helping to avoid unintended consequences of architectural changes.

4.1.2.2 Prepare

The *Prepare* objective is to *maintain a set of realistic cyber courses of action that address predicted cyber attacks*. For a CCoA to be realistic, it must take into consideration available resources, both cyber and non-cyber (e.g., personnel, which may include staffing levels, training, and exercise-based understanding of how to execute the CCoA).

4.1.2.3 Prevent

The *Prevent* objective is to *preclude successful execution of an attack on a set of cyber resources*. Key to this objective is the application of sound information systems security engineering (ISSE) principles and practices, to apply security controls at the most cost-effective

points in the enterprise or system architecture and to implement security measures in the most cost-effective way. Strategies specific to cyber resiliency include selectively hardening key resources based on adversary capabilities, deflecting adversary actions, taking actions that dissuade an adversary from attacking those resources, or limiting an adversary's incentive to attack.

4.1.2.4 Continue

The *Continue* objective is to *maximize the duration and viability of essential mission/business functions during an attack*. This can be achieved through a combination of graceful degradation of services, extending the area an adversary must attack to be successful, judicious distribution of mission/business functions, and employing alternate course of actions while under attack.

4.1.2.5 Constrain

The *Constrain* objective is to *limit damage from an adversary's attacks*. This is often achieved by isolating cyber resources involved in the attack from other cyber resources. Key to achieving this objective is the application of principles and practices from fault-tolerant and dependable computing.

4.1.2.6 Reconstitute

The *Reconstitute* objective is to *redeploy cyber resources to provide as complete a set of mission/business functionality as possible subsequent to a successful attack*. This may be achieved through a combination of ensuring failure to a known good state and providing the ability to return to a state that supports continuing mission/business operations as quickly as circumstances permit.

4.1.2.7 Transform

The *Transform* objective is to *change aspects of organizational behavior in response to prior, current, or prospective adversary attacks*. The intent is to minimize exposure of cyber resources to attacks by limiting or changing aspects of mission/business activities. Examples include, but are not limited to, changing the way a mission/business function is performed, doing something radically different relative to or changing, the scope of the mission/business function.

4.1.2.8 Re-architect

The *Re-architect* objective is to *modify architectures to apply cyber resiliency practices more effectively; to address predicted long-term changes in adversary capabilities, intent, and/or targeting; and to incorporate emerging technologies in ways that improve (or at least do not degrade) cyber resiliency*. This may include redesigning, re-implementing, or replacing existing cyber resources – particularly with new technologies, and reconfiguring existing resources to provide new or different capabilities.

4.1.3 Cyber Resiliency Practices

Cyber resiliency practices are approaches to achieving one or more cyber resiliency objectives that are applied to the architecture or design of mission/business functions and the cyber resources – mission/business segments, common infrastructures, shared services, or individual systems, services, or components – that support mission/business functions. Several practices are adapted from other disciplines related to cyber resiliency – most notably cyber security, dependability, continuity of operations planning, and resilience engineering. The set of cyber

resiliency practices described below, largely derived from (Goldman, 2010), is intended to be extensible.

Cyber resiliency practices are predicated on the assumptions that sound security engineering practices are applied (and thus that common security controls are already in place) and that mission criticality analyses are performed. In practice, these assumptions may fail to hold. If so, a cyber resiliency assessment will include mission criticality and dependency analyses. In addition, a cyber resiliency assessment will identify areas in which security engineering improvements are needed to support resiliency solutions.

4.1.3.1 Descriptions

Descriptions of the cyber resiliency practices are presented below. For ease of reference, the practices are presented in alphabetical order. The practices vary in the extent to which they are reflected in current engineering, architectural, and operational use. Some practices are currently commonly used to provide resilience in the presence of faults or disasters (e.g., privilege restriction, redundancy, segmentation) or to support security operations (e.g., analytic monitoring). Those practices can be re-oriented or leveraged to improve cyber resiliency. Other practices are partially or sometimes represented in current operations (e.g., adaptive response, coordinated defense, dynamic representation) or architectures (e.g., diversity, dynamic positioning, non-persistence, substantiated integrity). Still others are currently rare (e.g., deception, realignment, unpredictability).

The descriptions are followed by a presentation of relationships between practices and objectives; dependencies among practices; and how the practices are applied to systems engineering, architecture, and operations. Relationships to practices identified in other work are identified in Appendix B.

4.1.3.1.1 Adaptive Response

To practice Adaptive Response is to *take actions in response to indications that an attack is underway based on attack characteristics*. More specifically, Adaptive Response involves selecting, executing, and monitoring the effectiveness of the CCoA that best changes the attack surface, maintains critical capabilities, and restores functional capabilities. Indications that an attack is underway include detection of divergence from the organization's established conditions of normal operations, as well as externally provided threat intelligence. Responses to the attack include changes to the capabilities, processes, technologies, or security postures that were previously presented to the adversary. Examples include employing applications not previously presented to the adversary, repositioning of critical assets, and changing the configuration of networks, systems, or applications. Adaptive Response includes a mixture of human and automated decisions. Policy- and risk-driven automation will enable systems to evolve toward greater autonomic decision-making.

4.1.3.1.2 Analytic Monitoring

To practice Analytic Monitoring is to *gather and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities, and damage*. To gather data, sensors are deployed within, and at the boundary of, distinctly managed sets of cyber resources (e.g., a mission/business segment, a common infrastructure, a set of shared services, or a system). Coordination includes establishing coverage and timeframes or frequency for data gathering and analysis to avoid gaps or blind spots, and can include mechanisms for data fusion, correlation, and data mining. Examples of analysis include identifying anomalous behavior,

performing malware analysis (passive, active and post-mortem), and use of validation techniques to identify changes in infrastructure that indicate an ongoing attack.

Analytic Monitoring for cyber resiliency can use data gathered for security monitoring, performance monitoring and attack sensing and monitoring (AS&W)[17], but differs from these forms of monitoring in its emphasis on informing defender actions by

- Finding indications of a stealthy and well-resourced adversary (see Section 4.2);
- Detecting and assessing damage; and
- Watching for adversary activities during recovery and evolution.

Analytic Monitoring can depend on information sharing – e.g., about attack trends, vulnerabilities, and the results of forensic analysis – with other organizations (Bodeau, et al., 2010).

4.1.3.1.3 Coordinated Defense

To practice Coordinated Defense is to *manage adaptively and in a coordinated way multiple, distinct mechanisms to defend critical resources against adversary activities*[18]. Multiple mechanisms apply the same technique to different technologies or architectural layers; distinct mechanisms apply different practices. Greater asset criticality merits greater layering. Requiring the adversary to defeat multiple mechanisms makes it more difficult for the adversary to successfully attack critical resources, and increases the likelihood of adversary detection.

Managing such mechanisms adaptively entails changing how they are used (e.g., making configuration changes, turning on some mechanisms while turning off others) to adapt to adversary activities as well as to changes in mission/business needs or priorities and notification of newly discovered vulnerabilities in component technologies. Cyber defenses, supporting security controls, and supporting performance controls must be managed in a consistent manner across multiple administrative spans of control. Coordination is essential to ensure that an attack that involves one defensive mechanism does not create adverse unintended consequences (e.g., lockout, cascading alarms) by interfering with another defensive mechanism. Thus, cyber courses of action (CCoAs) and contingency plans must be defined in a coordinated way.

The effectiveness of Coordinated Defense is enhanced when combined with such practices as Adaptive Response, Privilege Restriction, Diversity, Deception and Segmentation.

4.1.3.1.4 Deception

To practice Deception is to *use obfuscation and misdirection (e.g., disinformation) to confuse an adversary*. Deception can make the adversary uncertain how to proceed, delay the effect of the adversary's attack,[19] increase the risk to the adversary of being discovered, or expose an adversary's tradecraft. Deception can take the form of dissimulation ("hiding the real") or simulation ("showing the false"). Dissimulation (or obfuscation) techniques include masking (e.g., using encryption or function hiding), repackaging (e.g., using data transformation), and

[17] AS&W is "Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed." (CNSS, 2010)

[18] Coordinated Defense assumes that security engineering has supplied multiple, distinct protective mechanisms, i.e., that a defense-in-depth strategy has been applied. Defense-in-depth is widely recognized as a necessary, but not sufficient, strategy for addressing cyber threats.

[19] Potential benefits of delaying the attack can include providing the organization additional time to complete critical mission functions, as well as providing time to deploy an adaptive response.

dazzling (e.g., using misdirection, responding to adversary queries with deliberately confusing or erroneous information). Simulation (or misdirection) techniques include inventing (e.g., simulating a non-existent application), mimicking (e.g., fabricating documents or data stores), and decoying (e.g., using honeypots). (See (Bell, et al., 1982), cited in (Tan, 2003), (MacQueen, et al., 2009).)

4.1.3.1.5 Diversity

To practice Diversity is to *use a heterogeneous set of technologies (e.g., hardware, software, firmware, protocols) to minimize the impact of attacks and force adversaries to attack multiple different types of technologies*. One mechanism for implementing diversity for software is virtualization, which allows rapid, inexpensive changes in applications, thus making some forms of diversity[20] easier to implement.

Diversity is a commonly cited technique for resilience (ReSIST, 2008) (Trimintzios, et al., 2011). Another term for diversity is heterogeneity (Richards, et al., 2008). As noted in (Goldman, 2010), Diversity is vital to effective Redundancy.

4.1.3.1.6 Dynamic Positioning

To practice Dynamic Positioning is to *use distributed processing and dynamic relocation of critical assets and sensors*. Dynamic Positioning applied to critical assets will impede an adversary's ability to locate, eliminate or corrupt mission/business assets, and will cause the adversary to spend more time and effort to find the organization's critical assets. As with Coordinated Defense, this increases the chance of adversaries revealing their actions and tradecraft. Dynamic Positioning applied to sensors supports Analytic Monitoring by allowing the monitoring of activities in specific parts of a system or involving specific assets to be adjusted in consideration of threat, vulnerability, or anomaly information. Examples of technologies to support this practice include virtualization and distributed processing.

4.1.3.1.7 Dynamic Representation

To practice Dynamic Representation is to *construct and maintain dynamic representations of components, systems, services, mission dependencies, adversary activities, and effects of alternative cyber courses of action*. A representation is *dynamic* if it can reflect changes in state or behavior. A static representation (e.g., a network diagram that does not allow for differences in mission criticality of network components depending on which mission functions are currently being supported) can serve as a starting point for, or can be incorporated into, a dynamic representation. Dynamic representations can be fed by analytic monitoring; conversely, requirements for information produced by analytic monitoring can be driven by the need to maintain a current representation. Dynamic representations support situation awareness, and thus inform adaptive response and coordinated defense.

Dynamic representations can be used to enhance understanding, particularly of dependencies among cyber and non-cyber resources; validate the realism of courses of action; raise awareness of cyber threats, and support training and preparation; and identify gaps in planning, for which additional cyber courses of action need to be developed. Dynamic representations can include

[20] Diversity requires that technologies that provide the same (or equivalent) functionality differ enough that they do not present the same attack surface to an adversary. Examples of methods to determine whether two instances are different include data pedigree, functional dependency analysis, hardware or software component pedigree as established by supply chain risk management (SCRM), and use of alternative specifications for automatically generated software.

simulation exercises as well as executable models[21]. Models of adversary behavior can be game-theoretic.

Dynamic Representation practices rely on

- Information about systems and components that is also used by system, network, and security managers (e.g., configuration, security patch status, availability and performance statistics). Some information is provided by system or network management tools; other information may be provided by continuous monitoring or other security management tools.
- Information about functional dependencies among systems, networks, and components. This information is typically included in continuity or contingency planning documentation.
- Information about mission dependencies on systems or services, networks or communications links, and information stores. This information may be provided by a Mission Impact Analysis or Business Impact Analysis (e.g., using the Map the Mission process (Foote, et al., 2011), Mission Based Analysis (Peters, 2009), or Mission-Driven Assessment (Belz, 2011)).

4.1.3.1.8 Non-Persistence

To practice Non-Persistence is to *retain information, services, and connectivity for a limited time, thereby reducing an adversary's opportunity to exploit vulnerabilities and establish a persistent foothold*. Non-Persistence involves quickly refreshing information, services, and connectivity to known trusted states, and eliminating services, information, and connectivity that are no longer needed. Virtualization makes such refreshment much easier. Non-Persistence is most appropriate when refresh is quick enough not to interfere with mission/business functions.

4.1.3.1.9 Privilege Restriction

To practice Privilege Restriction is to *restrict privileges required to use cyber resources, and privileges assigned to users and cyber entities, based on the type(s) and degree(s) of criticality[22] and trust[23] respectively, to minimize the potential consequences of adversary activities*. Examples of privilege restriction mechanisms include fine-grained access control and trust-based privilege assignment. Generally, the more critical the asset the more fine-grained the privileges that may be applied to it, and the more trusted an entity is, the greater privilege that it is granted.

Identifying critical and trusted assets is alluded to in (Goldman, 2010), and least privilege is identified as a technique but not defined. Least privilege is a well-established information security principle, identified with the objective of reducing vulnerabilities rather than increasing resilience in NIST SP 800-27 (Stoneburner, et al., 2004). However, the use of asset criticality as a driver for the granularity of privileges is not part of that principle.

---

[21] Simulation exercises can be model-based and automated, partially automated (e.g., training simulators, exercises, technology demonstrations), or purely manual (e.g., tabletop exercises). Simulation exercises are an established part of business continuity and disaster recovery (IBM, 2006). Such activities can also lead to changes in organizational behavior, due to increased awareness (ASD(CIIA), 2009).

[22] Criticality is determined based on analysis of the potential consequences of compromise; higher criticality requires more restrictive (typically more fine-grained as well as more closely controlled) privileges.

[23] Trust in a user is determined based on organizational policies and practices; trust in a cyber-resource depends not only on which user (if any) it represents, but also on such factors as its provenance and its recent history.

4.1.3.1.10 Realignment

To practice Realignment is to *align cyber resources with core aspects of mission/business functions, thus reducing the attack surface.* Realignment entails defining, and determining the operational implications and cyber resource needs of, alternative as well as primary mission and cyber defender courses of action. Realignment minimizes the chance that resources dedicated to activities that do not support mission/business functions could be used as an attack vector. One example of realignment is off-loading some less important cyber-supported functions to a service provider that is better able to support the functions.[24] Other examples are to perform a function using out-of-band communications (e.g., replace automated cross domain services with air gaps and sneaker nets), or to eliminate certain data feeds or connections where the benefits of those feeds are determined to be less than the potential risks such connectivity imposes on the core mission/business functions.

4.1.3.1.11 Redundancy

To practice Redundancy is to *maintain multiple protected instances of critical resources (information and services)*. These serve as backups in the case of localized damage to a resource and provide surge support when needed to support unexpected peak loads, faults and failovers. *Maintaining* an instance means keeping it compliant with the requirements that apply to it (e.g., patching software for security, updating databases for data quality), whether or not it is actively used. Maintaining a *protected* instance of a critical resource means viewing each instance as an adversary target and recognizing and mitigating ways in which a successful attack on one instance could propagate to all instances.

Redundancy is a commonly cited technique for resilience in general (Trimintzios, et al., 2011); however, some attention has been paid to the cyber threat (Richards, et al., 2008). The effectiveness of Redundancy is enhanced by combining it with Diversity (e.g., instances can provide the same functionality or information, while being implemented in different ways). Redundancy relies on Coordinated Defense (e.g., instances can be accorded different protections; one instance of software can be the current version, while another is the prior version) and Segmentation (e.g., instances can be protected by placing them on different segments).

4.1.3.1.12 Segmentation

To practice Segmentation is to *separate (logically or physically) components based on pedigree and/or criticality, to limit the spread of or damage from successful exploits*. Segmentation reduces the attack surface and enables more cost-effective placement of defenses based on resource criticality. Segmentation often employs either physically distinct entities or virtualization of computing enclaves to provide the desired separation. However, physical separation is challenging to achieve in the current technology environment, as devices are increasingly enabled for wireless communication. Examples of network segmentation include defining enclaves or sub-networks within an intranet, isolating an intranet from an extranet, and both from the Internet, separating inbound from outbound traffic, and separating requests from responses. Segmentation can also be applied at the system layer, by using virtualization, at the application layer, by partitioning services, and at the data layer, by providing separate data repositories.

[24] The trust required of the provider depends upon the importance of the functions and the sensitivity of the data it must handle.

4.1.3.1.13 Substantiated Integrity

To practice Substantiated Integrity is to *ascertain that critical services, information stores, information streams, and components have not been corrupted by an adversary*. Example mechanisms include use of integrity checks (e.g., cryptographic seals or checksums on critical records or software), data validation (checking that data conforms to its specified requirements, such as type or range), mission/business rule validation (checking that data makes sense), polling of inputs from diverse critical services (e.g., Byzantine quorum systems) to determine correct results in case of conflicts between the services, and tamper-evident technologies.

4.1.3.1.14 Unpredictability

To practice Unpredictability is to *make changes frequently and randomly, not just in response to actions by the adversary*. These changes, which may draw upon Diversity, Non-Persistence, and Dynamic Positioning practices, make it more difficult for an adversary to predict behavior and (as with Coordinated Defense) this increases the chance of adversary actions being detected or tradecraft revealed. Examples of unpredictable behavior include, but are not limited to, changing browsers and authentication mechanisms, encryption rekeying, and changing permitted ports.

4.1.3.2 Supporting Practices

Cyber resiliency practices depend on supporting security and performance practices. As cyber resiliency practices and solutions mature, they can be expected to become part of the security and performance practices of

- Security engineering, which applies generally accepted security principles and practices throughout the life-cycle to achieve the information security goals of confidentiality, integrity, and availability.
- Performance engineering, which applies generally accepted principles and practices to ensure that systems, services, and networks can meet service level agreements (SLAs) or achieve measures of performance (MOPs) or technical performance measures (TPMs).[25]
- Security management, which manages the mechanisms provided through security engineering to enforce organizational policies.
- Security operations, which uses the mechanisms provided through security engineering to identify and manage security risks in operational environments.

4.1.3.3 Mappings and Dependencies

Table 3 provides a mapping between the cyber resiliency objectives and the practices described in Sections 4.1.3.1 and 4.1.3.2. Note that the contribution of supporting practices to achieving cyber resiliency objectives is necessary but not sufficient. Cyber resiliency practices are needed to address significant cyber threats, as described in Sections 2.2.1 and 4.2.

[25] See (INCOSE, 1998) for definitions.

Table 3. Mapping Cyber Resiliency Practices to Objectives

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

The cyber resiliency practices are interdependent. As illustrated in Table 4, each practice enables mission operators, cyber defenders, or systems engineers and architects to perform key resilience-related activities. Key activities for most cyber resiliency practices depend on effective execution of activities enabled by other practices.

Table 4. Dependencies Among Cyber Resiliency Practices

Practice in Cyber Resiliency Engineering Framework	Key Activities	Relied-on Practices and Activities
Adaptive Response: Take actions in response to indications that an attack is underway based on attack characteristics.	Select and tailor CCoA Dynamically reconfigure existing resources Dynamically provision by reallocating existing resources Dynamically reconstitute critical assets or capabilities Track effectiveness of CCoA and adapt as necessary Identify and restore non-critical functional capabilities	Analytic Monitoring: Inform responses, so that best CCoA can be selected; Monitor effectiveness of CCoAs; Provide damage assessment Coordinated Defense: Define CCoAs that can be executed in a coordinated way; Coordinate response activities to ensure synergy rather than interference Diversity: Provide truly different alternative resources that can be used in executing CCoAs Dynamic Positioning: Reposition critical assets Dynamic Representation: Provide current representation of posture Redundancy: Provide redundant resources that can be reallocated
Analytic Monitoring: Gather and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities, and damage	Coordinate sensor coverage to avoid gaps or blind spots Correlate or otherwise combine data from different sensors Analyze data to identify anomalies, develop I&W, and monitor effectiveness of CCoAs Dynamically reposition or reconfigure sensors Perform malware and forensic analysis Perform damage assessment Perform retrospective analysis to investigate historical trends and activities	Deception: Monitor and analyze adversary behavior in deception environments Diversity: Provide alternative paths for reporting monitoring data, alternative analysis techniques and tools Dynamic Positioning: Deploy or reconfigure sensors to monitor specific resources, types of behavior, and/or effects of CCoAs Segmentation: Define boundaries so that sensors can be placed at boundaries and so that internal sensors can be configured to detect anomalies Substantiated Integrity: Report integrity status of resources to support damage assessment

Practice in Cyber Resiliency Engineering Framework	Key Activities	Relied-on Practices and Activities
Coordinated Defense: Manage adaptively and in a coordinated way multiple, distinct mechanisms to protect critical resources from adversary activities	Identify key locations to place mechanisms Provide protection mechanisms at different locations Identify dependencies and interactions among cyber defenses, security controls, and performance controls Coordinate ongoing management Coordinate definition and assignment of privileges Define / maintain CCoAs that can be executed in a coordinated way given existing controls and management responsibilities Coordinate response activities to ensure synergy rather than interference Coordinate recovery activities to avoid gaps in security coverage	Analytic Monitoring: Identify anomalies, provide I&W, and monitor CCoA effectiveness across multiple administrative spans of control Dynamic Representation: Provide status / resiliency posture information about cyber resources to those responsible for resources / capabilities that depend on those cyber resources Privilege Restriction: Enable privileges to be defined and managed consistently across multiple administrative spans of control Redundancy: Replicate mechanisms at different locations Segmentation: Enable administrative spans of control to be well-defined and limited
Deception: Use obfuscation and misdirection (e.g., disinformation) to confuse an adversary	Conceal mission processing and communications, e.g., function hiding Transform data for obfuscation Create and maintain deception environment(s), e.g., honeypots, honeynets, decoy documents or data stores Redirect adversary activities to deception environment(s) Observe and analyze adversary activities in deception environments	Analytic Monitoring: Inform decisions to redirect activities to deception environment(s); Observe and analyze behavior in deception environment(s) or in response to deceptive techniques Coordinated Defense: Develop representative information for use in deception environment; Manage deception techniques and/or environment(s) without interfering with mission operations Redundancy: Provide duplicate resources for use in deception environment(s) Segmentation: Isolate deception from operational/mission environments
Diversity: Use a heterogeneous set of technologies (e.g., hardware, software, firmware, protocols) to minimize the impact of attacks and force adversaries to attack multiple different types of technologies	Maintain or dynamically create determinably different instantiations / implementations of capabilities or component functionality (e.g., different operating systems, applications, hardware) Define and maintain determinably different alternative processing paths (i.e., different sequences of services or applications used to respond to the same request) Define and maintain determinably different alternative communications paths (e.g., different protocols, different communications media) Establish means to deploy diverse resources rapidly (e.g., in near real time) Identify and maintain determinably different mission data sources	Coordinated Defense: Manage diverse instantiations of equivalent capabilities consistently Analytic Monitoring: Analyze adversary effectiveness against various different types of technology Adaptive Response: Change frequency of diversity and selection of components in response to attacks.

Practice in Cyber Resiliency Engineering Framework	Key Activities	Relied-on Practices and Activities
Dynamic Positioning: Use distributed processing and dynamic relocation of critical assets and sensors	Use distributed processing and virtualization to relocate targeted resources Dynamically relocate critical assets Dynamically relocate sensors	Analytic Monitoring: Identify key locations and timing for repositioning of assets Privilege Restriction: Ensure that privilege restrictions are strongly bound to critical assets so that relocation does not unexpectedly change privileges Segmentation: Ensure that critical assets are not relocated to less-trusted enclaves
Dynamic Representation: Construct dynamic representations of components, systems, services, adversary activities, and effects of alternative cyber courses of action	Define and maintain a representation of the resiliency posture (including security posture, performance with respect to SLAs or KPPs, and quality as determined using Substantiated Integrity mechanisms) of cyber resources and adversary activities against cyber resources Identify, and maintain a representation of, functional and mission dependencies among cyber resources Simulate and/or exercise CCoAs	Analytic Monitoring: Populate models / representations of resiliency posture and adversary behaviors with results of analysis (note that, depending on the interface provided by a monitoring tool, the tool may actually maintain and present the dynamic representation) Deception: Observe and analyze adversary activities Segmentation: Enable discrete or separable sets of cyber resources to be represented Substantiated Integrity: Enable the quality (e.g., pedigree, non-corruption, currency) of cyber resources to be represented
Non-Persistence: Retain information, services, and connectivity for a limited time, thereby reducing an adversary's opportunity to exploit vulnerabilities and establish a persistent foothold	Identify services and information to which non-persistence can be applied Define lifespan conditions for services and connectivity Terminate services or connectivity when lifespan conditions no longer hold Define retention conditions for information Delete or move information when retention conditions no longer hold Ensure that termination, deletion, or movement does not leave residual data or software behind	Analytic Monitoring: Monitor lifespan / retention conditions and provide notification when conditions no longer hold Coordinated Defense: Coordinate definitions of lifespan / retention conditions to ensure that non-persistence does not interfere with mission or management functions

Practice in Cyber Resiliency Engineering Framework	Key Activities	Relied-on Practices and Activities
Privilege Restriction: Restrict privileges required to use cyber resources, and privileges assigned to users and cyber entities, based on the type(s) and degree(s) of criticality and trust respectively, to minimize the potential consequences of adversary activities	Determine degrees of criticality of cyber resources, thereby identifying critical assets Determine types and degrees of trust for users and cyber entities (e.g., components, data, processes, interfaces) Assign privileges based on types and degrees of trust Assign and maintain privilege restrictions, particularly for critical assets Increase or decrease privilege restrictions based on adversary activities	Coordinated Defense: Coordinate the use of privileges, especially at different locations and layers Segmentation: Restrict the scope of a privilege to a defined set of cyber resources
Realignment: Align cyber resources with core aspects of mission/business functions, thus reducing the attack surface	Identify mission / business function dependencies on cyber resources Identify non-mission / business function dependencies on or uses of cyber resources Assess mission / business function risks due to dependency on resources shared with non-mission functions Reallocate resources and/or reassign administrative / management responsibility based on risk to mission / business function Identify and remove or replace data feeds and connections for which risks outweigh benefits	Dynamic Representation: Use modeling and analysis to identify potential attack vectors via non-critical services Segmentation: Separate cyber resources needed to perform or support mission / business functions from those that perform or support other functions
Redundancy: Maintain multiple protected instances of critical resources (information and services)	Maintain multiple protected instances of hardware Create and maintain multiple protected instances of software Create and maintain multiple protected instances of information	Coordinated Defense: Provide consistent degrees of protection; Ensure that the quality of protected instances of software and data is managed consistently or in a coordinated way Segmentation: Place different protected instances in different enclaves
Segmentation: Separate (logically or physically) components of dubious pedigree from more trusted ones, to limit the spread of or damage from successful exploits	Define an enclave or set of cyber resources with a clear boundary Maintain boundary protections Isolate the enclave or set of cyber resources to contain adversary activities	Privilege Restriction; Employ different privileges in different segments. Redundancy: replicate key functions across segments to ensure segments are self-sufficient
Substantiated Integrity: Ascertain that critical services, information stores, information streams, and components have not been corrupted by an adversary	Validate data provenance Validate data integrity / quality to ensure it has not been corrupted Validate software / service integrity / behavior to ensure it has not been corrupted	Diversity: Use data from different sources to validate data quality; Use outputs from different implementations of the same functionality to validate software / service behavior Redundancy: Assess output from redundant services to identify inconsistencies and hence potential corruption

Practice in Cyber Resiliency Engineering Framework	Key Activities	Relied-on Practices and Activities
Unpredictability: Make changes frequently and randomly, not just in response to actions by the adversary	Define an implementable set of change parameters (e.g., conditions under which unpredictable changes should not be made, "distance" beyond which a service should not be moved, ranges for frequency of changes) Reconfigure components and services, use alternative equivalent components or services, or dynamically reposition processing randomly, in accordance with change parameters	Coordinated Defense: Constrain changes as needed to avoid interference with mission or cyber defense activities Diversity: Provide truly different alternative resources that can be used unpredictably Dynamic Positioning: Enable unpredictable changes to include relocation Non-Persistence: Ensure that unpredictable changes do not leave behind exposed information or software Redundancy: Provide duplicate resources that can be used unpredictably

The cyber resiliency practices can be applied in multiple ways. Table 5 describes how the cyber resiliency practices apply to systems engineering, architecture, and operations:

- Systems engineering involves designing and implementing systems for use in specific environments. Systems engineering can be supported by an Enterprise Architecture or the architecture for a mission/business segment. For each practice, representative answers are given to the question: What should the systems engineer seek to achieve when planning and evaluating a design or an implementation approach?
- The term "architecture" is applied at different levels of specificity, which can include an Enterprise Architecture (EA), the architecture of a mission/business segment, a system architecture, or the architecture of a product or component. In general, an architecture identifies architectural elements (e.g., systems, services, and common infrastructures for an enterprise architecture or a mission/business segment architecture; components and interfaces for a system architecture), information flows (e.g., transactional flows of mission/business information, control flows of instructions), and functional dependencies. An EA or a mission/business segment architecture typically also identifies or defines standards, criteria, and trade-off guidance to apply to all systems, services, or components within the scope of the architecture. For each practice, representative answers are given to the question: What should the architect specify, and what guidance should the architect give, for the components within the scope of the architecture?
- Operations includes mission operations and cyber defender operations. For each practice, representative answers are given to the question: What should be included in mission and/or cyber courses of action (CoAs)? For some practices, an additional question applies: What should be considered in exercises or training?

Table 5. Applying Cyber Resiliency Practices in Different Domains

Practice	Systems Engineering	Architecture	Operations
Adaptive Response	Enable dynamic reconfiguration and resource re-allocation, using Dynamic Representation and Substantiated Integrity mechanisms that accurately describe the system state Enable dynamic reconstitution, using discovery and Substantiated Integrity mechanisms	Define interfaces with Analytic Monitoring to enable situational awareness of cyber resources and (as feasible) of the surrounding environment and of alternative processing / communications capabilities Define external interfaces to enable situational awareness of the surrounding environment and of alternative processing / communications capabilities	Define CCoAs that use externally provided I&W (e.g., DIB tips) Define CCoAs that include I&W thresholds and triggers, as well as damage assessments, using data provided by Analytic Monitoring Define CCoAs that take into consideration mission priorities and constraints on timing of changes
Analytic Monitoring	Design to enable Dynamic Positioning and dynamic reconfiguration of sensors Implement data transformations on log/audit data for interoperability Incorporate results of Substantiated Integrity mechanisms into representations of system / component status	Define data interoperability standards to enable correlation and data fusion Define reporting criteria and data flows to consolidate monitoring and preliminary / local I&W and damage assessments across a defined set of cyber resources Leverage Segmentation to isolate asynchronous communications, analyze and correlate request-response traffic, and isolate different protocols for monitoring and analysis Define interfaces with Dynamic Positioning to position and configure sensors as needed	Define CCoAs that include, or make use of the results of, forensic analysis Define CCoAs that include damage assessment using local and consolidated data Define CCoAs using interfaces with Dynamic Positioning to position sensors as needed
Coordinated Defense	Incorporate notification / coordination mechanisms to deconflict actions (e.g., reconfiguration, refresh, resource re-allocation, isolation, failover, reconstitution) by cyber defenders and managers / administrators	Define mappings between the architecture and governance structures, so that those (functional roles and/or architectural components) whose decisions will affect sets of cyber resources are clearly identified	Define CCoAs that include coordination between cyber defenders and managers or administrators at different tiers or with different spans of control
Deception	Implement deception techniques (e.g., misdirection, data transformation / modification, mimicry)	Define criteria or trade-offs for using specific deception technologies Define interfaces with Analytic Monitoring to understand adversary behavior Incorporate deception environments (e.g., honeypots, honeynets) into the architecture	Define CCoAs that divert traffic to a deception environment

Practice	Systems Engineering	Architecture	Operations
Diversity	Use multiple specifications and implementations to provide the same capability / functionality Define common or consistent interface for mission users, cyber defenders, and managers / administrators	Define technical standards that accommodate diverse implementations (e.g., by specifying functionality and interfaces)	Define CCoAs and mission CoAs that use alternate or out-of-band communications / processing paths
Dynamic Positioning	Design to accommodate dynamic relocation of sensors, defenses, and critical resources (software and data)	Define criteria (trade-off analyses and technical standards) for dynamic relocation of sensors, defenses, and critical resources (software and data)	Define CCoAs that use dynamic relocation of sensors and defenses Define mission CoAs that take into consideration dynamic relocation of critical resources
Dynamic Representation	Integrate mapping and reporting capabilities to enable a current and accurate representation of the system	Define interfaces with Analytic Monitoring to understand normal or expected user or system behavior Define interfaces with Analytic Monitoring to facilitate investigation and damage assessment of adversary activities Define interfaces with Adaptive Response to provide current representation of security and resiliency posture of cyber resources	Perform realistic exercises to ensure that CCoAs are operationally feasible
Non-Persistence	Design for Non-Persistence (e.g., define temporal or behavioral triggers for decommissioning or refreshing an image)	Define retention requirements defined based on criticality and trade-off analyses	Define CCoAs that include pushing or refreshing known “good images” and/or images with more restrictive settings
Privilege Restriction	Apply the security principle of Least Privilege Use resource criticality to define criteria for user / interface / resource trust in granting access to / use of a cyber resource	Define criteria for determination / assessment of resource criticality and user / interface / resource trust	Define mission, cyber defense, and management CONOPS to take into consideration criticality and trust
Realignment	Design for agility and interoperability, enabling cyber resources to be repurposed	Define criteria and trade-offs for realigning resources and functionality	Update CCoAs based on lessons learned from incidents, changes to mission priorities and constraints

Practice	Systems Engineering	Architecture	Operations
Redundancy	Design for spare capacity and secure failover	Perform trade-off analyses for redundancy, diversity, and costs Provide alternate communications paths for reporting the results of Analytic Monitoring (including indications, warnings, and damage assessments)	Define alternate or out-of-band communications / processing paths identified and incorporated into CCoAs and mission CoAs
Segmentation	Design for modularity, so that functional segments can be easily defined Design to separate critical from non-critical data and processing Incorporate thin clients, secure browsers, and diskless nodes to minimize data retention	Define standards for modularity Provide guidance for defining segments to enable isolation Define standards for trusted, isolated enclaves (criteria or trade-off analyses for when physical separation is needed vs. when virtual enclaves suffice)	Define CCoAs that isolate mission-essential from non-essential cyber resources
Substantiated Integrity	Conventional integrity techniques (e.g., encrypted checksums, digital signatures, or MD5 or SHA-2 hashes) applied to data and software	Defined priorities and trade-offs for application of conventional and resiliency-specific integrity technologies	Define CCoAs and mission CoAs that use out-of-band validation of provenance or pedigree
Unpredictability	Design for modularity and agility, so that cyber resources can be relocated, refreshed, and/or replaced	Define standards (criteria and/or trade-offs) for technologies to be replicated, distributed, diversified and/or modularized to facilitate unpredictable location or usage patterns Define standards (criteria and trade-offs) for mission user and cyber defender interfaces that conceal unpredictable behavior that is not relevant to doing their jobs	Perform realistic exercises that include unpredictable behavior, to evaluate impacts on mission user and cyber defender effectiveness

4.2 Threat Model

Cyber resiliency engineering assumes an adversary at or above Cyber Prep Level 4[26],[27]. Table 6 presents adversary characteristics for Cyber Prep Levels 3 through 5 (Bodeau, et al., 2009). At these levels, adversaries can be expected to apply cyber resiliency practices to their own command and control (C2) structures (McAfee, 2011).

Table 6. Adversary Characteristics at Cyber Prep Levels 3 Through 5

Threat Level	Capability	Intent	Targeting
5: Advanced	The adversary is **very** sophisticated and **well resourced** and **can generate its own** opportunities to support multiple successful, continuous, **and coordinated** attacks.	The adversary seeks with **great** determination to undermine or impede **severely, or destroy,** a mission, program, or enterprise, by **exploiting** a presence in the organization's systems or infrastructure. **The adversary is concerned about disclosure of tradecraft only to the extent that it would impede their ability to complete their goal.**	The adversary targets a specific organization, enterprise, program, or mission, focusing on specific high value or mission-critical information, resources, supply flows, or functions and specific employees supporting those functions, **as well as on supporting infrastructure providers and suppliers and on partnering organizations.**
4: Significant	The adversary has a **sophisticated** level of expertise, **with significant** resources and opportunities to support multiple successful **coordinated** attacks.	The adversary seeks **with determination to undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the future**, by **maintaining a presence** in the organization's systems or infrastructure. The adversary is **very** concerned about minimizing detection of their attacks or disclosure of tradecraft**, particularly while preparing for future attacks.**	The adversary targets **a specific organization, enterprise, program, or mission, focusing on** specific high value **or mission-critical information, resources, supply flows, or functions and specific employees supporting those functions.**
3: Moderate	The adversary has **moderate** resources, expertise, and opportunities to support **multiple** successful attacks.	The adversary **persistently** seeks to obtain **or modify specific, critical** information and/or to usurp or disrupt the organization's cyber resources **by establishing a foothold in the organization's systems or infrastructure**, **but is concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly when carrying out attacks (e.g., exfiltration) over long time periods**. **The adversary is willing to knowingly impede aspects of the organization's mission to achieve these ends.**	The adversary targets **specific** high value organizations, **programs, or information.**

[26] However, lower threat levels can be accommodated.

[27] The definition of cyber resiliency in Section 2.3 mentions "adverse conditions, stresses, or attacks." These include the classes of threats included in the draft ENISA ontology (Vlacheas, et al., 2011): disasters, interaction conflicts, changes, supply chain attacks, dependability threats, and security threats. However, because adversaries will take advantage of or seek to make their actions indistinguishable from non-adversarial stresses and adverse conditions, cyber resiliency engineering focuses on adversarial threats.

Table 7 identifies adversary activities, including activities from the cyber kill chain (Cloppert, 2009) (Croom, 2010) in **bold**, and indicates how the cyber resiliency goals correspond to those activities.

Table 7. Cyber Resiliency Goals Address Adversary Activities

Adversary Activities	Cyber Resiliency Goal
The adversary is preparing the cyber battlefield, seeking to establish a foothold or consolidate a presence in the information infrastructure. The adversary performs **reconnaissance, weaponization,** and **delivery,** and attempts **exploitation/installation.**	**Anticipate**: Maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks
The adversary has established a foothold or consolidated a presence in the information infrastructure, and is using this to subvert the mission (disrupt, deceive, usurp) or compromise future missions (acquire information). The adversary performs **command and control** and **actions to achieve objectives**.	**Withstand**: Continue essential mission/business functions despite successful execution of an attack by an adversary
The adversary has demonstrated a presence in or had significant impacts on the information infrastructure, but adversary activities have receded or been curtailed to a tolerable level. The adversary performs maintenance, seeking to ensure future access.	**Recover**: Restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary
The adversary is preparing the cyber battlefield anew, and new adversaries are arising, seeking to establish a foothold or consolidate a presence in the information infrastructure. The adversary seeks intelligence about planned investments in and changes to the information infrastructure (**reconnaissance**), and may attack the supply chain (**weaponization** and **delivery**).	**Evolve**: Change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks

4.3 Domains for Applying Cyber Resiliency

Cyber resiliency objectives can be interpreted and resilience practices (including general resilience as well as cyber resiliency practices) can be applied at multiple layers in a notional layered architecture[28]:

- Organization or enterprise (including governance structures and processes)
- Mission or line of business (local to an organization, or cross-organizational)
- Mission/business process or task (local to an organization, or cross-organizational; when local to an organization, often identified with a business unit or sub-organization)
- Mission task or capability support
    - Cyber resources (e.g., mission/business segments, systems-of-systems, networks, shared services or infrastructure, systems, databases/knowledge bases)
        - Information assets
            - Software (e.g., protocol, hypervisor, OS, DBMS, middleware, application, presentation)
            - Mission Information (as provided via an information feed or as represented in a data store)
        - Nodes

[28] These layers correspond to those defined for space capabilities: enterprise, mission, function, domain, constellation (e.g., system-of-systems), and individual system. (OSD(SP), 2011)

        - Hardware (e.g., platform, mobile device, storage device, sensor, actuator)
        - Communications media (e.g., wire, fiber, spectrum)
    - Personnel (individuals who could be tasked with executing a mission function)
    - Organizational processes and structures
    - Facilities

Cyber resiliency *engineering* focuses on applying cyber resiliency practices to, or integrating specific resilience products or instances of those practices with, cyber resources. Thus, cyber resiliency engineering focuses on the architecture of a mission/business segment[29], a system-of-systems, a system, a set of shared services (which typically include a set of data stores or knowledge bases), or a network or other common infrastructure. However, the cyber resiliency practices identified in Section 4.1.3 do not apply equally well to all these types of cyber resources. For example, Privilege Restriction is most relevant when a set of privileges and attributes can be clearly defined and administered; this is problematic when multiple organizations or sub-organizations are involved (i.e., across a mission/business segment, a system-of-systems, or a set of shared services).

4.4 Aspects of Cost

The potential cost of applying a cyber resiliency practice or using a cyber resiliency product is multi-faceted. Three types of cost can be used to define and characterize cost metrics, representing organizational and operational concerns in the areas of:

- Initial Costs (I): Dollar or level-of-effort costs necessary to establish the resiliency techniques/technology that support the resiliency objective(s). This would include the development, acquisition, installation, and integration costs. Initial costs can be estimated in a variety of ways.
- Support Costs (S): Dollar or level-of-effort (LOE) costs necessary to maintain and facilitate the effective use of the approach; i.e., costs of support elements that are required to enable the approach be implemented, operated, and maintained in an effective manner. Support elements include, but are not limited to, CONOPS development, policy development, testing, risk assessment, and training.
- Consequential Costs and Benefits (C): The consequences of using the approach can be positive (benefits) or negative (costs), and can apply to all stakeholders or only to selected stakeholders. Consequential costs or benefits to mission owners or business function heads can involve mission effectiveness, performance, footprint, usability, changes to the CONOPS, and changes (up or down) in the amount of resources applied[30] to other mission support components. Consequential costs or benefits to IT/ICT providers

[29] An information system is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." (NIST, 2011) A system-of-systems consists of "multiple independent information systems (possibly distributed across a widespread geographic area) supporting a set of common missions and/or business functions." (NIST, 2010) A mission/business segment is the set of cyber resources – including information systems, common infrastructures (e.g., networks), shared services (e.g., Web services), and data stores – used to execute a mission or business process.

[30] Resources may be diverted from other components to support the resiliency approach, or the resiliency approach may free up resources that can then be applied to other components.

and program managers involve changes to programmatic risk[31] (e.g., schedule, technical, or certification risk) or to organizational risk (e.g., FISMA compliance risk, risks associated with organizational change); increases in risk are costs, while decreases in risk are benefits. Consequential costs also include opportunity costs, for example technical limitations on future architectural or acquisition decisions resulting from committing to a given technology.

Dollar and level-of-effort costs can be assessed quantitatively. Other types of cost can be assessed qualitatively or semi-quantitatively, and even those types of costs that can be estimated quantitatively may be better assessed qualitatively or semi-quantitatively.

[31] See (SEPO, 2011) for more on programmatic risk management.

5 Future Directions

This paper has presented an initial framework for cyber resiliency engineering. This framework provides a way to structure discussions and analyses of cyber resiliency goals, objectives, practices, and costs. It also serves to motivate and characterize cyber resiliency metrics.

Cyber resiliency engineering is part of enterprise systems engineering, and in particular part of mission assurance engineering. These engineering disciplines continue to evolve. In addition, cyber resiliency is an active research area. Thus, the framework presented here is expected to change. Feedback and discussion are welcome.

Appendix A: Bibliography

accenture. 2008. Mission Resilience: The New Imperative for High Performance in Public Service. [Online] November 24, 2008. [Cited: October 26, 2011.] http://www.homelandcouncil.org/pdfs/digital_library_pdfs/resiliencepov_ps_final_1124_accenture.pdf.

ADAAS. 2011. ADAAS: Assuring Dependability in Architecture-based Adaptive Systems. [Online] September 4, 2011. [Cited: October 26, 2011.] http://adaas.dei.uc.pt/adaas.

—. 2011. Vacancies: Extending the Concept of Dependability Cases to Address Resilience. [Online] 2011. [Cited: June 1, 2011.] http://adaas.dei.uc.pt/adaas/vacancies.

ADAPTIVE. 2011. The Third International Conference on Adaptive and Self-Adaptive Systems and Applications. [Online] 2011. [Cited: June 1, 2011.] http://www.iaria.org/conferences2011/ADAPTIVE11.html.

Allen, Julia and Davis, Noopur. 2010. Measuring Operational Resilience Using the CERT® Resilience Management Model. [Online] September 2010. [Cited: October 26, 2011.] http://www.cert.org/archive/pdf/10tn030.pdf.

Almeida, Raquel, Madeira, Henrique and Vieira, Marco. 2010. Benchmarking the Resilience of Self-Adaptive Systems: A New Research Challenge. *Proceedings of the 29th IEEE International Symposium on Reliable Distributed Systems.* 2010.

Alphatech, Inc. 2004. Real-Time Evaluation of Cyber Course of Action (CoA) Impact on Performance & Efectiveness, AFRL-IF-RS-TR-2004-75. [Online] March 2004. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA422197.

AMBER. 2009. Final Research Roadmap. [Online] 31 December, 2009. [Cited: May 26, 2011.] http://www.amber-project.eu/documents/md_207_amber_d3-2.1_preliminaryresearchroadmap_v1.0.pdf.

—. 2008. Preliminary Research Roadmap. [Online] September 30, 2008. [Cited: May 26, 2011.] http://www.amber-project.eu/documents/md_207_amber_d3-2.1_preliminaryresearchroadmap_v1.0.pdf.

ASD(CIIA). 2009. Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy. [Online] August 2009. [Cited: October 26, 2011.] http://cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf.

Avizienis, Algirdas, Laprie, Jean-Claude and Landwehr, Carl. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing.* January-March 2004, Vol. 1, 1.

Bargar, Anthony. 2009. *Cyber Resilience for Mission Assurance.* Unrestricted Warfare Symposium Proceedings 2009. 2009. p. http://www.jhuapl.edu/urw_symposium/Proceedings/2009/Authors/Bargar.pdf.

Beidleman, Scott W. 2009. Defining and Deterring Cyber War. [Online] June 1, 2009. [Cited: November 8, 2011.] http://www.hsdl.org/?view&did=28659.

Bell, J. and Whaley, B. 1982. *Cheating and Deception.* New Brunswick, NJ : Transaction Publishers, 1982.

Belz, Frank C. 2011. *Space Segment Information Assurance Guidance for Mission Success.* s.l. : Aerospace Report No. TOR-2011(8591)-22, 2011.

Bingham, Kevin. 2011. Computer Network Defense Architecture –Driving to enable defensibility, resilience and "fight through". *DoD CND Architect, Office of DoD CIO.* [Online] April 2011. [Cited: October 26, 2011.]

http://www.dodenterprisearchitecture.org/pastmeetings/Documents/2011_DoD_EA_CND%20Architecture_Bingham.pdf.
Bodeau, Deb, Graubart, Richard and Fabius, Jennifer. 2009. Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels, PR 09-4659. [Online] 2009. [Cited: September 1, 2011.] http://www.mitre.org/work/tech_papers/2010/09_4656/09_4656.pdf.
Bodeau, Deborah J., Graubart, Richard D. and Fabius-Greene, Jennifer. 2010. *Cyber Security Governance, MTR100308, PR 10-3710.* Bedford, MA : The MITRE Corporation, 2010.
Bodeau, Deborah, et al. 2010. *Using Cyber Prep: The Concept of Operations for MITRE's Cyber Preparedness Methodology.* Bedford, MA : The MITRE Corporation, 2010.
Bondavalli, A., Lollani, P. and Vadursi, M. 2010. *AMBER Roadmap: Ongoing Research Directions.* 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops (ICDCSW). Genova : IEEE, 2010.
Booz | Allen | Hamilton. 2011. Cyber Operations Maturity Framework: A Model for Collaborative, Dynamic Cybersecurity. [Online] 2011. [Cited: October 26, 2011.] http://www.boozallen.com/media/file/Cyber-Operations-Maturity-Framework-viewpoint.pdf.
Brun, Yuriy, et al. 2009. Engineering Self-Adaptive Systems through Feedback Loops. *B.H.C. Cheng et al. (Eds.): Self-Adaptive Systems, LNCS 5525, pp. 48-70.* [Online] 2009. [Cited: October 26, 2011.] http://www.cs.washington.edu/homes/brun/pubs/pubs/Brun09SEfSAS.pdf.
CERT Program. 2010. CERT® Resilience Management Model, Version 1.0: Improving Operational Resilience Processes. [Online] May 2010. [Cited: October 26, 2011.] http://www.cert.org/archive/pdf/10tr012.pdf.
Cheng, B. H.C., de Lemos, R. and Magee, J. 2009. *Software Engineering for Self-Adaptive Systems.* s.l. : Springer-Verlag Lecture Notes in Computer Science, 2009. Vol. 5525.
CIANCNF. 2010. *Information Assurance for Network-centric Naval Forces.* Washington, DC : National Academies Press, 2010.
Cloppert, Michael. 2009. Security Intelligence: Attacking the Kill Chain. *SANS Computer Forensics and Incident Response Blog.* [Online] October 14, 2009. [Cited: October 26, 2011.] http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/.
CMMI Team. 2007. Introduction to the Architecture of the CMMI® Framework, Software Engineering Institute (SEI), Carnegie-Mellon University (CMU), Technical Note CMU/SEI-2007-TN-009. [Online] July 2007. [Cited: October 26, 2011.] http://www.sei.cmu.edu/reports/07tn009.pdf.
CNSS. 2010. National Information Assurance (IA) Glossary, CNSSI No. 4009. [Online] April 26, 2010. [Cited: October 26, 2011.] http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.
Cole, Eric, Krutz, Ronald L. and Conley, James. 2009. *The Network Security Bible, 2nd Edition.* Hoboken, NJ : John Wiley and Sons, 2009.
Croom, Charles. 2010. The Defender's "Kill Chain". *Military Information Technology, Vol. 14, No. 10.* [Online] November 2010. [Cited: October 26, 2011.] http://www.military-information-technology.com/mit-home/288-mit-2010-volume-14-issue-10-november/3693-cyber-situational-awareness.html.
CyberCARD. 2011. Workshop on Cooperative Autonomous Resilient Defenses in Cyberspace. [Online] January 27-28, 2011. [Cited: June 6, 2011.] http://www.sis.pitt.edu/~cybercard/index.html.
Dalziell, E. P. and McManus, S. T. 2005. Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance. [Online] January 25, 2005. [Cited: October 26, 2011.] http://www.ifed.ethz.ch/events/forum04/erica_paper.pdf.

DARPA. 2010. Clean-Slate Design of Resilient, Adaptive, Secure Hosts. [Online] June 4, 2010. [Cited: October 26, 2011.] http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147484031.
Dekker, Sidney, et al. 2008. Resilience Engineering:New directions for measuring and maintaining safety in complex systems. *Lund University School of Aviation.* [Online] November 2008. [Cited: October 26, 2011.] https://msb.se/Upload/Kunskapsbank/Forskningsrapporter/Slutrapporter/Resilience%20Engineering%20New%20directions%20for%20measuring%20and%20maintaining%20safety%20in%20complex%20systems.pdf.
DESEREC. 2008. DEpendability and Security by Enhanced REConfigurability. [Online] November 9, 2008. [Cited: October 26, 2011.] http://www.deserec.eu/.
DHS. 2011. Enabling Distributed Security in Cyberspace: Builiding a Healthy and Secure Cyber Ecosystem. [Online] March 23, 2011. [Cited: October 26, 2011.] http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.
DoD. 2008. *Defense Critical Infrastructure Program (DCIP) Management, DoDI 3020.45.* 2008.
—. 2011. Fact Sheet: Resilience of Space Capabilities. [Online] October 11, 2011. [Cited: December 7, 2011.] http://www.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf.
—. 2011. Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, 8 November 2010, as amended. [Online] July 15, 2011. [Cited: September 1, 2011.] http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
—. 2006. National Military Strategy for Cyberspace Operations. [Online] 2006. [Cited: October 26, 2011.] http://www.carlisle.army.mil/DIME/documents/National%20Military%20Strategy%20for%20Cyberspace%20Operations.pdf.
Duffey, Romney. 2008. The Quantification of Resilience: Learning Environments and Managing Risk. *Proceedings of the 3rd Symposium on Resilience Engineering.* [Online] October 28-30, 2008. [Cited: October 26, 2011.] http://www.resilience-engineering.org/RE3/papers/Duffey_text.pdf.
Dugdale, Julie and Pavard, Bernard. 2009. Robustness and resilience in the design of emergency management systems. *MAGMA Recherche.* [Online] 2009. [Cited: August 4, 2011.] http://magma.imag.fr/publications/papers/Dugdale-Pavard-09.pdf.
Edwards, John. 2011. DARPA to help shield cloud networks from cyberattack. *Defense Systems.* [Online] August 17, 2011. [Cited: August 23, 2011.] http://defensesystems.com/articles/2011/08/08/tech-watch-darpa-cloud-security.aspx.
Ellison, Robert J. and Woody, Carol. 2010. Survivability Analysis Framework. *CMU/SEI-2010-TN-013.* [Online] June 2010. [Cited: May 28, 2011.] http://www.cert.org/archive/pdf/10tn013.pdf.
Eltoweissy, Mohamed. 2011. CyberCARD: Cooperative Autonomous Resilient Defenses in Cyberspace - Defining a path for the future. [Online] January 27-28, 2011. [Cited: June 6, 2011.] http://www.sis.pitt.edu/~cybercard/others/Eltoweissy-CyberCARD-Workshop.pptx.
2011. Enabling and managing end-to-end resilience. [Online] January 24, 2011. [Cited: May 26, 2011.] http://www.enisa.europa.eu/act/it/library/deliverables/e2eres/at_download/fullReport.
ENISA. 2011. Cyber Europe 2010 - Evaluation Report. [Online] March 18, 2011. [Cited: October 26, 2011.] http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/at_download/file.

—. 2009. Gaps in standardisation related to resilience of communication networks. [Online] December 18, 2009. [Cited: October 26, 2011.] http://www.enisa.europa.eu/act/it/library/deliverables/gapsstd/at_download/fullReport.
—. 2010. Inter-X: Resilience of the Internet Interconnection Ecosystem. [Online] September 9, 2010. [Cited: October 26, 2011.] http://www.enisa.europa.eu/act/res/other-areas/inter-x/about-the-inter-x-study/interconnections-flyers.
—. 2011. Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report (Discussion draft). [Online] February 21, 2011. [Cited: October 26, 2011.] http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report/at_download/fullReport.
—. 2011. Ontology and taxonomies for critical infrastructures . [Online] 2011. http://www.enisa.europa.eu/act/it/ontology-ws.
—. 2011. Proactive Detection of Network Security Incidents. [Online] December 7, 2011. [Cited: December 9, 2012.] http://www.enisa.europa.eu/act/cert/support/proactive-detection/proactive-detection-report/at_download/fullReport.
—. 2009. Resilience Features of IPv6, DNSSEC and MPLS: Resilience of communications networks. [Online] January 21, 2009. [Cited: May 26, 2011.] http://www.enisa.europa.eu/act/res/technologies/tech/resilience-features-of-technologies/at_download/fullReport.
—. 2011. Resilience Metrics and Measurements: Challenges and Recommendations . [Online] March 18, 2011. [Cited: May 23, 2011.] http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-survey/at_download/fullReport.
—. 2005-2011. Resilient technologies. [Online] 2005-2011. [Cited: May 26, 2011.] http://www.enisa.europa.eu/act/res/technologies/inf.
Erol, Ozgur, et al. 2010. Perspectives on Measuring Enterprise Resilience. *IEEE International Systems Conference, San Diego, CA.* [Online] April 5-8, 2010. [Cited: May 24, 2011.] http://www.stevens.edu/csr/fileadmin/csr/Publications/Erol_et_al._IEEE_systems_conference_2010_FINAL-1.pdf.
ETSI. 2008. Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN). *ETSI TR 187 010 V2.1.1 (2008-07).* [Online] 2008. [Cited: May 26, 2011.] http://www.etsi.org/deliver/etsi_tr/187000_187099/187010/02.01.01_60/tr_187010v020101p.pdf .
EUROCONTROL. 2009. A White Paper on Resilience Engineering for ATM [Air Traffic Management]. [Online] September 2009. [Cited: October 26, 2011.] http://www.eurocontrol.int/esp/gallery/content/public/library/A%20White%20Paper%20Resilience%20Engineering/A_White_Paper_Resilience_Engineering.pdf.
Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation (invited paper)" . [Online] http://www.ittc.ku.edu/resilinets/papers/Sterbenz-Cetinkaya-Hameed-Jabbar-Qian-Rohrer-2011.pdf.
Foote, Scott, Kramer, Mark and Yost, Beth. 2011. Alternative Processes and Operations Controlled via a Cyber Operations Center (CyOC), PR # 11-1567. *The MITRE Corporation.* [Online] 2011. [Cited: September 13, 2011.] http://www.mitre.org/work/areas/research/2011iebriefings/05MSR160-JO.pdf.
Foreman, Park. 2005. Implementing a Security Operations Center. *ISSA Journal.* [Online] August 2005. [Cited: November 7, 2011.]

http://www.issa.org/Library/Journals/2005/August/Foreman%20-%20Implementing%20a%20Security%20Operations%20Center.pdf.
Ghosh, Debanjan, et al. 2006. Self-healing systems — survey and synthesis. *Decision Support Systems 42 (2007) 2164–2185.* [Online] August 17, 2006. [Cited: May 28, 2011.] http://www.som.buffalo.edu/isinterface/papers/Self-healing%20systems.pdf.
Goldman, Harriet. 2010. *Building Secure, Resilient Architectures for Cyber Mission Assurance.* Bedford, MA : The MITRE Corporation, #10-3301, 2010. http://www.mitre.org/work/tech_papers/2010/10_3301/10_3301.pdf.
Goldman, Harriet, McQuaid, Rosalie and Picciotto, Jeffrey. 2011. Cyber Resilience for Mission Assurance. *Proceedings of the 2011 IEEE Conference on Technologies for Homeland Security.* Waltham, MA : IEEE, 2011.
Haimes, Yacov. 2009. On the Definition of Resilience in Systems. *Risk Analysis.* 2009, Vol. 29, 4.
Haimes, Yacov, Crowther, Kenneth and Horowitz, Barry. 2008. Homeland Security Preparedness: Balancing Protection with Resilience in Emerging Systems. *Systems Engineering.* 2008, Vol. 11, 4.
Hollnagel, Erik. 2004. *Barriers and Accident Prevention.* s.l. : Ashgate, 2004.
—. 2010. Prologue: The Scope of Resilience Engineering. *Sample pages from Resilience Engineering in Practice: A Guidebook, Ashgate.* [Online] 2010. [Cited: May 24, 2011.] http://www.ashgate.com/pdf/SamplePages/Resilience_Engineering_in_Practice_Prol.pdf.
—. 2009. The Four Cornerstones of Resilience Engineering. [book auth.] Christopher P. Nemeth, Erik Hollnagel and Sidney Dekker. *Resilience Engineering Perspectives.* s.l. : Ashgate, 2009.
Hollnagel, Erik, Nemeth, C.P. and Dekker, S. 2008. *Resilience Engineering Perspectives – Remaining Sensitive to the Possibility of Failure.* s.l. : Ashgate, 2008.
Hollnagel, Erik, Woods, David D. and Leveson, Nancy. 2006. *Resilience Engineering: Concepts and Precepts.* s.l. : Ashgate, 2006.
Homeland Security Studies and Analysis Institute. 2010. Risk and Resilience: Exploring the Relationship. [Online] November 22, 2010. [Cited: May 18, 2011.] http://www.homelandsecurity.org/hsireports/Risk-Resilience_Report_Final_public%20release%20version%20_Task_10-17_29-Nov-2010.pdf.
HSSIA. 2009. Concept Development: An Operational Framework for Resilience. [Online] August 2009, 2009. [Cited: October 26, 2011.] http://www.homelandsecurity.org/hsireports/Resilience_Task_09-01.pdf.
—. 2010. Risk and Resilience: Exploring the Relationship. [Online] November 22, 2010. [Cited: October 26, 2011.] http://www.homelandsecurity.org/hsireports/Risk-Resilience_Report_Final_public_release_version_Task_10-17_29-Nov-2010.pdf.
IBM. 2006. Crisis simulation exercise. *IBM Business Continuity and Recovery Services.* [Online] 2006. [Cited: September 20, 2011.] http://www-935.ibm.com/services/uk/its/pdf/crisis_management_06_its_001943.pdf.
IEEE . 2011. TC on Dependable Computing and Fault Tolerance. [Online] 2011. [Cited: May 24, 2011.] http://www.computer.org/portal/web/tandc/tcft.
IFIP. 2011. WG 10.4 on Dependable Computing and Fault Tolerance. [Online] February 15, 2011. [Cited: May 24, 2011.] http://www.dependability.org/wg10.4/.
INCOSE. 2010. Resilient Systems Working Group. [Online] May 20, 2010. [Cited: 31 May, 2011.] http://www.incose.org/practice/techactivities/wg/rswg/.
—. 1998. Systems Engineering Measurement Primer. [Online] March 1998. [Cited: May 23, 2011.]

http://www.afit.edu/cse/docs/guidance/System%20Engineering%20Measurement%20Primer%201998-03.pdf.
ITGI and ISACA. 2006. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition. [Online] 2006. [Cited: October 26, 2011.] http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf.
ITU-T. 2008. Overview of cybersecurity, ITU-T X.1205. [Online] April 2008. http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items.
Jackson, Scott. 2009. *Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions.* Hoboken, NJ : John Wiley and Sons, 2009.
JCS. 2009. Joint Terminology for Cyberspace Operations. [Online] August 18, 2009. http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.
Johansson , Björn and Lindgren, Mattias. 2008. A quick and dirty evaluation of resilience enhancing properties in safety critical systems. *Proceedings of the 3rd Symposium on Resilience Engineering.* [Online] October 28-30, 2008. [Cited: May 23, 2011.] http://www.resilience-engineering.org/RE3/papers/Johansson_Lindgren_text.pdf.
King, Steven. 2011. DoD Cyber S&T Priority Steering Council Research Roadmap for the National Defense Industrial Association Disruptive Technologies Conference. [Online] November 8, 2011. [Cited: December 9, 2011.] http://www.acq.osd.mil/chieftechnologist/publications/docs/2011%2011%2001%20Cyber%20PSC%20Roadmap.pdf.
Koopman, Philip. 2003. Elements of the Self-Healing Problem Space. *Workshop on Algorithms and Data Structures.* [Online] 2003. http://www.ece.cmu.edu/~koopman/roses/wads03/wads03.pdf.
Krekel, Bryan. 2009. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. *The US-China Economic and Security Review Commission.* [Online] October 9, 2009. [Cited: June 8, 2011.] http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.
Laprie, Jean-Claude. 2008. From Dependability to Resilience. *Proceedings of the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.* [Online] 2008. [Cited: May 24, 2011.] http://www.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_laprie.pdf.
Lay, Elizabeth, Wreathall and John. 2008. Improving Resilience by "Pinging" to Determine Risk Profile Changes during Maintenance Work. *Proceedings of the 3rd Symposium on Resilience Engineering.* [Online] October 28-30, 2008. [Cited: May 24, 2011.] http://www.resilience-engineering.org/RE3/papers/Lay_Wreathall_text.pdf.
Lima, Nogueira Michele, dos Santos, Aldri Luiz and Pujolle, Guy. 2009. A Survey of Survivability in Mobile Ad Hoc Networks. *IEEE Communications Surveys & Tutorials.* 2009, Vol. 11, 1.
LMCA. 2010. The Lockheed Martin Cybersecurity Alliance. [Online] May 21, 2010. [Cited: May 18, 2011.] http://www.lockheedmartin.com/data/assets/isgs/documents/LM-cyber-security-alliance-brochure.pdf.
MacIntosh, JP, Reid, J and Tyler, LR. 2011. Cyber Doctrine: Toward a coherent evolutionary framework for learning resilience. *Insititue for Security & Resilience Studies.* [Online] June 2011. [Cited: August 31, 2011.] http://www.ucl.ac.uk/isrs/publications/CyberDoctrine.

MacQueen, Miles and Boyer, Wayne. 2009. *Deception used for Cyber Defense of Control Systems.* Proceedings of the 2009 IEEE Conference on Human-System Interactions (HSI 2009). Catania, Italy : IEEE, 2009.
Madni, Azad M. and Jackson, Scott. 2009. Towards a Conceptual Framework for Resilience Engineering. *IEEE Systems Journal, Vol. 3, No. 2.* June 2009.
Madni, Azad M. 2007. *Designing for Resilience.* s.l. : ISTI Lecture Notes on Advanced Topics in Systems Engineering, 2007.
McAfee. 2011. Ten Days of Rain: Expert analysis of distributed denial-of-service attacks targeting South Korea. [Online] July 2011. [Cited: September 6, 2011.] http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf.
Meredith, Michael G. 2003. Enhancing Survivability with Proactive Fault-Containment. *Student Forum, IEEE International Conference on Dependable Systems and Networks (DSN). San Francisco, CA. June 2003.* [Online] June 2003. [Cited: May 28, 2011.] http://www.ece.cmu.edu/~starfish/papers/merideth03enhancing.pdf.
Merideth, Michael G. and Narasimhan, Priya. 2003. Metrics for the Evaluation of Proactive and Reactive Survivability. *Fast Abstracts Session, IEEE International Conference on Dependable Systems and Networks (DSN). San Francisco, CA. June 2003.* [Online] June 2003. [Cited: May 28, 2011.] http://www.ece.cmu.edu/~starfish/papers/merideth03metrics.pdf.
—. 2003. Proactive Containment of Malice in Survivable Distributed Systems. *International Conference on Security and Management (SAM). Las Vegas, NV. June 2003.* . [Online] June 2003. [Cited: May 28, 2011.] http://www.ece.cmu.edu/~starfish/papers/merideth03proactive.pdf.
Merriam-Webster. 2011. Merriam-Webster Dictionary. [Online] 2011. [Cited: October 26, 2011.] http://www.merriam-webster.com/dictionary/cybersecurity.
MITRE. 2011. Systems Engineering for Mission Assurance. *Systems Engineering Guide.* [Online] April 26, 2011. [Cited: December 13, 2011.] http://www.mitre.org/work/systems_engineering/guide/enterprise_engineering/se_for_mission_assurance/.
Napoli, Joseph C. 2007. Resiliency, Resilience, Resilient: A Paradigm Shift? [Online] 2007. [Cited: August 31, 2011.] http://www.resiliency.us/media/Resiliency,%20R,%20R_%20A_%20Paradigm_Shift_08-22-07.doc.
NDIA. 2009. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. [Online] 2009. [Cited: May 24, 2011.] http://www.ndia.org/Advocacy/PolicyPublicationsResources/Documents/Cyberspace_policy_review_2009.pdf .
Nemeth, Christopher P. 2008. Resilience Engineering: The Birth of a Notion. [book auth.] Erik Hollnagel, Christopher P. Nemeth and Sidney Dekker. *Resilience Engineering Perspectives, Volume 1: Remaining Sensitive to the Possibility of Failure.* s.l. : Ashgate, 2008.
NIAC. 2010. A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council. [Online] October 19, 2010. [Cited: October 26, 2011.] http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.
NIST. 2004. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. [Online] February 2004. [Cited: October 26, 2011.] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

—. 2011. Glossary of Key Information Security Terms, NIST IR 7298 Revision 1. [Online] February 2011. [Cited: October 26, 2011.] http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf.
—. 2010. Guide for Applying the Risk Management Framework to Federal Information Systems, NIST SP 800-37, Rev. 1. *NIST.* [Online] February 2010. [Cited: October 10, 2011.] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
—. 2010. NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. [Online] November 11, 2010. [Cited: May 19, 2011.] http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.
—. 2011. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. [Online] March 2011. [Cited: May 23, 2011.] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.
NITRD CSIA IWG. 2010. Cybersecurity Game-Change Research & Development Recommendations. [Online] May 13, 2010. [Cited: October 26, 2011.] http://www.nitrd.gov/CSThemes/CSIA_IWG_Cybersecurity_Game-Change_%20RD_Recommendations_20100513.pdf.
NSC. undated. Cybersecurity. [Online] undated. [Cited: October 26, 2011.] http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.
OCS. 2009. Cyber Security Strategy of the United Kingdom. [Online] June 2009. [Cited: October 26, 2011.] http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf.
Omer, Mayada, Nilchiani, Roshanak and Mostashari, Ali. 2010. Measuring the Resilience of the Global Internet Infrastructure System. *The Center for Secure and Resilient Maritime Commerce* . [Online] 2010. [Cited: May 24, 2011.] http://www.stevens.edu/csr/fileadmin/csr/Publications/Omer_Measuring_the_Resilience_of_the_Global_Internet__Infrastructure.pdf.
OSD(SP). 2011. *Resilience of Space Capabilities: White Paper.* Washington, DC : Office of the Secretary of Defense -Space Policy, 2011.
O'Shea, Kevin. 2003. Cyber-Attack Investigative Tools and Technologies. *Institute for Security Technology Studies, Dartmouth College.* [Online] May 7, 2003. [Cited: November 8, 2011.] http://www.ists.dartmouth.edu/library/107.pdf.
Pal, Partha, et al. 2010. Fighting Through Cyber Attacks: An Informed Perspective Toward the Future. *Workshop on Survivability in Cyber Space* . [Online] April 12, 2010. [Cited: June 6, 2011.] http://www.dist-systems.bbn.com/papers/2010/AFRL-SCS/paper.pdf.
Peters, Wende. 2009. Mission Based Analysis for Cyber Measurement and Mission Assurance. [Online] October 28, 2009. [Cited: December 13, 2011.] http://scap.nist.gov/events/2009/itsac/presentations/day3/Day3_Compliance_Peters.pdf.
Preparedness, Response, and Resilience Task Force. 2011. Interim Task Force Report on Resilience. *Homeland Security Policy Institute, George Washington University.* [Online] May 16, 2011. [Cited: October 26, 2011.] http://www.gwumc.edu/hspi/policy/report_Resilience1.pdf.
Psaier, Harald and Dustdar, Schahram. 2011. A survey on self-healing systems: approaches and systems. *Computing, DOI 10.1007/s00607-010-0107-y.* [Online] August 5, 2011. [Cited: mAY 28, 2011.] http://www.infosys.tuwien.ac.at/Staff/sd/papers/Zeitschrift%20Computing%20H.%20Psaier.pdf.
Ramasamy, HariGovind V., Agbaria, Adnan and Saunders, William H. 2004. *CoBFIT: A Component-Based Framework for Intrusion Tolerance.* Proceedings of the 30th Euromicro Conference. 2004.
REN. 2011. Resilience Engineering Network. [Online] 2011. [Cited: May 31, 2011.] http://www.resilience-engineering.org/.

ReSIST. 2007. Resilience for Survivability in IST: Summary. [Online] 2007. [Cited: May 26, 2011.] http://www.resist-noe.org/DOC/ReSIST_Summary.pdf.
—. 2008. Resilience ontology: final. [Online] December 2008. [Cited: May 26, 2011.] http://www.resist-noe.org/Publications/Deliverables/D34-Resilience_Ontology_Final.pdf.
—. 2006. Resilience-Building Technologies: State of Knowledge. [Online] September 2006. [Cited: May 26, 2011.] http://www.resist-noe.org/Publications/Deliverables/D12-StateKnowledge.pdf.
—. 2009. Resilience-Building Technologies: State of Knowledge - Appendices – Papers produced by ReSIST partners since January 2006. [Online] November 2009. [Cited: May 26, 2011.] http://www.resist-noe.org/Publications/Deliverables/D12-StateKnowledgeAppend.pdf.
—. 2008. Resilience-Explicit Computing: final. [Online] December 2008. [Cited: May 26, 2011.] http://www.resist-noe.org/Publications/Deliverables/D33-ResEx_computing_final.pdf.
—. 2006-2009. RESIST : Resilience for survivability in IST. [Online] 2006-2009. [Cited: May 26, 2011.] http://www.resist-noe.org/.
—. 2007. Support for Resilience-Explicit Computing - first edition. [Online] September 2007. [Cited: May 26, 2011.] http://www.resist-noe.org/Publications/Deliverables/D11-ResEx_Computing.pdf.
Richards, M. G., et al. 2009. Design for Survivability: Concept Generation and Evaluation in Dynamic Tradespace Exploration. *Second International Symposium on Engineering Systems, MIT, Cambridge, Massachusetts, June 15-17, 2009.* [Online] June 15-17, 2009. [Cited: May 28, 2011.] http://web.mit.edu/mgr/www/Portfolio/Design%20for%20Survivability%20-%20Concept%20Generation%20and%20Evaluation%20in%20Dynamic%20Tradespace%20Exploration.pdf.
Richards, Matthew G., et al. 2008. Empirical Validation of Design Principles for Survivable System Architecture. *2nd IEEE Systems Conference, Montreal, Canada, April 2008.* [Online] April 2008. [Cited: May 28, 2011.] http://web.mit.edu/mgr/www/Portfolio/Empirical%20Validation%20of%20Design%20Principles%20for%20Survivable%20System%20Architecture.pdf.
Rieger, Craig, Gertman, David and McQueen, Miles. 2009. Resilient Control Systems: Next Generation Design Research. *Proceedings of the 2009 IEEE Conference on Human Systems Interactions (HSI).* s.l. : IEEE, 2009.
Risk Steering Committee. 2010. DHS Risk Lexicon, 2010 Edition. [Online] September 2010. [Cited: May 23, 2011.] http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.
Roscini, Marco. 2010. World Wide Warfare - Jus ad Bellam and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law, Vol. 14, 2010, pp. 85-130.* [Online] 2010. [Cited: November 8, 2011.] http://www.mpil.de/shared/data/pdf/pdfmpunyb/03_roscini_14.pdf.
Sandia. 2009. A Framework for Critical Infrastructure Resilience Analysis. [Online] September 2009. [Cited: October 26, 2011.] http://www.sandia.gov/mission/ste/stories/2009/September%202009/individual%20files/Snyder-09.pdf.
Schulte, Gregory. 2011. Building Architectures for New Challenges in Space and the Budget. [Online] June 28, 2011. [Cited: December 14, 2011.] http://www.defense.gov/home/features/2011/0111_nsss/docs/Speech_at_the_National_Security_Space_Policy_and_Architecture_Symposium,_June_28,_2011.pdf.
SEPO. 2011. SEPO Risk Management Toolkit. [Online] August 31, 2011. [Cited: August 31, 2011.] http://www.mitre.org/work/sepo/toolkits/risk/.
Sheard, Sarah and Mostashari, Ali. 2003. A Framework for System Resilience Discussions. *Foresight.* [Online] 2003. [Cited: October 20, 2011.]

http://www.stevens.edu/csr/fileadmin/csr/Publications/Sheard_SystemsResilienceDiscussions.pdf.
Sheridan, Thomas B. 2008. Risk, Human Error, and System Resilience: Fundamental Ideas. *Human Factors: The Journal of the Human Factors and Ergonomics Society.* June 2008, pp. 418-426.
Shrobe, Howard. 2011. Secure Computer Systems. *DARPA Cyber Colloquium.* [Online] November 7, 2011. [Cited: December 9, 2011.] http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147484460.
SLSIS. 2011. Announcement: The 2011 International Workshop on Survivable Large-Scale Information Systems. [Online] 2011. [Cited: October 26, 2011.] http://www.cs.unic.ac.cy/harald/SLSIS2011.html.
Space Daily Staff. 2011. US, Britain urge cooperation on cyber threats. *Space Daily.* [Online] June 4, 2011. [Cited: June 8, 2011.] http://www.spacedaily.com/reports/US_Britain_urge_cooperation_on_cyber_threats_999.html.
Sterbenz, James P.G. and Hutchinson, David. 2006. ResilieNets: Multilevel Resilient and Survivable Networking Initiative. [Online] August 15, 2006. [Cited: May 24, 2011.] http://www.ittc.ku.edu/resilinets/.
—. 2011. ResiliNets Wiki. [Online] May 14, 2011. [Cited: May 24, 2011.] https://wiki.ittc.ku.edu/resilinets/Main_Page.
Sterbenz, James P.G., et al. 2011. Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation (invited paper). *Accepted by Springer Telecommunications Journal.* [Online] March 2011. [Cited: May 23, 2011.]
Sterbenz, James P.G., et al. 2010. Resilience and survivability in communication networks: Strategies,principles, and survey of disciplines. *Computer Networks 54 (2010) 1245–1265.* [Online] March 17, 2010. [Cited: May 23, 2011.] http://www.ittc.ku.edu/resilinets/papers/Sterbenz-Hutchison-Cetinkaya-Jabbar-Rohrer-Scholler-Smith-2010.pdf.
Stoneburner, Gary, Hayden, Clark and Feringa, Alexis. 2004. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication 800-27 Rev A. [Online] June 2004. [Cited: September 19, 2011.] http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
Swarup, Vipin. 2009. Mission Assurance Against Advanced Cyber Threats, PR 09-1253. *The MITRE Corporation.* [Online] May 5, 2009. [Cited: September 30, 2011.] http://www.mitre.org/news/events/exchange09/05MSR147.pdf.
Tan, Kheng Lee Gregory. 2003. Confronting Cyberterrorism with Cyber Deception. [Online] December 2003. [Cited: November 8, 2011.] http://www.au.af.mil/au/awc/awcgate/nps/cyberterr_cyberdecep.pdf.
Tarvainen, Pentti. 2004. Survey of the Survivability of IT Systems. [Online] November 17, 2004. [Cited: May 28, 2011.] http://virtual.vtt.fi/virtual/proj1/projects/merlin/pub/survey_of_the_survivability_of_it_systems.pdf.
TASC. 2011. Understanding Today's Cyber Challenges. [Online] May 2011. [Cited: May 29, 2011.] http://www.tasc.com/news_media/white_papers/TASC_Cyber_Challenges_Study_May_2011_FINAL.pdf.

TISP. 2011. Regional Disaster Resilience: Guide for Developing an Action Plan (Draft for External Review). [Online] April 11, 2011. [Cited: May 31, 2011.] http://www.tisp.org/index.cfm?pk=download&pid=10261&id=12078.
Trade-off Strategies in Engineering Design. **Otto, Kevin N. and Antonsson, Erik K. 1991.** 2, s.l. : Research in Engineering Design, 1991, Vol. 3, pp. 87-104.
Trimintzios, Panagiotis , et al. 2011. Inter-X: Resilience of the Internet Interconnection Ecosystem. [Online] April 2011. [Cited: May 26, 2011.] http://www.enisa.europa.eu/act/res/other-areas/inter-x/report/interx-report/at_download/fullReport.
van Moorsel, Aad and Madeira, Henrique. 2009. State of the Art. [Online] October 19, 2009. [Cited: May 26, 2011.] http://www.amber-project.eu/documents/md_242_amber_d2.2_stateoftheart_v2.0final_submit.pdf.
Vlacheas, Panagiotis T., et al. 2011. Ontology and taxonomies of resilience (DRAFT). *ENISA.* [Online] October 2011. [Cited: October 21, 2011.] http://www.enisa.europa.eu/act/it/ontology-ws/resontax-draft.
Wang, Alex Hai, Yan, Su and Liu, Peng. 2010. *A Semi-Markov Survivability Evaluation Model for Intrusion Tolerant Database Systems.* 2010 International Conference on Availability, Reliability and Security (ARES 2010). Krakow, Poland : IEEE, 2010.
White House. 2009. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. [Online] May 29, 2009. [Cited: August 30, 2011.] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
—. 2010. National Security Strategy. [Online] May 2010. [Cited: November 7, 2011.] http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
—. 2011. Presidential Policy Directive-8, National Preparedness. [Online] March 30, 2011. [Cited: November 7, 2011.] http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm.
Whitworth, Brian. 2009. A Brief Introduction to Sociotechnical Systems. [book auth.] Mehdi Khosrow-Pour. *Encyclopedia of Information Sicence and Technology, 2nd Edition.* s.l. : IGI Global, 2009.
—. 2009. The Social Requirements of Technical Systems. [book auth.] Brian Whitworth and Aldo de Moor. *Socio-Technical Design and Social Networking Systems.* s.l. : IGI Global, 2009.
Woltjer, Rogier. 2008. Resilience Assessment Based on Models of Functional Resonance. *Proceedings of the 3rd Symposium on Resilience Engineering.* [Online] October 28-30, 2008. [Cited: May 24, 2011.] http://www.resilience-engineering.org/RE3/papers/Woltjer_text.pdf.
Woods, David and Wreathall, John. Stress-Strain Plots as a Basis for Assessing System Resilience. *Chapter 12 in Resilience Engineering Perspectives, Volume 1: Remaining Sensitive to the Possibility of Failure, Ashgate.* [Online] [Cited: May 24, 2011.] http://csel.eng.ohio-state.edu/productions/ibm/Woods_Wreathall-stress-strain%20w-refs.pdf.
Wright, Austin. 2009. National-Security Infrastructure Faces Relentless Cyberespionage Campaign . *National Defense Magazine.* [Online] December 2009. [Cited: June 8, 2011.] http://www.nationaldefensemagazine.org/archive/2009/December/Pages/National-SecurityInfrastructureFacesRelentlessCyberespionageCampaign.aspx.
WSC. 2010. Workshop on Survivability in Cyberspace. [Online] April 12, 2010. [Cited: June 6, 2011.] http://eecs.ucf.edu/scs/program.html.
Zhang, Wensheng, et al. 2005. *Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks.* MobiHoc'05. Chicago : ACM, 2005.

Appendix B: Related Engineering Disciplines and Other Work

This appendix provides background on the related engineering disciplines which inform the cyber resiliency engineering framework presented in Section 4. Cyber resiliency engineering is informed by a variety of overlapping systems engineering disciplines, including

- Resilience engineering
- Network resilience
- System resilience in critical infrastructures
- Resilience management
- Contingency planning
- High-performance computing and networking
- Dependable computing and fault-tolerance, including
    - Survivable and self-adaptive systems
    - Self-healing systems
    - Intrusion-tolerant systems

The relationships between cyber resiliency engineering and other systems engineering disciplines are discussed below, with attention to how resilience can be assessed or measured, the relationship between resilience and risk, and research which might be relevant to cyber resiliency. The relationships between the cyber resiliency practices identified in Section 4 and other work are also identified.

B.1 Resilience Engineering

Cyber resiliency engineering could be characterized as resilience engineering focused on cyber threats. Certainly, the cyber resiliency engineering framework presented in Section 4 is informed by frameworks and heuristics developed by resilience engineers. However, the cyber resiliency engineering framework focuses on architectural practices, emphasizing technical systems; socio-technical aspects are treated as supporting rather than central.

As defined in (Hollnagel, et al., 2006) (Hollnagel, et al., 2008),

> "Resilience engineering is a paradigm for safety management that focuses on how to help people cope with complexity under pressure to achieve success… The initial steps in developing a practice of Resilience Engineering have focused on methods and tools:
>
> - to analyse, measure and monitor the resilience of organisations in their operating environment.
> - to improve an organisation's resilience vis-à-vis the environment.
> - to model and predict the short- and long-term effects of change and line management decisions on resilience and therefore on risk."

Resilience engineering builds on safety engineering, but treats faults and failures in socio-technical systems[32] rather than in purely technical systems. The focus of resilience engineering is on the organization and on the socio-technical system in the presence of accidents, errors, and

[32] Socio-technical systems are combinations of social and technical elements which collectively are intended to achieve goals. Socio-technical systems can be viewed as the top of four levels, layered on top of human-computer interaction (HCI) systems, which are in turn layered on top of software systems, which are layered on top of hardware systems (Whitworth, 2009).

disasters. In particular, resilience engineering is well suited to systems which are tightly coupled but intractable (incapable of being completely described or specified) from a management standpoint (EUROCONTROL, 2009).

B.1.1 Conceptual Framework for Resilience Engineering

Madni defines four aspects of resilience which can be interpreted with respect to the cyber threat ((Madni, 2007), quoted in (Madni, et al., 2009)):

- Avoid (anticipation)[33]
- Withstand (absorption)
- Recover from (restoration)
- Adapt to (reconfiguration)

Based on an extensive literature review, Madni defines a conceptual framework for resilience engineering. In that framework, system attributes are affected by disruptions, which can be natural or man-made; external or systemic; single-agent or multi-agent; and short-lived or enduring. For cyber resiliency, disruptions are typically man-made, but can involve deliberate exploitation of transient vulnerabilities resulting from natural disaster; disruptions can be systemic (i.e., the result of actions within the system) when malicious insiders are involved, but are more typically externally created; prudence suggests assuming multiple agents and enduring disruption. The framework identifies several types of metrics:

- "Time/cost to restore operation
- Time/cost to restore configuration/reconfigure
- Time/cost to restore functionality/performance
- Degree to which pre-disruption state is restored
- Potential disruption circumvented
- Successful adaptations within time and cost constraints"

Finally, Madni and Jackson identify "resilience heuristics" – "qualitative design methods grounded in experience" – which strongly resemble some of the cyber resiliency practices discussed in (Goldman, 2010): functional redundancy, physical redundancy, reorganization, human backup, "human-in-the-loop", predictability, complexity avoidance, context spanning, graceful degradation, drift correction, "neutral" state, inspectability, intent awareness, and learning/adaptation (Madni, et al., 2009).

B.1.2 Resilience Engineering and Metrics

Despite the types of metrics suggested above, skepticism regarding metrics remains: "It is now too early to expect resilience engineering to offer much in terms of quantitative models, but eventually human factors engineers will demand it." ((Sheridan, 2008), quoted in (Johansson , et al., 2008)) One approach is to model and assess stability (Duffey, 2008). The Functional

[33] "Resilience involves anticipation. This includes the consideration of how and why a particular risk assessment may be limited, having the resources and abilities to anticipate and remove challenges, knowing the state of defenses now and where they may be in the future, and knowing what challenges may surprise. Taking a prospective view assumes that challenges to system performance will occur, and actively seeks out the range and details of these threats." (Nemeth, 2008)

Resonance Analysis Method (Hollnagel, 2004) provides a basis for identifying assessable resilience characteristics: "buffering capacity, flexibility, margin, tolerance, and cross-scale interactions" (Woltjer, 2008) (Dekker, et al., 2008). An approach to assessing two key aspects of resilience – detection and adaptation – is presented in (Johansson , et al., 2008).

These assessment approaches are systems-oriented. However, resilience engineering considers the organization or enterprise as well; some metrics for enterprise resilience are recovery time, level of recovery, and level of vulnerability to disruptions (Erol, et al., 2010). A stress-strain state space analogy provides a way of visualizing – with notional assessments – an organization's or a system's resilience (Woods, et al.).

B.1.3 Resilience Engineering and Risk Management

Resilience engineering takes a different approach to risk than safety engineering: While safety engineering seeks to reduce risk to an acceptable level, "Resilience Engineering sees the 'things that go wrong' as the flip side of the 'things that go right,' and therefore assumes that they are a result of the same underlying processes. In consequence of that, 'things that go right' and 'things that go wrong' should be explained in basically the same way." (Hollnagel, 2010) Resilience management is thus viewed as a complement to risk management:

> "Evaluating and improving system resilience is an important partner to traditional risk management techniques. Risk management typically focuses on the probability and consequences of particular events occurring. One of the major challenges in risk management is how to deal with ontological uncertainties. Ontological uncertainties are essentially the "unknown unknowns"; the events that have not been thought of, and therefore are not assessed or managed. By approaching the problem from a different angle, resilience management provides one strategy for dealing with these events. Resilience management shifts the focus from "*what could make the lights go out?*" to "*it doesn't matter what makes the lights go out, how are we going to deal with it if they do?*"." (Dalziell, et al., 2005)

B.2 Network Resilience

Several international initiatives focus on network resilience, i.e., "the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation" (ENISA, 2011). Examples of challenges include malicious attacks from intelligent adversaries, as well as unintentional misconfigurations, large-scale disasters, hardware destruction, surges in network traffic, and failures of service providers. These initiatives include

- ResiliNets, the resilient and survivable networking initiative which "is investigating the architecture, protocols, and mechanisms to provide resilient, survivable, and disruption-tolerant networks, services, and applications" (Sterbenz, et al., 2006), (Sterbenz, et al., 2011).
- The Multiannual Thematic Program being executed by the European Network and Information Security Agency (ENISA) "with the ultimate objective to collectively evaluate and improve the resilience of public communications in Europe." (ENISA, 2005-2011), including
    - Inter-X, ENISA's short-term study of the resilience of the Internet interconnection ecosystem (ENISA, 2010).

    - Cyber Europe 2010, the cyber security exercise structured around several incidents compromising the resilience of the Internet (ENISA, 2011).
- ReSIST, the Network of Excellence (NoE) that was established under the European Commission's Sixth Framework Programme to bring together leading researchers active in the multidisciplinary domains of Dependability, Security, and Human Factors. (ReSIST, 2006-2009)
- DESEREC (DEpendability and Security by Enhanced REConfigurability), a past project under the Sixth Framework Programme seeking to integrate three approaches: modeling and simulation, detection, and response. (DESEREC, 2008)
- The AMBER (Assessing, Measuring, and Benchmarking Resilience) Consortium, an EU-sponsored Coordination Action.

In addition to work under these initiatives, other researchers are investigating network resilience and defining metrics, such as node-to-node resiliency (Omer, et al., 2010).

B.2.1 ResiliNets Conceptual Framework

The ResiliNets initiative decomposes resilience into two broad categories, Challenge Tolerance and Trustworthiness (Sterbenz, et al., 2010). Challenge Tolerance includes survivability, disruption tolerance, and traffic tolerance (or elasticity); Trustworthiness includes dependability, security, and performability. The ResiliNets strategy for implementing resilience includes a control loop (defend, detect, remediate, recover) enclosed by two overarching processes to diagnose and refine the effectiveness of the control processes. The ResiliNets framework, strategy, and evaluation approach are presented in (Sterbenz, et al., 2011).

B.2.2 ENISA Conceptual Framework and Resilience-Improving Techniques

ENISA analyzed the security and resilience features of three key technologies: IPv6, DNSSEC, and MPLS (ENISA, 2009). ENISA also analyzed standardization efforts and identified areas in which further activities are needed (ENISA, 2009), emphasizing resilience as a component of protection in the ITU-T and ETSI ontological model of cyber security (ETSI, 2008).

Most importantly for cyber resiliency, ENISA surveyed frameworks and metrics for resilient networks and services, and presents a two-dimensional approach to categorizing resilience metrics (ENISA, 2011). One dimension is incident-based, the other domain- or discipline-based. The incident-based dimension identifies three phases or time periods with respect to the incident (the single fault or challenge that threatens the normal level of service): preparation, service delivery (roughly, while successfully withstanding the fault or challenge), and recovery (when the level of service is no longer acceptable, and actions are taken to restore an acceptable level of service). The ENISA report does not specify a set of domains, but instead cites the framework provided by the ResiliNets initiative. While noting the challenge of composing and aggregating resilience metrics beyond the organization, the ENISA metrics report presents a variety of possible metrics and mentions a number of others.

One of the areas identified as a standardization gap was the lack of a consistent taxonomy for cyber security that identifies the role of resilience (ENISA, 2009). A draft report presents a proposed ontology (Vlacheas, et al., 2011). In that ontology, resilience is expressed by measurable properties: availability, reliability, safety, confidentiality, integrity, and maintainability. Resilience is enabled by trust management, supply chain integrity management,

fault management, cooperation, risk management, governance, security, and cognitive and self-management.

The ENISA Virtual Working Group on Network Providers' Resilience Measures defined challenges to network resilience and security in several areas: infrastructure, technology, operational processes and people, organizational continuity, commercial, and regulatory. The group identified threats "of concern when discussing resilience" and mapped those threats to the challenges. The group identified 68 actions that could be taken to improve resilience; of these, several are of specific interest to cyber resiliency engineering:

> "12: New technologies platforms are assessed for resilience features and compatibility"
>
> "15: Risk management used for critical components and processes"
>
> "16: End-point security practices – awareness raising"
>
> "17: End-point access shutdown or quarantine"
>
> "18: End-user notification of incidents"
>
> "19: End-user incentives for practising secure computing"
>
> "22: Detection and mitigation of cyber threats given a high priority and assigned specific resources"
>
> "29: Proactively structure operational responses to incidents requiring third party participation"
>
> "35: Extroversive attitude to addressing high magnitude incidents (cross-sector communication, coordination, and collaboration structures)"
>
> "36: EU-wide monitoring and early warning on external threats"
>
> "51: Generate a flexible operational framework for gathering data [specifically, security incidents, measures, threats, and risks] on resilience performance measures to enable a confidential benchmarking exercise to take place"
>
> Consideration of resilience and security throughout the life-cycle (55-61)
>
> "62: Tracking of exposures of technology platform and mitigation at EU level"

In a report (ENISA, 2011) which more closely considers the relationship between resilience and security, ENISA identified key principles for resilience assessment in organizations. These principles are relevant to cyber resiliency metrics, particularly operational metrics. Another report identifies emerging areas in which resilience challenges are anticipated:

- Cloud computing
- Real-time detection and diagnosis (particularly with respect to malicious attacks)
- Future wireless networks
- Sensor networks
- Integrity of supply chain

Under Inter-X, ENISA has also identified factors in the ICT ecosystem relevant for analyzing end-to-end network resilience ("mouth to ear for voice services; user to on-line service or user to user for data services; broadcaster to subscriber for broadcast services") (2011). The emphasis is on faults and failures; malicious actors are mentioned only briefly. The end-to-end resilience report discusses an asset-focused approach to risk management for resilience. More broadly, an

ENISA study looks at the resilience of the Internet interconnection ecosystem (Trimintzios, et al., 2011), taking into consideration cyber incidents as well as disasters and faults. The Inter-X study recommends research into resilience metrics and measurement frameworks, and identifies considerations[34] which strongly overlap with the cyber resilience practices discussed in Section 4.

B.2.3 ReSIST Conceptual Framework

The ReSIST initiative defined a model for scalable resilience (ReSIST, 2007) and a resilience ontology (ReSIST, 2008) consistent with the dependability and security ontology (Avizienis, et al., 2004) discussed below. The ReSIST initiative surveyed the state of knowledge in resilience-building technologies (ReSIST, 2006), and collected papers by researchers in the NoE from 2006-2009 (ReSIST, 2009). From the standpoint of cyber resiliency, relevant techniques in the survey include intrusion-tolerant architectures, Byzantine consensus, compositional modeling, evaluation with respect to malicious threats, dependability benchmarking with respect to intrusions, diversity, and verification of systems containing cryptography. The ReSIST initiative developed the concept of *resilience-explicit computing*, i.e., an approach "aims to support the achievement and prediction of system resilience by making explicit the resilience-related properties of components and infrastructure. These properties are described in terms of *metadata*, which can be used at design time to inform decisions about the choice of design patterns and development tools, or potentially at run-time to tune or reconfigure, maintaining resilience." (ReSIST, 2008). Mechanisms for resilience-explicit computing identified by the resilience-explicit computing reports (ReSIST, 2007), (ReSIST, 2008) can be mapped to the cyber resilience strategies identified in Section 4 below.

B.2.4 AMBER Research Roadmap and Survey

The AMBER project developed a research roadmap (AMBER, 2008) (AMBER, 2009) (Bondavalli, et al., 2010), supported by a state-of-the-art survey (van Moorsel, et al., 2009). The research roadmap identifies needs, challenges, and recommended actions in the areas of (i) scientific and technological foundations, (ii) measurement and assessment, (iii) benchmarking, and (iv) education, training, standardization, and take-up. The state-of-the-art report articulates challenges for metrics:

> "Concerns about improving measurement and quantitative prediction are often driven by the concrete difficulties in applying existing methods in new systems: just as increasing levels of circuit integration and miniaturisation made it infeasible to monitor circuit operation at a very detailed level via simple probes and oscilloscopes, so the deployment of services over large open networks and through dynamic composition may create new difficulties in measuring their dependability. More general problems may arise, however: do we need to choose appropriate new measures for characterising the qualities of real interest? If they are amenable to measurement in practice, to what extent will they support trustworthy predictions? To what extent may the benefit of "reasonably good" measures (perhaps acceptable proxies for the "truly important" ones) be offset by the reaction to their adoption: designers and organisations focusing on the false target of good values of these measures, perhaps to the detriment of the actual goal of dependability and resilience."

[34] These are (1) spare capacity – redundancy, (2) diversity, (3) independence, (4) separacy – physical separation, (5) [avoidance of] vulnerabilities and single points of failure, (6) best practice, (7) supplier management and selection, and (8) preparation – disaster planning.

B.3 System Resilience in Critical Infrastructures

System resilience is primarily investigated in the context of critical infrastructures. INCOSE (the International Council on Systems Engineering) has chartered a working group on resilience (INCOSE, 2010), which is part of the International Resilience Engineering Network (REN, 2011) and which is supporting TISP (The Infrastructure Security Partnership) in developing a regional resilience guide (TISP, 2011). In this context, resilience is oriented toward disasters (including man-made disasters, specifically cyber attacks and disruptions) and critical infrastructure systems. The identified needs and recommended actions for assuring regional cyber security and IT system resilience are largely process-oriented, with a technical focus on intrusion detection and protection (TISP, 2011).

One framework for discussing system resilience (Sheard, et al., 2003), based on an extensive literature survey, has five aspects: time periods, system types, events, resilience actions, and properties to preserve. Sandia's resilience assessment framework identifies qualitative system characteristics (absorptive, adaptive, and restorative capacity) and qualitative measurements (system performance, recovery duration, and recovery effort) (Sandia, 2009).

A construct for describing resilience practices presented in (NIAC, 2010) "consists of four outcome-focused abilities: (1) Robustness—the ability to absorb shocks and continue operating; (2) Resourcefulness—the ability to skillfully manage a crisis as it unfolds; (3) Rapid Recovery—the ability to get services back as quickly as possible; and (4) Adaptability—the ability to incorporate lessons learned from past events to improve resilience."

B.4 Dependable Computing and Fault Tolerance

The discipline of dependable computing is well-established; the IFIP Working Group on Dependable Computing and Fault Tolerance was established in 1980 and defines dependability as "the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers" (IFIP, 2011). As described in (Avizienis, et al., 2004), dependability encompasses availability, reliability, safety, integrity, and maintainability, while security encompasses availability, integrity, and confidentiality; a common set of engineering principles addresses both dependability and security:

- "Fault prevention means to prevent the occurrence or introduction of faults.
- Fault tolerance means to avoid service failures in the presence of faults.
- Fault removal means to reduce the number and severity of faults.
- Fault forecasting means to estimate the present number, the future incidence, and the likely consequences of faults."

An extensive taxonomy of faults is provided, including malicious faults[35], and the relationship between dependability, survivability, high confidence, and trustworthiness is discussed.

The relationship between resilience and dependability has increasingly been explored by the Dependable and Secure Computing community. For example, resilience has been defined as "the persistence of dependability when facing changes" (Laprie, 2008), with evolvability, assessability, usability, and diversity being the central properties of resilience.

[35] Similarly, the IEEE Technical Committee on Dependable Computing and Fault Tolerance considers both "accidental faults (physical, design-induced, or originating from human interaction) and intentional and/or malicious faults, as well, namely those affecting the security of systems" (IEEE , 2011).

B.4.1 Survivability

Survivability as a specific form of dependability has been defined for a variety of systems domains: IT, networks and telecommunications, and critical and defense systems. (Tarvainen, 2004) Survivable systems can be defined as "systems that are able to continue discharging their normal operation despite the presence of malicious or arbitrary faults … Survivable systems may need to be both fault-tolerant and secure, for example, detect a malicious fault, and remove the same from the system and attempt to secure the system" (Ghosh, et al., 2006)

Research in survivable systems *per se* was most active in the 1995-2005 timeframe, with results transitioned into some systems engineering curricula and into CERT's Survivability Analysis Framework (Ellison, et al., 2010) and the development of survivability engineering principles. Richards et al. (Richards, et al., 2008) (Richards, et al., 2009) identify 17 survivability design principles. These largely correspond to the cyber resilience strategies identified in (Goldman, 2010) and discussed in Section 4.1:

- "Type I: Reduce susceptibility
    - Prevention: suppression of a future or potential future disturbance
    - Mobility: relocation to avoid detection by an external change agent
    - Concealment: reduction of the visibility of a system from an external change agent
    - Deterrence: dissuasion of a rational external change agent from committing a disturbance
    - Preemption: suppression of an imminent disturbance
    - Avoidance: maneuverability away from disturbance
- Type II: Reduce vulnerability
    - Hardness: resistance of a system to deformation
    - Redundancy: duplication of critical system functions to increase reliability
    - Margin: allowance of extra capability for maintaining value delivery despite losses
    - Heterogeneity: variation in system elements to mitigate homogeneous disturbances
    - Distribution: separation of critical system elements to mitigate local disturbances
    - Failure mode reduction: elimination of system hazards through intrinsic design: substitution, simplification, decoupling, and reduction of hazardous materials
    - Fail-safe: prevention or delay of degradation via physics of incipient failure
    - Evolution: alteration of system elements to reduce disturbance effectiveness
    - Containment: isolation or minimization of the propagation of failure
- Type III: Enhance resilience
    - Replacement: substitution of system elements to improve value delivery
    - Repair: restoration of system to improve value delivery" (Richards, et al., 2008)

Strategies for survivability in the face of cyber threats include proactive fault-containment[36] (Meredith, 2003), for which several metrics can be defined:

- The length of the window of vulnerability – the length of the time period during which additional faults could lead to more problems;
- Fault-detection latency – the length of time between the fault and its detection;
- Recovery latency – the length of time between the detection of the fault and its remediation; and
- Reactive fault-detection latency – "The likelihood that fault detection involves neither false positives (i.e., detection of faults that do not exist) nor false negatives (i.e., failure to detect faults that do exist)." (Merideth, et al., 2003)

Survivability research continues for mobile ad-hoc networks (MANETs) (Lima, et al., 2009). In addition, survivability research in large-scale systems continues (SLSIS, 2011), with an increasing focus on software engineering for *self-adaptive systems*. Self-adaptive (or self-adapting) systems "decide autonomously (i.e., without or with minimal interference) how to adapt or organize to accommodate changes in their contexts and environments." ((Brun, et al., 2009) in (Cheng, et al., 2009)) Challenges – which are also relevant to resilience – include modeling, creating a library of control-loop types for self-adaptive systems, architecture and design principles, detection of unintended interactions, maintenance, middleware support, verification and validation (V&V), reengineering legacy systems, and human-computer interaction (HCI) (Brun, et al., 2009). Security issues and metrics for self-adaptive systems have been identified as research topics (ADAPTIVE, 2011). A recently initiated international initiative, Assuring Dependability in Architecture-based Adaptive Systems (ADAAS, 2011), has identified the need for research to extend the concept of dependability cases to address resilience (ADAAS, 2011).

A research roadmap for benchmarking the resilience of self-adaptive systems has been proposed (Almeida, et al., 2010). That roadmap provides a framework for characterizing resilience benchmarking metrics: such metrics can be characterized as

- Service-related metrics, e.g.,
    - Performance
    - Uptime or availability
    - Robustness
- Metrics related to self-adaptation, including
    - Time-related metrics to characterize self-adaptation, e.g.,
        - Time to react
        - Time to adapt
        - Time to stabilize
    - Sensitivity

[36] "Proactively survivable systems differ from reactively survivable systems in that proactive systems may act (i) to increase resistance, (ii) to initiate recovery, or (iii) to adapt: before or concurrently with the recognition of a problem in the system." (Merideth, et al., 2003) Proactive containment uses "knowledge of faults to notify potentially damaged areas of the system, in order to contain the tainted parts." (Merideth, et al., 2003)

- Degree of autonomy

Finally, the phrase "survivability in cyberspace" is used to characterize the confluence of survivability, attack tolerance, and security, and largely overlaps with cyber resiliency (WSC, 2010).

B.4.2 Self-Healing Systems

Within the fault-tolerance literature, self-healing systems are of particular interest from the standpoint of resilience. One framework for describing the self-healing system problem space, consists of (1) the fault model (or fault hypothesis) – the duration, severity, granularity, and profile of expectations for faults to be tolerated – explicitly allowing for consideration of malicious faults; (2) the system response – characterized in terms of detection, degradation, response, recovery, time constants, and assurance; (3) the system's completeness, the extent to which the system is known – architecturally, by designers, by the system itself, and as the system evolves; and (4) the design context – abstraction level, component homogeneity, behavioral predetermination, user involvement in healing, system linearity, and system scope. (Koopman, 2003)

A survey of research in self-healing systems (Ghosh, et al., 2006) identifies multiple strategies, categorizing them as follows:

- Maintain system health
  - Maintain redundancy
  - Probe to monitor health
  - Use an architectural model for system monitoring
  - Maintain diversity
  - Analyze performance logs
- Detect system failure
  - Detect something amiss (e.g., missing response, missing component)
  - Use a system monitoring model
  - Identify and provide notification of foreign elements
- Recover to a healthy state
  - Use redundancy techniques
  - Use architectural models and repair plans
  - Use Byzantine agreement and voting
  - Use other non-traditional models (e.g., Recovery-Oriented Computing)

A subsequent research survey (Psaier, et al., 2011) identifies common characteristics in approaches to self-healing being actively explored: separation of concerns, intrusive vs. non-intrusive self-healing techniques, closed vs. open techniques, detecting and reporting suspicious behavior, diagnosis and selection of recovery strategy, and recovery techniques involving redundancy. These redundancy techniques include: replacement, balancing, isolation, persistence, redirection, relocation, and diversity.

B.4.3 Intrusion-Tolerant Systems

Intrusion tolerance involves the use of techniques which also support resilience, including diversity and unpredictability (Ramasamy, et al., 2004).

B.5 Relationship of Cyber Resiliency Goals and Objectives to Other Frameworks

The cyber resiliency goals and objectives described in Section 4 are derived from the larger resilience literature. Relationships are indicated in Table 8.

Table 8. Cyber Resiliency Goals and Objectives in Relation to Other Frameworks

Cyber Resiliency Goal	Related Terms and Concepts
Anticipate	Avoid (Madni, 2007), Avoidance (DoD, 2011), Defend and Detect (Sterbenz, et al., 2010), Preparation (ENISA, 2011), Long-term prevention and Short-term avoidance (Sheard, et al., 2003), Anticipate (NIAC, 2010),Resist / Inhibit Basic State Change (HSSIA, 2010)
Withstand	Absorb (Madni, 2007), Remediate (Sterbenz, et al., 2010), Service Delivery (ENISA, 2011), Absorptive capacity (Sandia, 2009), Absorb (NIAC, 2010), Immediate-term coping, Cope with ongoing trouble (Sheard, et al., 2003), Absorb / Maintain Continuity of Function and Graceful Degradation (HSSIA, 2010), Robustness (DoD, 2011)
Recover	Restore (Madni, 2007), Reconstitution and Recovery (DoD, 2011), Recover (Sterbenz, et al., 2010), Recovery (ENISA, 2011), Restorative capacity (Sandia, 2009), Rapid Recovery (NIAC, 2010), Long term recovery (Sheard, et al., 2003), Recover (HSSIA, 2010)
Evolve	Adapt (Madni, 2007), Adaptive capacity (Sandia, 2009), Adapt (NIAC, 2010), Long-term recovery (reorganize if necessary) (Sheard, et al., 2003)
Cyber Resiliency Objective	
Understand	Probe to monitor health, Use an architectural model for system monitoring (Ghosh, et al., 2006)
Prepare	Preparation (Trimintzios, et al., 2011)
Prevent	Prevention, Deterrence, Preemption, Avoidance, Hardness (Richards, et al., 2009)
Constrain	Containment (Richards, et al., 2009), Proactive containment (Merideth, et al., 2003)
Continue	See Withstand, above.
Reconstitute	Repair (Richards, et al., 2009). See also Recover, above.
Transform	See Evolve, above.
Re-architect	Architectural trades for resilient mission-information exchanges to drive Mission Risk Management Approach, Refresh Cyber Response Capabilities (Belz, 2011) Replacement, Evolution (Richards, et al., 2009)

B.6 Relationship of Cyber Resiliency Practices to Other Frameworks

The cyber resiliency practices described in Section 4 are derived from previous MITRE work, together with the larger resiliency literature. Relationships are indicated in Table 9.

Table 9. Mapping of Practices in Cyber Resiliency Engineering Framework to Other Work

Practice in Cyber Resiliency Engineering Framework	Techniques and Practices Described in Other Frameworks	Relationship to Previously Published MITRE Work		
		Practices in (Goldman, 2010)	Practices in (Goldman, et al., 2011)	Rationale for Differences
Adaptive Response	Integration of sensing, detection, response, and recovery mechanisms (King, 2011) "Human-in-the-loop," graceful degradation, drift correction (Madni, et al., 2009) Pre-emption (Richards, et al., 2009) Privilege deprivation (Zhang, et al., 2005)	Adaptive Management & Response	Dynamic Reconfiguration, Dynamic Reconstitution, Dynamic Composition	Adaptive Response involves executing a Cyber Course of Action (CCoA), which can include reconfiguration, reconstitution, and/or composition (as well as using other techniques).
Analytic Monitoring	Develop measurement plan and associated instrumentation approach, Require Mission-based Cyber Situational Awareness (Belz, 2011) Shared situational awareness, trust modeling, and diagnosis (Shrobe, 2011) Proactive intrusion detection (ENISA, 2011) Inspectability (Madni, et al., 2009) Use a system monitoring model (Ghosh, et al., 2006) Principle 22 (Stoneburner, et al., 2004)	Detection / Monitoring	-	Differentiate from Detection & Monitoring as purely information security functions; emphasize need for analysis.
Coordinated Defense	Require Mission-based Cyber Course of Action Development (Belz, 2011) Vulnerabilities and single points of failure (Trimintzios, et al., 2011) Principle 16 (implement layered security) (Stoneburner, et al., 2004)	Adaptive Management & Response	Alternative Operations	Coordinated Defense includes the management aspect of Adaptive Management & Response, emphasizing the need to coordinate management activities to avoid conflicts and single points of failure. Coordinated Defense includes planning and execution of the CCoA for Alternative Operations.
Deception	Concealment (Richards, et al., 2008)	Deception	Deception	No difference.
Diversity	Manageable and taskable diversity (Shrobe, 2011) Diversity (ReSIST, 2006-2009), (Trimintzios, et al., 2011), (Ghosh, et al., 2006), (Psaier, et al., 2011) Heterogeneity (Richards, et al., 2008)	Diversity	Diversity & Randomness	Diversity is an approach in itself. It can be made more effective when combined with Unpredictability.

Practice in Cyber Resiliency Engineering Framework	Techniques and Practices Described in Other Frameworks	Relationship to Previously Published MITRE Work		
		Practices in (Goldman, 2010)	Practices in (Goldman, et al., 2011)	Rationale for Differences
Dynamic Positioning	Moving Target Defense (NITRD CSIA IWG, 2010) Mobility, Distribution (Richards, et al., 2009) Relocation, Redirection (Psaier, et al., 2011)	Distributedness & moving target defense	Moving target & distributedness	Brevity. "Distributedness" is not a well-defined term.
Dynamic Representation	Resiliency-specific modeling and simulation (King, 2011) Mission-Driven Analysis to determine mission-information dependencies (Belz, 2011) Intent awareness (Madni, et al., 2009) Compositional modeling (ReSIST, 2006-2009)	-	-	Additional approach to support Understand & Prepare objectives.
Non-Persistence	Concealment (Richards, et al., 2009)	Non-Persistence	Non-Persistence	No difference.
Privilege Restriction	Establish and Implement Access Control functions across system lifecycle (Belz, 2011) Least Privilege (Zhang, et al., 2005)	Least Privilege	-	Differentiate from (more narrow) information security technique; include criticality as a driver for privilege criteria.
Realignment	Reorganization, learning/awareness (Madni, et al., 2009)	-	-	Additional approach to support Evolve goal and Transform objective.
Redundancy	Functional redundancy, physical redundancy, human backup (Madni, et al., 2009) Redundancy (Ghosh, et al., 2006) Space capacity – redundancy (Trimintzios, et al., 2011) Redundancy, Margin (Richards, et al., 2009)	Redundancy	Redundancy, Alternative Operations	Alternative Operations makes use of Redundancy; the planning and execution of the CCoA for Alternative Operations is part of Coordinated Defense.

Practice in Cyber Resiliency Engineering Framework	Techniques and Practices Described in Other Frameworks	Relationship to Previously Published MITRE Work		
		Practices in (Goldman, 2010)	Practices in (Goldman, et al., 2011)	Rationale for Differences
Segmentation	Secure modularization and virtualization of nodes and networks (King, 2011) "Neutral" state (Madni, et al., 2009) Independence, Physical Separation (Trimintzios, et al., 2011) Separation of concerns, isolation (Psaier, et al., 2011) Principles 17, 19, 20, and 21 (Stoneburner, et al., 2004)	Isolation / Segmentation / Containment	Segmentation, Isolation, Containment	Containment is an objective. Isolation is typically a transient result of a CCoA enabled by Segmentation.
Substantiated Integrity	Byzantine consensus (ReSIST, 2006-2009), (Ghosh, et al., 2006)	Integrity	Data and System Integrity & Availability	Avoid confusion with Integrity and availability as information security objectives; allow for integrity substantiation of system components.
Unpredictability	Unpredictable communications (Ramasamy, et al., 2004)	Randomness & Unpredictability	Diversity & Randomness	Unpredictability can use Diversity and Randomness.

Appendix C: Acronyms

ADAAS	Assuring Dependability in Architecture-based Adaptive Systems
AFRL	Air Force Research Laboratory
AMBER	Assessing, Measuring, and Benchmarking Resilience
AS&W	Attack Sensing and Warning
ASD	Assistant Secretary of Defense
ATM	Air Traffic Management
C2	command and control
CoA (or COA)	course of action
CCoA	cyber course of action
CIANCNF	Committee on Information Assurance for Network-Centric Naval Forces, Naval Studies Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies
CIIA	Cyber, Identity and Information Assurance
CMMI	Capability Maturity Model Integration
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
CCoA	cyber course of action
CoA	course of action
CONOPS	concept of operations
CRASH	Clean-slate design of Resilient, Adaptive, Secure Hosts
CyberCARD	Cooperative Autonomous Resilient Defenses in Cyberspace
DARPA	Defense Advanced Research Projects Agency
DBMS	database management system
DCIP	Defense Critical Infrastructure Program
DESEREC	Dependability and Security by Advanced Reconfigurability

DHS	Department of Homeland Security
DIB	Defense Industrial Base
DoD	Department of Defense
EA	enterprise architecture
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
EUROCONTROL	European Organisation for the Safety of Air Navigation
FISMA	Federal Information Security Management Act
HCI	human-computer interaction
HSSIA	Homeland Security Studies and Analysis Institute
HSPI	Homeland Security Policy Institute (George Washington University)
I&W	indications and warnings
ICT	information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IFIP	International Federation for Information Processing
INCOSE	International Council on Systems Engineering
ISACA	Information Systems Audit and Control Association
ISSE	information systems security engineering
IT	information technology
ITGI	Information Technology Governance Institute
ITU	International Telecommunications Union
JCS	Joint Chiefs of Staff
LMCA	Lockheed Martin Cybersecurity Alliance
LOE	level of effort
MAE	Mission Assurance Engineering
MOE	Measure of Effectiveness
MOP	Measure of Performance
MPLS	multiprotocol label switching

MRC	Mission-oriented Resilient Clouds
NDIA	National Defense Industrial Association
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NITRD CSIA IWG	Networking and Information Technology Research and Development Interagency Working Group on Cyber Security and Information Assurance
NoE	Network of Excellence
NSC	National Security Council
OCS	(United Kingdom) Office of Cyber Security
OS	operating system
OSD(SP)	Office of the Secretary of Defense (Space Policy)
PACyR	Process for Assessing Cyber Resiliency
RAMBO	Resilient Architectures for Mission Assurance and Business Objectives
REN	Resilience Engineering Network
ReSIST	Resilience for Survivability in IST (information systems technology)
SEI	Software Engineering Institute at Carnegie-Mellon University
SEPO	(MITRE) Systems Engineering Program Office
SLA	service level agreement
SLSIS	Survivable Large-Scale Information Systems
TISP	The Infrastructure Security Partnership
TPM	Technical Performance Measure
TTPs	tactics, techniques, and procedures
V&V	verification and validation
WSC	Workshop on Survivability in Cyberspace