MTR140499R1

Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques

Deborah Bodeau
Richard Graubart
William Heinbockel
Ellen Laderman

May 2015

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

Approved for Public Release

Distribution Unlimited

PR 15-1334

©2015 The MITRE Corporation.
All rights reserved.

Bedford, MA

Abstract

Cyber resiliency is the ability of cyber systems and cyber-dependent missions to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats. This paper updates MITRE's Cyber Resiliency Engineering Framework and provides information that systems engineers and architects can use when deciding which cyber resiliency techniques to apply. Specifically, it identifies potential interactions (e.g., dependencies, synergies, conflicts) between techniques, depending on the implementation approach. It identifies potential effects that implementations of cyber resiliency techniques could have on adversary activities throughout different stages in the cyber attack lifecycle. It also includes provisional information on relative maturity and ease of adoption for representative approaches to implementing cyber resiliency techniques.

Table of Contents

1 Introduction: Cyber Resiliency 7
1.1 Cyber Resiliency Foundations 7
1.2 Using This Document 9
2 The Cyber Resiliency Engineering Framework (CREF) 10
2.1 Cyber Resiliency Techniques 11
2.1.1 Definitions 12
2.1.2 Representative Approaches 15
2.2 What about …? Frequently Asked Questions 17
2.2.1 What about Moving Target? 17
2.2.2 Why Isn't Virtualization a Technique? 17
2.2.3 How Do Cyber Resiliency Techniques Differ from Conventional Security? 17
3 Selecting Cyber Resiliency Techniques and Approaches 19
3.1 Consider Relative Maturity and Readiness for Adoption 19
3.2 Take Potential Interactions into Consideration 20
3.3 Seek Effects Throughout the Cyber Attack Lifecycle 21
4 References 24
5 Acronyms 26
Appendix A Details on Cyber Resiliency Techniques 28
Appendix B Supporting Definitions and Summaries 57
B.1 Maturity and Ease of Adoption 57
B.2 Potential Interactions 60
B.3 Effects on Adversary Activities 61

List of Figures

Figure 1. Foundations of Cyber Resiliency 8
Figure 2. Future Vision: Cyber Resiliency as Part of Cybersecurity..... 9
Figure 3. Cyber Resiliency Engineering Framework 10
Figure 4. Relative Maturity and Ease of Adoption for Approaches to Implementing Cyber Resiliency Techniques 20
Figure 5. Cyber Attack Lifecycle..... 21

List of Tables

Table 1. Cyber Resiliency Goals 10
Table 2. Cyber Resiliency Objectives 11
Table 3. Cyber Resiliency Techniques 13
Table 4. Cyber Resiliency Techniques Support Cyber Resiliency Objectives 15
Table 5. Representative Approaches to Implementing Cyber Resiliency Techniques 16
Table 6. Potential Effects of Cyber Resiliency Techniques on Adversary Activities Across the Cyber Attack Lifecycle 22
Table 7. Adaptive Response 29
Table 8. Analytic Monitoring 31
Table 9. Coordinated Defense 33
Table 10. Deception 34
Table 11. Diversity 36
Table 12. Dynamic Positioning 40
Table 13. Dynamic Representation 42
Table 14. Non-Persistence 44
Table 15. Privilege Restriction 46
Table 16. Realignment 48
Table 17. Redundancy 50
Table 18. Segmentation / Isolation 51
Table 19. Substantiated Integrity 53
Table 20. Unpredictability 55
Table 21. Levels of Maturity 57
Table 22. Relative Readiness for Adoption for Cyber Resiliency 59
Table 23. Potential Interactions Between Cyber Resiliency Techniques 60
Table 24. Stages of the Cyber Attack Lifecycle 61
Table 25. Potential Effects on Cyber Adversary Activities 61

1 Introduction: Cyber Resiliency

Cyber resiliency – the ability of cyber systems and cyber-dependent missions to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats[1] – is emerging as a key component in any effective strategy for mission assurance or operational resilience.

This white paper updates MITRE's Cyber Resiliency Engineering Framework (CREF) and provides information that systems engineers and architects can use when deciding which cyber resiliency techniques to apply. Specifically, it identifies potential interactions (e.g., dependencies, synergies, conflicts) between techniques, depending on the implementation approach. It also identifies potential effects that implementations of cyber resiliency techniques could have on adversary activities throughout different stages in the cyber attack lifecycle.[2] Finally, it includes provisional[3] information about the relative maturity and the relative ease of adoption of representative approaches to implementing cyber resiliency techniques.

1.1 Cyber Resiliency Foundations

As illustrated in Figure 1 below, cyber resiliency builds on a foundation of conventional security, cybersecurity, and continuity of operations (COOP). However, cyber resiliency is based on a different assumption: a stealthy, persistent, and sophisticated adversary, who may have already compromised system components and established a foothold within an organization's systems. As organizations become more threat-aware, cyber resiliency can be expected to be integrated with (and no longer differentiated from) these disciplines.

Conventional security[4] focuses on achieving the security objectives of confidentiality, integrity, availability, and accountability to acceptable levels, by using a combination of perimeter protections and internal controls. COOP (as well as related engineering disciplines such as survivability) assumes an easily recognized adverse event or set of adverse conditions. The term "cybersecurity" is often used without definition, and with the relationship between cybersecurity and conventional security poorly

[1] This definition, while it indicates the scope of cyber resiliency, relies on the terms "resilience" and "cyber." For purposes of the CREF, resilience is defined as "the extent to which a nation, organization, or mission is able to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks, accidents, or naturally occurring threats or incidents." This definition of resilience is aligned with Resilience Engineering [24] and Operational Resilience [23], but is consistent with the ResiliNets definition ("Resilience is 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.") [22]. Cyber refers to "actual or potential accessibility via network communications" – that is, to participation in cyberspace, "the notional environment in which communication over computer networks occurs" [25].

[2] This paper excerpts and updates material from Cyber Resiliency Engineering Framework (CREF) [1], Cyber Resiliency Assessment: Enabling Architectural Improvement [2], Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain [3], Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment [21], and an earlier version of the Cyber Resiliency Engineering Aid which this paper supersedes. These documents, as well as numerous other resources on cyber resiliency, can be found at www.mitre.org.

[3] The assessment of relative maturity is with respect to general-purpose systems and generally accepted standards of good practice. Similarly, the assessment of relative ease of adoption is for organizations that have an established information security program or cyber security program. Assessments will change over time, as new technologies and practices are adopted, and as standards of good practice evolve.

[4] Conventional security is the primary focus of FIPS 199 and the baselines defined.in NIST SP 800-53R4 and CNSS 1253. The series of publications by the Joint Transformation Initiative (JTI) – including NIST SP 800-39, NIST SP 800-53R4, and NIST SP 800-30R1 – include consideration of advanced cyber threats and cyber resiliency [20], but organizations using those publications can restrict themselves to conventional security.

© 2015 The MITRE Corporation. All Rights Reserved.

articulated. When "cybersecurity" is defined[5], the definitions focus on protecting, detecting, and responding to attacks.

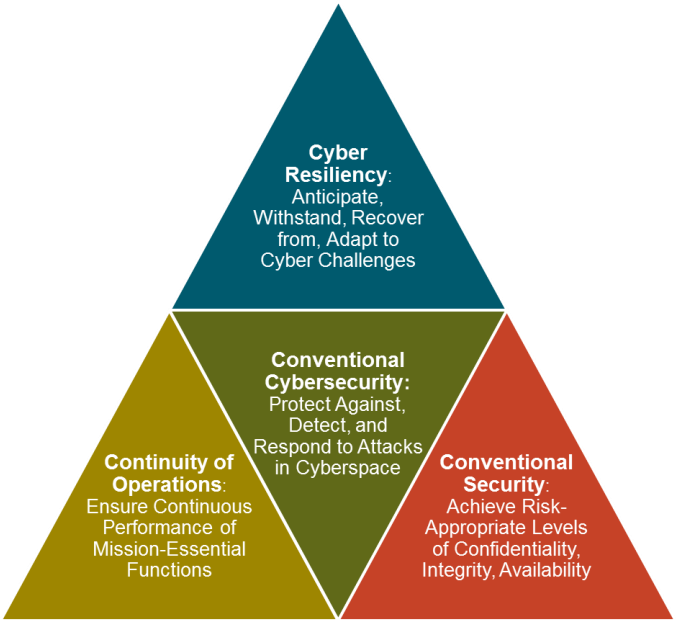

Figure 1. Foundations of Cyber Resiliency

Cyber resiliency assumes that good COOP, conventional security, and cybersecurity practices are already in place, but have limited effectiveness against ongoing – and largely stealthy – campaigns by sophisticated adversaries. In fact, sophisticated adversaries can sometimes exploit conventional practices to cause additional harm to the operational environment. Such adversaries can take advantage of (or make their behavior appear to result from) other forms of adversity, including human error, structural failure, or natural disaster. Cyber resiliency assumes that an advanced adversary will be able to establish a presence on an enterprise's systems or networks. (See the discussion of the cyber attack lifecycle later in this paper.) Such an adversary is positioned to deny or degrade functions; to destroy, modify, or fabricate data; to exfiltrate sensitive information; or to usurp or compromise services. Cyber resiliency focuses on the question: *Given this adversary advantage, how can cyber-dependent missions and business functions be adequately assured?*

It must be emphasized that Figure 1 illustrates *current* relationships among security- and dependability-related disciplines based on different risk frames.[6] As the need to address advanced cyber threats

[5] For example, CNSSI 4009 [5] / NISTIR 7298R2 defines cybersecurity as "The ability to protect or defend the use of cyberspace from cyber attacks" while the NIST Cybersecurity Framework (NCF) defines it as "The process of protecting information by preventing, detecting, and responding to attacks." [26]

[6] As discussed in NIST SP 800-39 [30], an organization's "risk frame" identifies "(i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses)."

© 2015 The MITRE Corporation. All Rights Reserved.

becomes part of the conventional wisdom, these currently-distinct disciplines will be integrated into aspects of a more mature cybersecurity. This is illustrated in Figure 2.

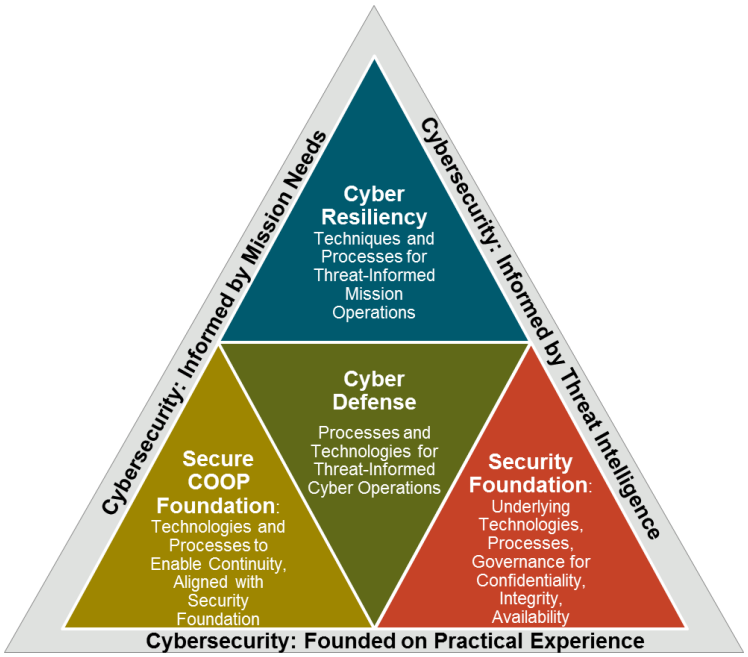

Figure 2. Future Vision: Cyber Resiliency as Part of Cybersecurity

1.2 Using This Document

The reader can use Section 2 become familiar with the Cyber Resiliency Engineering Framework (CREF). Readers already familiar with the CREF may want to consult the tables in Section 2 to ensure that they are using the current definitions of goals, objectives, and techniques. Section 3 presents three principles that systems security engineers and architects can apply when selecting or making tradeoffs among different approaches to implementing cyber resiliency techniques.

Two appendices provide the supporting details needed by systems security engineers and architects to apply those principles. Appendix A provide a set of reference tables on representative approaches to implementing cyber resiliency techniques. Appendix B provides definitions of terms used in Appendix A and in summary materials in Section 3.

© 2015 The MITRE Corporation. All Rights Reserved.

2 The Cyber Resiliency Engineering Framework (CREF)

The Cyber Resiliency Engineering Framework (CREF) illustrated in Figure 3 below organizes the cyber resiliency domain into a set of goals, objectives, and techniques.

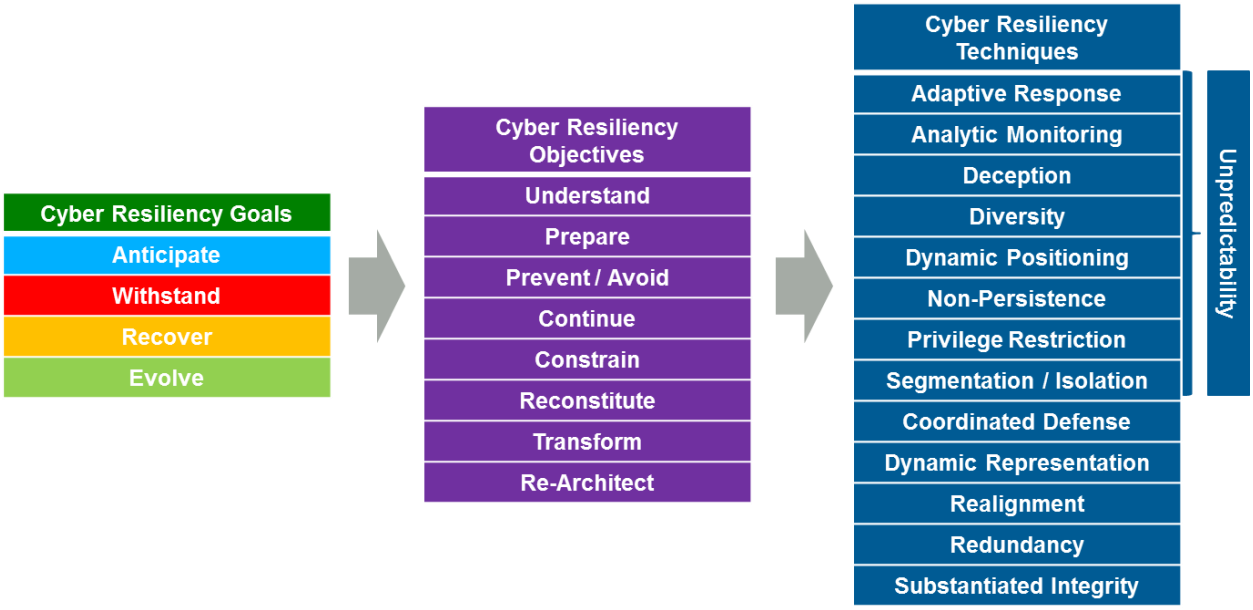

Figure 3. Cyber Resiliency Engineering Framework

Goals are high-level statements of intended outcomes, which help scope the cyber resiliency domain. As noted above, "adversity" as used in the cyber resiliency goals, defined in Table 1, specifically includes stealthy, persistent, and sophisticated adversaries, who may have already compromised system components and established a foothold within an organization's systems.

Table 1. Cyber Resiliency Goals

Goal	Description
Anticipate	Maintain a state of informed preparedness for adversity
Withstand	Continue essential mission/business functions despite adversity
Recover	Restore mission/business functions during and after adversity
Evolve	Adapt mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments

Objectives, defined in Table 2, are more specific statements of intended outcomes that serve as a bridge between techniques and goals. Objectives are expressed so as to facilitate assessment, making it straightforward to develop questions of "how well," "how quickly," or "with what degree of confidence or trust" can each objective be achieved. Objectives enable different stakeholders to assert their different resiliency priorities based on mission or business functions.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 2. Cyber Resiliency Objectives

Objective	Description	Goals Supported
Understand	Maintain useful representations of mission dependencies and the status of resources with respect to possible adversity	
Prepare	Maintain a set of realistic courses of action that address predicted or anticipated adversity	
Prevent / Avoid	Preclude the successful execution of an attack or the realization of adverse conditions	
Continue	Maximize the duration and viability of essential mission/business functions during adversity	
Constrain	Limit damage from adversity	
Reconstitute	Restore as much mission/business functionality as possible subsequent to adversity	
Transform	Modify mission / business functions and supporting processes to handle adversity more effectively	
Re-architect	Modify architectures to handle adversity more effectively	

The CREF looks at *architectural* approaches to achieving or improving resilience in the face of *cyber* threats. Therefore, objectives and techniques that relate to organizational resilience or business continuity in the face of non-cyber threats (e.g., natural disaster, human error) are not included.[7] As discussed earlier, the CREF assumes a good foundation of conventional security, cybersecurity, and COOP policies, procedures, technologies, and practices.

Cyber resiliency *techniques* are ways to achieve one or more cyber resiliency objectives. The CREF assumes that techniques will be *selectively* applied to the architecture or design of mission/business functions and their supporting cyber resources. Since natural synergies and conflicts arise between various cyber resiliency techniques, engineering trade-offs must be made. Section 3 and Appendix A of this paper provide information to support engineering analysis.

2.1 Cyber Resiliency Techniques

Cyber resiliency techniques characterize approaches to achieving one or more cyber resiliency objectives that can be applied to the architecture or design of mission/business functions and the cyber resources that support them. Each technique refers to a set of related approaches and technologies; these are presented in more detail in the Appendix. As stated in earlier CREF documents [1] [2] [3], the expectation is that the set of cyber resiliency techniques will change over time, as research in some of them fails to prove out, as others become standard conventional security, cybersecurity, or COOP practice, and as new research ideas emerge. Therefore, this paper presents updated descriptions of cyber resiliency techniques. In addition, the relationship between Unpredictability and other techniques

[7] See the CERT Resilience Management Model [23].

© 2015 The MITRE Corporation. All Rights Reserved.

is clarified: As illustrated in Figure 3, Unpredictability can be used together with some – but not all – of the other techniques to improve their effectiveness.

2.1.1 Definitions

The descriptions of techniques (and representative approaches, as described in Appendix A) rely on the following terms:

- Adverse cyber event. An event involving cyber resources that has adverse consequences for cyber resources. Adverse cyber events include, but are not limited to, cyber attacks.
- Attack surface. The set of resources and vulnerabilities that are exposed to potential attack.
- Component. A part of a system that can be replaced or managed separately from other parts of the system. Examples of components include hardware devices, embedded devices (e.g., sensors, controllers, medical devices such as pacemakers, vehicle automation such as collision avoidance), desktop or laptop computers, servers, routers, firewalls, virtual machine monitors (VMMs) or hypervisors, operating systems (OSs), applications, and databases. When "system" is construed as a socio-technical system, examples also include people and separately managed processes.
- Cyber. A modifier that indicates a presence in, or involvement with, cyberspace, due to actual or potential accessibility via network communications.
- Defensive Cyber Course of Action (CCoA). A set of activities or tactics, techniques, and procedures (TTPs) employed by automation, 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 in response to adverse cyber events.[8]
- Dynamic. Occurring (or capable of occurring) without interrupting or suspending operations.
- Mission / business function. An activity, process, or set of related activities or processes intended to achieve a mission or business objective.
- Nimble. Able to change direction quickly and easily. (A synonym for agile, which avoids the connotation of agile software development.)
- Process. A structured set of activities within an organization. Note that this usage does not refer to a computing process, i.e., to a running instance of a program. A process can be supported by tools.
- Resource. A component of, or a service or capability provided by, a system, which can be used by multiple mission / business functions. General examples include bandwidth, processing, and storage. Other examples are more system- or mission/business process-specific, and can include

[8] An organization sometimes documents its cyber courses of action in a "cyber playbook." The definition presented here is for cyber defense. Attackers also have TTPs and can define offensive CCoAs.

© 2015 The MITRE Corporation. All Rights Reserved.

information resources (e.g., data of a specified quality) as well as computing or networking services subject to service-level agreements (SLAs).

- System. A set of interacting or interdependent parts forming an integrated whole [4]; any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions [5]. This definition is recursive; it includes a system-of-systems, i.e., "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities" [6]. The term "system" typically includes people and organizational processes as well as technology; among those who use the term more restrictively, to include only technology, the term "socio-technical system" is used to refer to the combination of technology, people, and processes.
- Tactics, Techniques, and Procedures (TTPs). The use of capabilities and resources in relation to each other (tactics); non-prescriptive ways or methods used to perform missions, functions, or tasks (techniques); and standard, detailed steps that prescribe how to perform specific tasks (procedures) ([7], adapted).
- Tool. A technology or type of technology that can be used to perform some function (e.g., implement an approach or technique). While specific products could be identified as examples of tools, such identification can quickly be outdated; therefore, the following table identifies classes of products.

In addition, the effectiveness of many of the techniques can be enhanced by using virtualization and/or modularity / layering. These are defined as follows:

- Modularity / layering. Define and implement services and capabilities in a modular way, and in a way that respects the differences between layers in a layered architecture, to enable separation, substitution, and privilege restriction based on criticality.
- Virtualization. Create and manage an instance of a component or system that is separable from the physical resources it uses. Virtualization typically creates an operating environment (i.e., an operating system together with applications and storage), a computer platform (i.e., an operating environment together with underlying hardware devices), storage device (e.g., a virtual disk implemented via a flat file), or a network (i.e., a set of network resources, including routers and firewalls).

The cyber resiliency techniques defined in Table 3 are interdependent (for example, Analytic Monitoring supports Dynamic Representation); see Section 3.1 and Appendix A for more information.

Table 3. Cyber Resiliency Techniques

Cyber Resiliency Technique	Rationale
Adaptive Response: Implement nimble cyber courses of action (CCoAs) to manage risks	Optimize the organization's ability to respond in a timely and appropriate manner to adversary activities, thus maximizing the ability to maintain mission operations, limit consequences, and avoid destabilization.

© 2015 The MITRE Corporation. All Rights Reserved.

Cyber Resiliency Technique	Rationale
Analytic Monitoring: Gather, fuse, and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities, and damage	Maximize the organization's ability to detect potential adverse conditions, reveal the extent of adversary activity, and identify potential or actual damage. Provide data needed for cyber situational awareness (SA).
Coordinated Defense: Manage multiple, distinct mechanisms in a non-disruptive or complementary way	Require the adversary to defeat multiple safeguards, thereby making it more difficult for the adversary to successfully attack critical resources, increasing the cost to the adversary, and raising the likelihood of adversary detection. Ensure that uses of any given defensive mechanism do not create adverse unintended consequences by interfering with other defensive mechanisms.
Deception: Mislead, confuse, or hide critical assets from, the adversary	Mislead or confuse the adversary, or hide critical assets from the adversary, making them uncertain how to proceed, delaying the effect of their attack, increasing the risk to them of being discovered, causing them to misdirect or waste their attack, and expose their tradecraft prematurely.
Diversity: Use heterogeneity[9] to minimize common mode failures, particularly attacks exploiting common vulnerabilities	Cause the adversary to work harder by developing malware or other TTPs appropriate for multiple targets, increase the chance that the adversary will waste or expose TTPs by applying them to targets for which they are inappropriate, and maximize the chance that some of the defending organization's system's will survive the adversary's attack.
Dynamic Positioning: Distribute and dynamically relocate functionality or assets	Impede an adversary's ability to locate, eliminate or corrupt mission/business assets, and cause the adversary to spend more time and effort to find the organization's critical assets, thereby increasing the chance of the adversary revealing their actions and tradecraft prematurely.
Dynamic Representation: Construct and maintain current representations of mission posture in light of cyber events and cyber courses of action	Support situation awareness, enhance understanding dependencies among cyber and non-cyber resources, reveal patterns / trends in adversary behavior; and validate the realism of courses of action.
Non-Persistence: Generate and retain resources as needed or for a limited time	Reduce exposure to corruption, modification or corruption; provide a means of curtailing an adversary's advance and potentially expunging an adversary's foothold from in the system.
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	Impede the adversary by requiring them invest more time and effort in obtaining credentials; curtail the adversary's ability to take full advantage of credentials that they have obtained.
Realignment: Align cyber resources with core aspects of mission/business functions	Reduce the attack surface of the defending organization by minimizing the chance that non-mission / business functions could be used as an attack vector.

[9] As indicated in Appendix A, numerous forms of heterogeneity are possible.

© 2015 The MITRE Corporation. All Rights Reserved.

Cyber Resiliency Technique	Rationale
Redundancy: Provide multiple protected instances of critical resources	Reduce the consequences of loss of information or services; facilitate recovery from the effects of an adverse cyber event; limit the time during which critical services are denied or limited.
Segmentation / Isolation: Define and separate (logically or physically) components on the basis of criticality and trustworthiness	Contain adversary activities to the enclave/segment in which they have established a presence, thereby limiting the number of possible targets to which malware can easily be propagated.
Substantiated Integrity: Ascertain whether critical services, information stores, information streams, and components have been corrupted	Detect attempts by the adversary to deliver compromised data, software, or hardware, as well as successful modification or fabrication; provide limited capabilities for repair.
Unpredictability: Make changes randomly or unpredictably	Increase the adversary's uncertainty regarding the cyber defenses that they may encounter, thus making it more difficult for them to ascertain the appropriate course of action.

Each cyber resiliency technique supports one or more cyber resiliency objectives, as Table 4 illustrates.

Table 4. Cyber Resiliency Techniques Support Cyber Resiliency 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 / Isolation			X	X				
Substantiated Integrity	X			X	X	X		
Unpredictability	X		X		X			

2.1.2 Representative Approaches

For systems engineering to incorporate cyber resiliency, engineers need to understand what technologies and processes are available to them, and how readily those technologies and processes can be applied to meeting cyber resiliency goals and objectives. To this end, a set of representative approaches to implementing cyber resiliency techniques has been identified; these are listed in Table

© 2015 The MITRE Corporation. All Rights Reserved.

5.[10] With few exceptions, these approaches build on technologies and processes originally defined for cyber security, and to a lesser extent for conventional security, COOP, or performance management and dependability.

Table 5. Representative Approaches to Implementing Cyber Resiliency Techniques

Cyber Resiliency Technique	Representative Approaches	
AR: Adaptive Response	Dynamic Reconfiguration Dynamic Resource Allocation Adaptive Management	
AM: Analytic Monitoring	Monitoring & Damage Assessment Sensor Fusion & Analysis Malware & Forensic Analysis	
CD: Coordinated Defense	Technical Defense-in-Depth Coordination & Consistency Analysis	
DC: Deception	Obfuscation Dissimulation / Disinformation Misdirection / Simulation	
DV: Diversity	Architectural Diversity / Heterogeneity Design Diversity / Heterogeneity Synthetic Diversity	Information Diversity Command, Control, and Communications Path Diversity Supply Chain Diversity
DP: Dynamic Positioning	Functional Relocation of Sensors Functional Relocation of Cyber Assets	Asset Mobility Distributed Functionality
DR: Dynamic Representation	Dynamic Mapping & Profiling Dynamic Threat Modeling Mission Dependency & Status Visualization	
NP: Non-Persistence	Non-Persistent Information Non-Persistent Services Non-Persistent Connectivity	
PR: Privilege Restriction	Privilege Management Privilege-Based Usage Restriction Dynamic Privileges	
RA: Realignment	Purposing Offloading / Outsourcing	Restriction Replacement
RD: Redundancy	Protected Backup & Restore Surplus Capacity Replication	
SG: Segmentation / Isolation	Predefined Segmentation Dynamic Segmentation / Isolation	
SI: Substantiated Integrity	Integrity / Quality Checks Provenance Tracking Behavior Validation	
UN: Unpredictability	Temporal Unpredictability Contextual Unpredictability	

[10] The two-letter codes for the cyber resiliency techniques are used in Figure 5 in Section 3.The descriptions of the approaches are given in Appendix A.

© 2015 The MITRE Corporation. All Rights Reserved.

2.2 What about …? Frequently Asked Questions

This section provides responses to several frequently asked questions about the CREF.

2.2.1 What about Moving Target?

The phrase "moving target defense (MTD)" is often used to describe ways of changing the attack surface to make the adversary's job harder. That phrase encompasses multiple approaches, which are achieved in different ways. First, some moving target defenses actually move the target; in the CREF, these fall under Dynamic Positioning. Second, many moving target defenses involve changing configurations or swapping out components; these fall under Adaptive Response. Third, some moving target defenses involve diversification [8]; these fall under Diversity. While the CREF provides one way to structure discussion of the cyber resiliency space, others are equally viable. The CREF, by separating goals and objectives from techniques, reflects the assumption that the set of cyber resiliency techniques will change over time, as research in some of them fails to prove out, as others become standard cybersecurity or COOP practice, and as new research ideas emerge.

2.2.2 Why Isn't Virtualization a Technique?

Virtualization refers to a largely mature and commonly used set of technologies used to create (and subsequently destroy) virtual platforms, operating system (OS) environments, or networks, which present themselves as separate to higher architectural layers while sharing resources at lower layers. Many of the approaches to implementing cyber resiliency techniques depend on or use virtualization technology. These include Adaptive Response, Deception, Dynamic Positioning, Realignment, and Segmentation / Isolation. However, virtualization *per se* is not intended to provide resilience against advanced cyber threats; separation is motivated by accountability (so that resource use can be charged) and limitation of the effects of errors.

2.2.3 How Do Cyber Resiliency Techniques Differ from Conventional Security?

The question of how cyber resiliency relates to or differs from conventional or cyber security was addressed briefly in Section 1.1, but merits further discussion. Cyber resiliency is an additional component of the broader discipline of cyber security, and builds on that discipline (which in turn builds on conventional security). However, conventional security (sometimes referred to as good cyber security hygiene) has focused primarily on keeping an adversary out of a system, and cyber security has focused on the triad of "Protect, Detect, React" with the assumption that reacting can expunge an adversary's presence. Cyber resiliency assumes that an advanced adversary will be able to establish a presence on an enterprise's systems or networks, and frequently will be able to maintain that presence despite defender actions. Cyber resiliency therefore focuses on taking appropriate actions to ensure that the organization's mission can continue despite compromise of some aspects of the system by the adversary. As cyber resiliency techniques mature and are more widely adopted, the disciplines of cyber resiliency, cyber security, and conventional security will merge. In the meantime, there is overlap between some of the cyber resiliency techniques and some approaches used in conventional security or cyber security.

© 2015 The MITRE Corporation. All Rights Reserved.

1. The technologies used in support of resiliency techniques such as Redundancy and Privilege Restriction are largely those used for cyber hygiene. However, the processes for using those technologies take the APT into consideration.
2. Many of the technologies that support Analytic Monitoring, Coordinated Defense, and Segmentation, can be traced back to conventional security or cyber security, but they need to be implemented in a different manner, location, or with some different emphasis to support cyber resiliency. For example, firewalls and routers are conventionally used to segment the DMZ from an organization's internal infrastructure. Those same mechanisms can be used to provide segmentation in the organization's internal network, isolating some sensitive areas from others. In addition, conventional segmentation mechanisms may be modified in some way to enhance their ability to respond more dynamically to compromises of the organization's more sensitive components.
3. Some of the other resiliency techniques (Substantiated Integrity, Diversity, Dynamic Representation, Non-Persistence, and Realignment) are derived from other engineering disciplines that deal with non-adversarial concerns and threats, but require modifications or extensions to established approaches to address the APT. Dynamic Representation, for example, draws upon visualization methods to provide mission and business leaders with insight into the status of the mission-essential functions, in light of adversary activities and the organization's defenses. Substantiated Integrity draws upon established safety concepts such as polling of inputs from diverse critical services (e.g., Byzantine quorum systems) to determine correct results in case of conflicts between the services.
4. Finally, some cyber resiliency techniques borrow from disciplines (e.g., military, counter intelligence) that deal with a more active threats, but apply a cyber perspective. For example, the concept of feeding an adversary false information or concealing sensors (playing the role of scouts) are well-established deception techniques employed by the military and intelligence services. Cyber resiliency takes these concepts and adopts them in a cyber setting (e.g., honey nets, detonation chambers).

From (1)-(4) above, a progression from traditional cyber hygiene to full-blown cyber resiliency can be seen. This progression is not about the ease, difficulty, or complexity of the different technologies or techniques. It may be as hard (or harder) to implement some of the measures listed in (1) as those in (4). But the intent and benefit of these measures is likely to be very different. Broadly speaking the techniques in (1)-(3) are largely focused on impeding, detecting, containing, curtailing, and recovering from the actions of an adversary. Those techniques in (4) (and to some extent (3)), while able to have many of the same effects are also able to redirect, preclude, and (in some instances) expunge the adversary. Another way to view it is that techniques and mitigations in (1)-(3) are largely concerned with traditional actions such as Protect, Detect, Identify and React. Measures in (4) (and part of (3)) are more focused on disrupting the attack surface.

© 2015 The MITRE Corporation. All Rights Reserved.

3 Selecting Cyber Resiliency Techniques and Approaches

It is neither desirable nor feasible to apply all cyber resiliency techniques to an architecture. Resources are limited. The need for interoperability with legacy components, systems, and applications can constrain the solutions (products, services, architectural decisions, procedural or environmental controls) that can be applied to a given cyber security or resiliency problem. Implementations of some techniques can make implementations of others more difficult.

Therefore, systems security engineers and architects need to select cyber resiliency techniques, and specific approaches to implementing those techniques, with care. Three principles can guide that selection:

- Consider the relative maturity and readiness for cyber resiliency application of different implementation approaches. Leverage existing capabilities, developed for other purposes (e.g., performance, stability, security). Use approaches to implementing cyber resiliency techniques that apply established technologies.
- Consider potential interactions among techniques. Take advantage of synergies among techniques and implementation approaches. Avoid potential conflicts among techniques and approaches.
- Take the Advanced Persistent Threat into consideration. Apply techniques to affect adversary activities throughout the cyber attack lifecycle, rather than concentrating on a single stage. Apply techniques to achieve a variety of effects on adversary activities, rather than concentrating on one or two effects (e.g., negate, detect).

3.1 Consider Relative Maturity and Readiness for Adoption

As illustrated in Figure 4, each approach to applying a cyber resiliency technique can be situated with respect to (1) its general relative maturity, recognizing that technologies and processes have been developed to meet general needs for performance, dependability, or security, and (2) its relative readiness for adoption to cyber resiliency. For cyber resiliency, the context of is that of threat-informed engineering and operations: How easily can the technique or approach be applied to achieve cyber resiliency goals and objectives *in the face of advanced cyber threats*? Approaches that are highly challenging to adopt, and thus are topics for research rather than engineering, are not shown.

For each approach, Appendix A includes a description, an assessment of its maturity – that is, of how easily the approach can be integrated into a system or a mission architecture – as well as of how readily the approach can be adopted for cyber resiliency. Appendix B provides definitions of the levels of relative maturity and ease of adoption for cyber resiliency.

© 2015 The MITRE Corporation. All Rights Reserved.

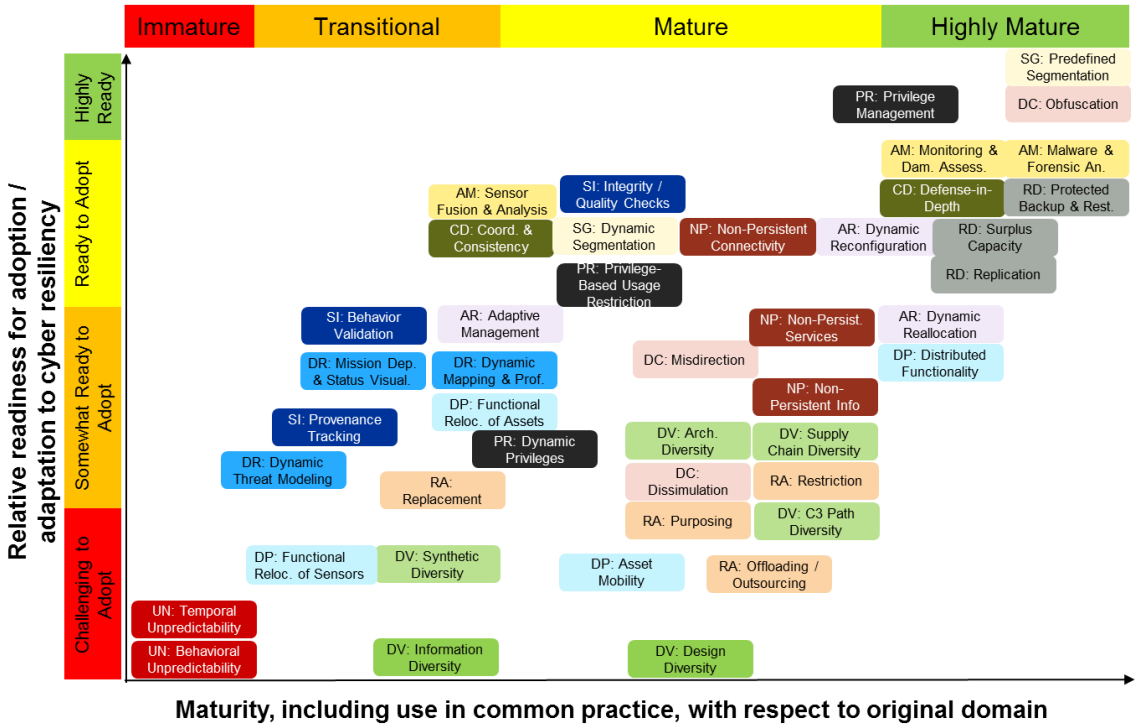

Figure 4. Relative Maturity and Ease of Adoption for Approaches to Implementing Cyber Resiliency Techniques

Note that the assessments are in the context of general-purpose enterprise computing (i.e., common uses of information and communications technology or ICT); different results can be expected for other contexts, such as cyber-physical systems (CPS). In addition, it must be emphasized that these are generalizations: the product landscape continues to change; operational practices vary widely depending on sector; and trends toward converged architectures, cloud computing, and the Internet of Things introduce new challenges that affect the usefulness of existing solutions and constrain the feasibility of emerging ones. Finally, it must be emphasized that the 44 approaches described in Appendix A are representative, rather than exhaustive, of the cyber resiliency techniques. Many aspects of cyber resiliency are active areas of research; these are not covered in this Engineering Aid.[11]

3.2 Take Potential Interactions into Consideration

The fourteen cyber resiliency techniques identified in the Cyber Resiliency Engineering Framework must not be considered in isolation. A given implementation of a technique can support, use, depend on, or conflict with, or complicate (i.e., make effective use more difficult or costly) implementations of other techniques. For example, Unpredictability can be used in conjunction with Adaptive Response, Analytic Monitoring, Deception, Diversity, Dynamic Positioning, Non-Persistence, Privilege Restriction, and Segmentation. However, it can also make some implementations of those and other techniques more difficult. Coordinated Defense – particularly the Technical Defense-in-Depth implementation approach – can be applied to any of the other techniques.

[11] For more information, see [29] and Appendix D of [2].

© 2015 The MITRE Corporation. All Rights Reserved.

Details of interactions among representative implementation approaches are given in Appendix A. A summary of potential interactions is given in Appendix B.

3.3 Seek Effects Throughout the Cyber Attack Lifecycle

Attacks or intrusions by the APT against organizations or missions are multistage, and occur over periods of months or years. Recognition of this has led to the development of Cyber Attack Lifecycle (CAL) models, which define stages an adversary goes through to achieve their objectives. The CAL[12] provides a framework for understanding and analyzing how distinct adversary activities contribute to an attack. This understanding is crucial to crafting an effective defense. Understanding the CAL gives insight into the steps the adversary needs to complete to be successful. This understanding enables the defender to identify actions and opportunities for countering adversary activities. Rather than focusing on a single stage of the lifecycle (e.g., trying to prevent deliver of malware), the defender can attempt to counter the adversary at various stages, as the adversary needs to satisfy all the stages to achieve its goals.

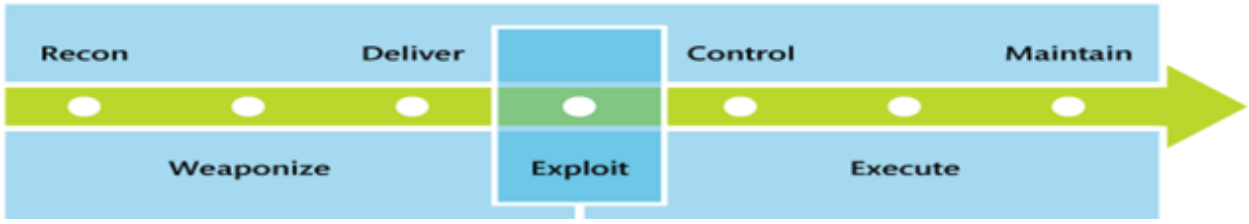

Figure 5. Cyber Attack Lifecycle

Figure 5 depicts and Appendix B describes the CAL stages of a malware-based cyber attack. The pre-exploit stages represent a defensive opportunity to proactively deter, detect, and mitigate threats before the adversary establishes a foothold. The structure of the adversary cyber attack campaign is recursive. In the post-exploit stages, the adversary attempts lateral movement to extend the foothold in the organization and the cycle repeats. Post-exploit, organizations can perform incident detection/response together with resilient operations to ensure that mission-critical assets continue to support mission operations.

Cyber resiliency techniques can impact adversary activities. To provide coverage of the entire cyber attack lifecycle or to ensure a variety of effects on the adversary, some combination of cyber resiliency techniques will be needed. Table 6 summarizes possible effects of applying cyber resiliency techniques on adversary activities at different stages in the cyber attack lifecycle; details are given in Appendix A. Terms are defined in Appendix B.

[12] There are multiple versions of the Cyber Attack Lifecycle, also referred to as the Cyber Kill Chain. The one depicted here is consistent with what is described as a cyber campaign in NIST SP 800-30 R1 [27].

© 2015 The MITRE Corporation. All Rights Reserved.

Table 6. Potential Effects of Cyber Resiliency Techniques on Adversary Activities Across the Cyber Attack Lifecycle

Cyber Resiliency Technique	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Adaptive Response	Contain Curtail		Negate Curtail	Negate	Degrade Delay Contain Curtail	Negate Curtail Degrade Delay Recover	Degrade Delay Contain Curtail
Analytic Monitoring	Detect Analyze		Detect Analyze	Analyze	Detect Analyze	Detect Analyze	Detect Analyze
Coordinated Defense		Delay		Degrade Delay	Detect Degrade Delay	Degrade Delay	Detect Degrade Delay
Deception	Degrade Delay Divert Deceive Detect Analyze	Deter Deceive	Deter Divert Deceive Analyze	Deter Divert Deceive Analyze	Deter Divert Deceive Detect Analyze	Deter Divert Deceive Degrade Detect Analyze	Deter Divert Deceive Detect Analyze
Diversity	Degrade Delay	Degrade Delay	Degrade Delay Contain	Degrade Negate	Degrade Contain Recover	Degrade Recover	Degrade Contain Recover
Dynamic Positioning	Detect Curtail		Negate Divert		Detect Degrade Delay Curtail Expunge Recover	Degrade Delay Curtail Expunge Recover	Detect Degrade Delay Curtail Expunge Recover
Dynamic Representation	Analyze				Detect Analyze	Detect Recover	Detect Analyze
Non-Persistence	Degrade Delay		Negate	Curtail Expunge	Curtail Expunge	Curtail	Curtail Expunge
Privilege Restriction	Degrade Delay			Negate Degrade Delay Contain	Negate Degrade Delay Contain	Negate Degrade Delay Contain	Negate Degrade Delay Contain
Realignment	Degrade Delay	Negate Degrade Delay	Negate Degrade Delay	Degrade Delay	Negate Degrade	Negate Degrade	Negate Degrade
Redundancy						Degrade Curtail Recover	
Segmentation / Isolation	Contain		Degrade	Contain	Degrade Delay Contain	Degrade Delay Contain Recover	Degrade Delay Contain
Substantiated Integrity			Negate Detect		Detect Curtail	Curtail Recover	Detect Curtail
Unpredictability	Delay	Delay	Detect	Delay	Delay Detect	Delay Detect	Detect

© 2015 The MITRE Corporation. All Rights Reserved.

The effects of a given approach on adversary activities will depend on the specific implementation and on the specific adversary TTPs. For example, some of the cyber resiliency implementation approaches affect adversary reconnaissance. However, those implementations will not affect recon performed outside the systems in which the techniques are implemented (e.g., social engineering activities in external social networks frequented by system users or administrators).

© 2015 The MITRE Corporation. All Rights Reserved.

4 References

[1] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework (MTR110237, PR 11-4436)," September 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

[2] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR 12-3795)," May 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf.

[3] D. Bodeau, J. Brtis, R. Graubart and J. Salwen, "Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain (MTR 130515, PR 13-3513)," September 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-3513-ResiliencyTechniques_0.pdf.

[4] Merriam-Webster, "Merriam-Webster Dictionary," Encyclopedia Britannica, 2015. [Online]. Available: http://www.merriam-webster.com/dictionary/system.

[5] CNSS, "National Information Assurance (IA) Glossary (CNSS Instruction No. 4009)," 26 April 2010. [Online]. Available: https://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[6] OSD, "Systems Engineering Guide for Systems of Systems, Version 1.0," August 2008. [Online]. Available: http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf.

[7] C. Zimmerman, Ten Strategies of a World-Class Computer Security Incident Response Team, Mclean,VA: The MITRE Corporation, 2014. (PR 12-4100)

[8] J. Xu, P. Guo and M. Zhao, "Comparing Different Moving Target Defense Techniques," in *Proceedings of the First ACM Workshop on Moving Target Defense*, 2014.

[9] DoD, "Technology Readiness Assessment (TRA) Guidance," April 2011. [Online]. Available: http://www.acq.osd.mil/chieftechnologist/publications/docs/TRA2011.pdf.

[10] J. Kruse, S. Landsman, P. Smyton, A. Dziewulski, H. Hawley and M. King, "The POET Approach: A collaborative means for enhancing C2 systems engineering," in *Proceedings of the International Command and Control Research and Technology Symposium*, Fairfax, VA, 2012.

[11] ArcSight, "Implementing ArcSight CEF, Version 20," 5 June 2013. [Online]. Available: https://protect724.hp.com/docs/DOC-1072.

[12] Control Systems Security Program, National Cyber Security Division, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October 2009. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf.

[13] Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks," 13 April 2012. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.

[14] NIST, "Supply Chain Risk Management Processes for Federal Information Systems and Organizations, NIST SP 800-161 (2nd Draft)," 3 June 2014. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf.

[15] The MITRE Corporation, "Crown Jewels Analysis," MITRE Systems Engineering Guide, [Online]. Available: http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

[16] S. Musman, M. Tanner, A. Temin, E. Elsaesser and L. Loren, "A systems engineering approach for crown jewels estimation and mission assurance decision making," in *IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, 2011.

© 2015 The MITRE Corporation. All Rights Reserved.

[17] T. Llanso, G. Talley, M. Silberglitt and T. Anderson, "Mission-Based Analysis for Assessing Cyber Risk in Critical Infrastructure Systems," in *Critical Infrastructure Protection VII, IFIP AICT 417*, International Federation for Information Processing, 2013, pp. 201-214.

[18] ICS-ISAC, "Situational Awareness Reference Architecture (SARA)," Industrial Control System Information Sharing and Analysis Center, 2015. [Online]. Available: http://ics-isac.org/blog/sara/.

[19] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[20] D. Bodeau, Graubart and Richard, "Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls (MTR 130531, PR 13-4037)," September 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-4047.pdf.

[21] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment (MTR 130432, PR 13-4173)," November 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf.

[22] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller and P. Smith, "Resilience and survivability in communication networks: Strategies,principles, and survey of disciplines," 17 March 2010. [Online]. Available: http://www.ittc.ku.edu/resilinets/papers/Sterbenz-Hutchison-Cetinkaya-Jabbar-Rohrer-Scholler-Smith-2010.pdf.

[23] CERT Program, "CERT® Resilience Management Model, Version 1.0: Improving Operational Resilience Processes," May 2010. [Online]. Available: http://www.cert.org/archive/pdf/10tr012.pdf. [Accessed 26 October 2011].

[24] A. M. Madni and S. Jackson, "Towards a Conceptual Framework for Resilience Engineering," *IEEE Systems Journal, Vol. 3, No. 2,* June 2009.

[25] Oxford University Press, "Definition of Cyberspace," Oxford Dictionaries, [Online]. Available: http://www.oxforddictionaries.com/us/definition/american_english/cyberspace.

[26] NIST, "Framework for Improving Critical Infrastructure Security, Version 1.0," 12 February 2014. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[27] NIST, "Guide for Conducting Risk Assessments, NIST SP 800-30 Rev.1," September 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[28] Booz | Allen | Hamilton, "Cyber Operations Maturity Framework," 16 June 2011. [Online]. Available: http://www.boozallen.com/media/file/Cyber-Operations-Maturity-Framework-viewpoint.pdf.

[29] R. Pietravalle and D. Lanz, "Resiliency Research Snapshot," June 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_3023.pdf.

[30] NIST, "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[31] CNSS, "Security Categorization and Control Selection for National Security Systems (CNSSI No. 1253), Version 2," 15 March 2012. [Online]. Available: http://www.disa.mil/Services/DoD-Cloud-Broker/~/media/Files/DISA/Services/Cloud-Broker/cnssi-security-categorization.pdf.

[32] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems, NIST SP 800-37 Rev. 1," February 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[33] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework," September 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

[34] The MITRE Corporation, "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness," The MITRE Corporation, Bedford, MA, 2015. (PR 15-0837)

© 2015 The MITRE Corporation. All Rights Reserved.

5 Acronyms

ADH	Architectural Diversity/ Heterogeneity
AM	Asset Mobility
AMgt	Adaptive Management
APT	Advanced Persistent Threat
AS&W	Attack Sensing & Warning
ASLR	Address Space Layout Randomization
BV	Behavior Validation
C3	Command, Control, and Communications
CAL	Cyber Attack Lifecycle
CAPEC	Common Attack Pattern Enumeration and Classification, https://capec.mitre.org/
C&CA	Coordination and Consistency Analysis
CCoA	Cyber Course of Action
CEF	Common Event Format
CND	Computer Network Defense
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
COOP	Continuity of Operations
COP	Common Operational Picture
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System(s)
CREF	Cyber Resiliency Engineering Framework
CRITs	Collaborative Research Into Threats, https://crits.github.io/
CVE	Common Vulnerabilities and Exposures, https://cve.mitre.org/
CWE	Common Weakness Enumeration, https://cwe.mitre.org/
CybOX	Cyber Observable eXpression, https://cybox.mitre.org/
CyCS	Cyber Command System, http://www.mitre.org/research/technology-transfer/technology-licensing/cyber-command-system-cycs
DDH	Design Diversity/ Heterogeneity
DF	Distributed Functionality
DiD	Defense-in-Depth
Dis	Dissimulation/ Disinformation
DivA	Synthetic Diversity system, https://www.atcorp.com/technologies/verifiable-computing/synthetic-diversity
DM&P	Dynamic Mapping and Profiling
DMZ	Demilitarized Zone
DRA	Dynamic Resource Allocation
DReconf	Dynamic Reconfiguration
DSI	Dynamic Segmentation / Isolation
DTM	Dynamic Threat Modeling
FOSS	Free and Open Source Software
GOTS	Government Off-The-Shelf
FRA	Functional Relocation of Cyber Assets
I&W	Indications & Warning
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IdAM	Identity and Access Management
IDS	Intrusion Detection System

© 2015 The MITRE Corporation. All Rights Reserved.

InfoD	Information Diversity
IQC	Integrity/Quality Checks
ISAC	Information Sharing and Analysis Center
ISO	International Standards Organization
LDAP	Lightweight Directory Access Protocol
M&DA	Monitoring and Damage Assessment
M&FA	Malware and Forensic Analysis
MAEC	Malware Attribute Enumeration and Characterization, https://maec.mitre.org/
MD&SV	Mission Dependency and Status Visualization
MTD	Moving Target Defense
NCF	NIST Cybersecurity Framework
NIST	National Institute of Standards and Technology
NPC	Non-Persistent Connectivity
NPI	Non-Persistent Information
NPS	Non-Persistent Services
O/O	Offloading/Outsourcing
OAI-ORE	Open Archives Initiative Object Reuse and Exchange
OPM	Open Provenance Model, http://openprovenance.org/
OPSEC	Operations Security
OS	Operating System
P2P	Peer-to-Peer
PB&R	Protected Backup and Restore
PII	Personally Identifiable Information
PM	Privilege Management
POET	Political, Operational, Economic, and Technical
PROV	W3C Provenance family of specifications, http://www.w3.org/TR/prov-dm/
PS	Predefined Segmentation
PT	Provenance Tracking
PUR	Privilege-Based Usage Restrictions
QoS	Quality of Service
RAdAC	Risk-Adaptable (or Adaptive) Access Control
RBAC	Role-Based Access Control
SA	Situational Awareness
SARA	Situational Awareness Reference Architecture
SC	Surplus Capacity
SCD	Supply Chain Diversity
SCRM	Supply Chain Risk Management
SD	Synthetic Diversity
SDN	Software-Defined Networking
SF&A	Sensor Fusion and Analysis
SIEM	Security Information and Event Management
Sim	Misdirection/ Simulation
SOA	Service-Oriented Architecture
SLA	Service Level Agreement
STIX	Structured Threat Information eXpression, https://stix.mitre.org/
TAXII	Trusted Automated eXchange of Indicator Information, http://taxii.mitre.org/
TTPs	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
VMM	Virtual Machine Monitor
VPN	Virtual Private Network
W3C	World-Wide Web Consortium

© 2015 The MITRE Corporation. All Rights Reserved.

XML	eXtensible Markup Language

Appendix A Details on Cyber Resiliency Techniques

This Appendix is intended to support engineering analysis, in particular identification and analysis of alternatives in system architecture and design. Each cyber resiliency technique is presented in a table, which identifies representative approaches to implementing it.

In the left cell under an approach, the maturity of each approach is assessed in the context of general-purpose enterprise computing, with respect to its original domain (e.g., performance, dependability, conventional security). In support of the assessments, examples are given of ways to implement the approaches, using representative

- Tools or technologies. These refer to classes of products, or technical capabilities provided by multiple classes of products.
- Processes. These refer to organizational or operational processes or procedures.
- Standards. These refer to technical and data standards, which need not be promulgated by standards organizations. (See the list of acronyms.)

Each approach is also assessed with respect to its readiness for use in achieving cyber resiliency goals and objectives in the face of advanced cyber threats; information about the latter is in *italics*. Maturity and examples for general uses such as performance and dependability are identified to encourage consideration of ways (primarily procedural, but possibly tool-supported) that existing technologies and processes could be used differently to address advanced cyber threats as well as non-adversarial sources of adversity.

In the middle cell under each approach, additional details are given on interactions with other approaches. It must be noted that some interactions among techniques are thus not identified, because the approaches are representative but not exhaustive of the techniques.

In the right cell under each approach, potential effects on adversary activities are identified.[13] Adversary activities are in **bold**; potential effects are in *italics*.

However, the discussion remains somewhat general. The potential interactions among approaches must be understood as representative; for example, the extent to which Dynamic Reconfiguration (DReconfig) depends on Monitoring and Damage Assessment (M&DA) will be determined by the specific DReconfig and M&DA implementations. Similarly, the potential effects on adversary activities will depend on how – and how effectively – the approach is used. Finally, the assessment of relative maturity is with respect to general-purpose systems and generally accepted standards of good practice. Similarly, the assessment of relative ease of adoption is for organizations that have an established information security program or cyber security program. Assessments will change over time, as new technologies and practices are adopted, and as standards of good practice evolve.

[13] The effects on adversary activities updates the information in Appendix C of [21].

© 2015 The MITRE Corporation. All Rights Reserved.

Table 7. Adaptive Response

Adaptive Response: Implement nimble cyber courses of action (CCoAs) to manage risks (concluded on next page)		
Dynamic Reconfiguration (DReconf): Make changes to an element or component while it continues operating.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Highly mature for system / network management. Mature for conventional cybersecurity. • **Tools**: Configuration Management, Dynamic Reconfiguration *Cyber Resiliency:* *Ready to adopt.* *Technical and operational challenges with respect to ensuring consistency and avoiding cascading failures across distributed systems.* • ***Tools**: Automated Threat Response, some products characterized as MTD*	Depends on Analytic Monitoring (M&DA, SF&A) Uses Dynamic Positioning Uses Dynamic Representation (DM&P, MD&SV) Supports and uses Non-Persistence Supports and uses Privilege Restriction Supports and uses Segmentation / Isolation Uses Substantiated Integrity Uses Unpredictability	**Recon**: *Curtail*: The adversary's knowledge of resources and configuration becomes outdated. *Contain*: The resources against which the adversary can conduct recon are restricted. **Deliver**: *Negate*: The adversary's attack payload is not delivered. *Curtail*: The adversary's delivery mechanism stops working. **Exploit**: *Negate*: The adversary's exploit is based on outdated premises. **Control, Maintain**: *Contain*: The adversary's activities are limited to resources that have not been reconfigured. *Curtail*: Reconfiguration (e.g., changing internal communications or call paths) renders the adversary's activities ineffective. **Execute**: *Negate*: Reconfiguration (e.g., blocking ports and protocols) renders ineffective the activities the adversary could take to achieve consequences by changing the assumptions on which adversary actions are based. *Delay*: Reconfiguration requires the adversary to revise plans or take additional steps in order to achieve consequences.

© 2015 The MITRE Corporation. All Rights Reserved.

Adaptive Response (concluded)		
Dynamic Resource Allocation (DRA): Change the allocation of resources to tasks or functions without terminating critical functions or processes.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Mature and widely used, primarily for performance optimization. • **Tools**: On-demand computing, load balancing, lowering the priority of or terminating non-critical functions • **Process**: Enterprise Resource Planning *Cyber Resiliency:* *Somewhat ready to adopt.* *Technical and operational challenges with respect to ensuring consistency and avoiding unanticipated consequences.*	Depends on Analytic Monitoring (M&DA, SF&A) Uses Diversity (DDH) Supports and uses Dynamic Positioning (FR, DF) Uses Dynamic Representation (DM&P, MD&SV) Uses Redundancy (SC, Replication) Uses Unpredictability	**Control, Execute, Maintain**: *Curtail*: Resource reallocation removes resources from the adversary's control. **Execute**: *Degrade*: Resource reallocation enables mission continuity at some level, reducing the effectiveness of the adversary's goal of denying mission capabilities. *Delay*: The adversary must revise plans or take additional steps, due to changes in available resources. *Recover*: Resource reallocation enables recovery of mission functions when the adversary's goal is denial of service.
Adaptive Management (AMgt): Change how defensive mechanisms are used based on changes in the operational environment as well as changes in the threat environment.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Assumes a foundation of Incident Response. Transitional for cyber security, but uptake largely depends on governance and interoperability. • **Processes**: Integrated Risk Management, Tabletop Exercises, Cyber Playbooks *Cyber Resiliency:* *Somewhat ready to adopt.* *Technical and operational challenges with respect to ensuring consistency and avoiding unanticipated consequences; political challenges with respect to responsibilities for ongoing / dynamic risk management.*	Depends on Analytic Monitoring Supports Coordinated Defense Uses Dynamic Representation	**Control, Maintain**: *Degrade* and *Delay*: The adversary must adapt to changing processes. **Execute**: *Negate:* The state variables on which the adversary's attack was based can be changed, foiling the attack. *Recover*: The ability to change how mechanisms are used provides more recovery options.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 8. Analytic Monitoring

Analytic Monitoring: Continuously gather, fuse, and analyze threat intelligence data to identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage (concluded on next page)		
Monitoring and Damage Assessment (MD&A): Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, detect and assess damage, and watch for adversary activities during recovery and evolution.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
For conventional and cyber security, Increasingly mature for indicators; highly mature and widely used for detection and damage assessment. However, effectiveness against the APT is often limited. • **Tools**: Intrusion Detection Systems (IDSs), sensors (host & network), event log management, telemetry, static/dynamic code analysis tools • **Process**: Establish coverage and timeframes or frequency for data gathering and analysis to avoid gaps or blind spots • **Standards**: Syslog, Windows Event XML, CEF [11], CWE, CAPEC *Cyber Resiliency:* *Ready to adopt. Operational challenges in the context of recovery and evolution; political and operational challenges regarding managing (and managing risks associated with) large volumes of monitoring data.*	Supports Adaptive Response Supports Analytic Monitoring (SF&A) Depends on Coordinated Defense (C&CA) Uses Deception (Dis, Sim) to obtain data; conflicts with Deception (Obfuscation) by requiring data in the clear Uses Diversity (DDH for different sensors); conflicts with Diversity (C3) which makes monitoring more complex Uses Dynamic Positioning (FR) for sensor relocation Supports Dynamic Representation (DM&P, MD&SV) Uses Substantiated Integrity (BV)	**Recon, Deliver, Control, Maintain**: *Detect*: Monitoring provides indications and warning (I&W) or attack sensing and warning (AS&W), making the adversary's activities visible to defenders. Damage assessment reveals the extent of the effects of adversary activities. **Execute**: *Analyze*: Damage assessment determines the extent of adversary effects on capabilities and data.
Sensor Fusion and Analysis (SF&A): Fuse and analyze monitoring data and preliminary analysis results from different components, together with externally provided threat intelligence.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
For conventional and cyber security, Transitional-to- mature for ICT; widely used within the enterprise and by CND service providers; SF&A beyond the enterprise face policy and data quality challenges • **Tools**: SIEM (aggregation & correlation), threat intelligence feeds • **Standards**: STIX, TAXII, CAPEC *Cyber Resiliency:* *Ready to adopt. Technical challenges with respect to synergy with other techniques, coordination across architectural layers; operational / political challenges with fusion across systems with different owners. Significant benefits to be gained from meaningful combinations of indicators, sense-making.*	Supports Adaptive Response Depends on Coordinated Defense (C&CA) Uses Deception (Dis, Sim) to obtain data Uses Diversity (InfoD) Uses Dynamic Positioning (DF) Supports Dynamic Representation (DM&P, MD&SV)	**Recon, Control, Maintain**: *Detect*: Sensor fusion enables enhanced I&W or AS&W, making the adversary's activities visible to defenders. *Analyze*: Sensor fusion enables more complete and comprehensive analysis of adversary activities.

© 2015 The MITRE Corporation. All Rights Reserved.

Analytic Monitoring (concluded)		
Malware and Forensic Analysis (M&FA): Analyze malware and other artifacts left behind by adversary activities.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature for widely used technologies (particularly at the network and OS layers). Supports damage assessment. • **Tools**: Reverse Engineering • **Process**: Penetration testing or active probing • **Standards**: MAEC, CybOX *Cyber Resiliency:* *Ready to adopt. Economic challenge of need for ongoing resource commitment; operational / political challenge of balancing need to preserve artifacts with goal of expunging adversary presence.*	Supports Adaptive Response Depends on Coordinated Defense (C&CA) Uses Deception (Dis, Sim) to obtain data Uses Diversity (DDH for different malware analysis tools) Uses and supports Substantiated Integrity (IQC)	**Deliver, Exploit, Control, Maintain**: *Analyze*: The adversary's TTPs and capabilities are better understood.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 9. **Coordinated Defense**

Coordinated Defense: Manage multiple, distinct mechanisms in a non-disruptive or complementary way		
Technical Defense-in-Depth (DiD): Use multiple protective mechanisms, at different architectural layers or locations.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Highly mature for widely used technologies. • **Process**: Cyber Defense in Depth processes, e.g., [12] *Cyber Resiliency:* *Ready to adopt. Political challenge of defining threat-informed analysis processes; economic challenges include the need for ongoing resource commitment, and potential increases to (1) the cost of development and testing and (2) the complexity of management, training and maintenance.*	Supports Analytic Monitoring (M&DA, SF&A) to ensure coverage Uses Diversity Uses Realignment (Restriction) Uses Segmentation / Isolation	**Weaponize**: *Delay*: The adversary must develop or acquire exploits effective against multiple defensive technologies deployed concurrently at a single layer to be successful. **Exploit**: *Degrade* and *Delay*: The adversary must use multiple exploits to obtain a foothold.
Coordination and Consistency Analysis (C&CA): Apply processes, supported by analytic tools, to ensure that defenses are applied and cyber courses of action are defined and executed in a coordinated, consistent way that minimizes interference.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Transitional-to-Mature, depending on governance and interoperability. • **Tools**: Unified IdAM administration tools • **Processes**: Tabletop exercises, fault injection, red teaming, exercises of TTPs *Cyber Resiliency:* *Ready to adopt. Political challenges of (1) defining threat-informed analysis processes, (2) resolving policy conflicts across organizations while still respecting equities, particularly as mission needs change over time; operational challenge of identifying unforeseen functional or mission dependencies.*	Uses Adaptive Response (AMgt) Supports Analytic Monitoring (M&DA, SF&A) to ensure coverage Supports Coordinated Defense (DiD) Supports and uses Privilege Restriction	**Control, Maintain**: *Detect*: Inconsistencies (e.g., in configurations or in privilege assignments) provide indications of adversary activities. *Degrade* and *Delay*: The adversary cannot take advantages of inconsistencies in configurations, privileges, or behaviors of defensive tools to expand or retain their presence. **Execute**: *Degrade* and *Delay*: The adversary cannot take advantage of unintended consequences or unforeseen dependencies to cause adverse consequences of defensive actions (e.g., cascading failures).

© 2015 The MITRE Corporation. All Rights Reserved.

Table 10. Deception

Deception: Mislead, confuse, or hide critical assets from, the adversary (concluded on next page)		
Obfuscation: Hide, transform, or otherwise obfuscate information from the adversary.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Mature and widely used, particularly in the form of encryption. • **Tools**: Data encryption, traffic obfuscation via onion routing *Cyber Resiliency:* *Highly ready to adopt. Operational challenges of identifying information to be obfuscated, addressing interactions between obfuscation and other techniques.*	Conflicts with Analytic Monitoring (M&DA) Uses Dynamic Positioning (FR) Supports Substantiated Integrity (IQC, PT) by making adversary fabrication or modification harder	**Recon**: *Degrade* and *Delay*: The adversary must perform additional analysis to determine or acquire the utility of repackaged data (e.g., configuration files). **Execute**: *Degrade*: The adversary cannot reliably determine which targets are valuable or cannot make the correlations needed to deduce the value of possible targets, and hence must either try to affect more targets (e.g., exfiltrate more files, bring down more VMs) than necessary to achieve objectives, or accept more uncertainty as to effectiveness. *or* The adversary cannot make as effective use of target data (e.g., the adversary must make additional transformations, possibly with data loss).
Dissimulation/ Disinformation (Dis): Provide deliberately misleading information to adversaries.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Mature – but not often practiced – when made part of an overall OPSEC strategy. • **Tools**: Function hooking, Man-in-the-middle • **Processes**: Respond to adversary queries with deliberately confusing or erroneous information; fabricate documents or data stores *Cyber Resiliency:* *Somewhat ready to adopt.* *Political and operational challenges of determining what dissimulation is appropriate; operational and economic challenges of applying the significant ongoing effort needed for effectiveness.*	Supports Analytic Monitoring (M&DA) Supports Dynamic Representation (DTM) Uses Unpredictability [Note: could use other techniques, such as Adaptive Response, Dynamic Positioning]	**Recon, Control, Execute, Maintain**: *Detect*: The adversary's use of fabricated control data (e.g., configuration, network topology, or asset inventory data) serves as an indicator of adversary activity. *Deceive*: The adversary's knowledge about mission or defender activities is incomplete or (if defenders place false information on C3 paths to which the adversary has access) false. **Recon, Execute**: *Detect*: Attempts to access fabricated targets provides an indication of adversary activities. *Divert*: The adversary directs efforts at fabricated targets (e.g., fabricated mission, configuration, or topology data). **Weaponize**: *Deceive*: The adversary's efforts are based on false information (e.g., configuration data, identification of software and versions) and thus are wasted. **All phases post-Recon**: *Deter*: Adversary reconnaissance falsely indicates that the expected value of carrying out a cyber attack does not justify the expected costs or risks.

© 2015 The MITRE Corporation. All Rights Reserved.

Deception (concluded)		
Misdirection/ Simulation (Sim): Maintain deception resources or environments and direct adversary activities there.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature, but with wide variations in operational use. • **Tools**: Decoy servers, services, or deception environments (e.g., Honeypots, Honeynets) *Cyber Resiliency:* *Somewhat ready to adopt. Political and operational challenges of committing to misdirection; operational and economic challenges of applying the significant ongoing effort needed for effectiveness; operational challenge of maintaining realistic deception; operational challenge of possible defender complacency, if the adversary executes a multi-pronged attack and not all prongs are confined to the deception environment.*	Supports and uses Analytic Monitoring (MD&A) Uses Dynamic Positioning (FR) Supports Dynamic Representation (DTM) Uses Segmentation / Isolation (PS) to maintain deception sub-networks Uses Unpredictability	**Recon**: *Divert*: The adversary is directed to false targets; the adversary's efforts are wasted unless and until the adversary recognizes the misdirection. *Deceive*: The adversary develops false intelligence about the defender's cyber resources, mission / business function dependencies, or TTPs. *Analyze*: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting. **Weaponize**: *Deter*: The adversary is daunted by the technical complexity of the system for which exploits must be developed, and seeks an easier target elsewhere. *Deceive*: The adversary develops or acquires exploits compatible with the deception environment rather than the operational environment; the adversary's efforts are wasted. **Exploit**: *Deceive*: The adversary's exploits falsely appear to succeed and grant access to targets; the adversary's efforts are wasted. *Analyze*: Analysis of the adversary's exploits increases understanding of adversary TTPs and capabilities. **Deliver, Control, Execute, Maintain**: *Deter*: The adversary determines that the potential consequences or the required effort of achieving effects is not worth the potential benefits. *Divert*: The adversary's efforts are wasted on false targets. *Deceive*: The adversary develops a false understanding of the operational environment and of the effects achieved, leading to wasted efforts. *Analyze*: Analysis of adversary activities increases understanding of adversary TTPs, capabilities, intent, and targeting.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 11. Diversity

Diversity: Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities (continued on next page)		
Architectural Diversity/ Heterogeneity (ADH): Use multiple sets of technical standards, different technologies, and different architectural patterns.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Dependability: Maturity varies depending on technology, with wide variations in intentional operational use. To contain operations and maintenance costs, many organizations seek heterogeneity. (Incidental architectural diversity often results from procurement over time and differing user preferences.) • **Tools**: Support architectural diversity by using security management tools capable of managing products with different architectures • **Process**: Use products that follow different standards or architectures (e.g., using both Linux and Windows based operating systems) to provide equivalent functionality *Cyber Resiliency:* *Somewhat ready to adopt. Technical challenges with respect to cost-effective application, lack of interface standards; economic challenge of maintaining multiple current versions.*	Supports Adaptive Response (DRA) Supports and complicates Analytic Monitoring (multiple sensor architectures support M&DA, but make SF&A harder; multiple technologies make M&FA harder) Supports and complicates Coordinated Defense (improves options for DiD, but makes C&CA harder) Complicates Dynamic Representation (makes DM&P harder) Supports Redundancy (makes Replication much more effective) Supports Unpredictability	**Weaponize**: *Degrade* and *Delay*: The adversary must develop or acquire exploits effective against variant implementations. **Exploit**: *Negate*: The adversary's exploits will not work against variant implementations as they are different from the one's implementations the adversary anticipated. *Degrade*: The adversary's exploits will work only against a subset of the variant implementations. [Note that each of these effects can be short-lived, as the adversary adapts.] **Control, Maintain**: *Degrade*: The adversary must control a set of compromised resources with different characteristics (requiring greater expertise and effort). *Contain*: The adversary is limited to controlling compromised resources about which they have expertise and for which they have control tools. **Execute**: *Recover*: Recovery from the mission effects of adversary activities can create opportunities for further adversary activities. Secure recovery is facilitated by using components against which the adversary does not have exploits or control tools.

© 2015 The MITRE Corporation. All Rights Reserved.

Diversity: Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities (continued)		
Design Diversity/ Heterogeneity (DDH): Use different designs to meet the same requirements or provide equivalent functionality.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Dependability: Mature but rarely used, due to costs. • **Tools**: N-variant software generation tools (used during development) • **Process**: N-version programming (Start with a single specification and use parallel teams to do design and implementation, as in fault tolerance and safety critical environments, e.g., avionics). Re-implement and replace, or custom-develop, critical components *Cyber Resiliency:* *Challenging to adopt. Technical challenges with respect to ensuring consistency; economic challenges of maintaining multiple current versions (i.e., costs & complexity of management, training and maintenance).*	Supports Adaptive Response (DRA) Supports and complicates Analytic Monitoring as above Supports and complicates Coordinated Defense as above Complicates Dynamic Representation Supports Redundancy (Replication) Supports Unpredictability	**Weaponize, Exploit, Control, Execute, Maintain**: Same as for Architectural Diversity / Heterogeneity.
Synthetic Diversity (SD): Transform implementations to produce a variety of instances.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature for a few software components, otherwise immature-to-transitional • **Tools**: ASLR in software, DivA (in development) *Cyber Resiliency:* *Challenging to adopt, except when highly mature. Technical challenges relate to ensuring correctness and consistency of functionality.*	Supports Adaptive Response (DC) Supports Redundancy (Replication) Supports Unpredictability	**Weaponize, Exploit, Control, Execute, Maintain**: Same as for Architectural Diversity / Heterogeneity. In addition, SD can have the strategic effect of forcing the adversary to change targets.

© 2015 The MITRE Corporation. All Rights Reserved.

Diversity (continued)		
Information Diversity (InfoD): Provide information from different sources or transform information in different ways.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Contingency Planning and COOP: Maturity and operational use vary, depending on technology and mission / business process. *Cyber Resiliency:* *Challenging to adopt. Technical challenges relate to (1) availability of and differences in quality of different sources and (2) ensuring ability to use data in different forms; economic challenges of obtaining, managing, and storing data from different sources.* • ***Process**: Identify alternative sources of information, determine the extent to which they are independent, and define methods for using alternative sources*	Supports Adaptive Response (DReconf) Conflicts with Analytic Monitoring (M&DA) Uses Diversity (C3) Complicates Dynamic Representation Uses Privilege Restriction (PM) Supports Redundancy (Replication) Uses Substantiated Integrity (IQC, PT) Supports Unpredictability	**Control, Execute, Maintain**: *Degrade*: The adversary must modify or replace multiple different versions of information in order to corrupt mission or system information without detection. *Recover*: Reconstruction of mission or system information is facilitated by having multiple sources.
Command, Control, and Communications (C3) Path Diversity: Provide multiple paths, with demonstrable degrees of independence, for information to flow between components.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Contingency Planning and COOP: Mature, but operational use varies. • **Tools**: Decentralized networks, P2P, Software-Defined Networking (SDN) [13]; alternative protocols and communications media *Cyber Resiliency:* *Challenging to adopt. Technical and operational challenges relate to determining and ensuring degrees of independence, particularly in federated or cloud environments.*	Supports Adaptive Response (DReconf) Complicates Analytic Monitoring (M&DA) Supports Coordinated Defense (DiD) Supports Dynamic Positioning (DF) Conflicts with Dynamic Representation Uses Privilege Restriction (PM) Supports Redundancy (Replication) Supports Unpredictability	**Control, Execute, Maintain**: *Recover*: Recovery from the mission effects of adversary activities is facilitated by the use of C3 paths to which the adversary lacks access (e.g., out-of-band communications among defenders).

© 2015 The MITRE Corporation. All Rights Reserved.

Diversity (concluded)		
Supply Chain Diversity (SCD): Use multiple, demonstrably independent, supply chains for critical components.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security; supply chain risk management for non-adversarial risks Mature (generally accepted standards of good practice) but not widely adopted. • **Processes**: Supply Chain Risk Management (SCRM) processes [14] *Cyber Resiliency:* *Somewhat ready to adopt. Technical and operational challenge of establishing that supply chains are truly independent, particularly for COTS / FOSS; technical and operational challenge of identifying individual components, particularly with complex systems and embedded components; economic challenge of relying on multiple supply chains.* • ***Processes**: Crown Jewels Analysis (CJA)* [15] [16]*, Mission-Based Analysis (MBA)* [17]	Supports Coordinated Defense (DiD) Uses Realignment (Purposing) Supports Unpredictability	**Recon**: *Degrade* and *Delay*: The adversary must investigate multiple supply chains. **Deliver**: *Degrade* and *Delay*: The adversary must compromise multiple supply chains, or accept that only a subset of target components will be compromised. *Contain*: The adversary's effects are limited to a subset of target components.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 12. Dynamic Positioning

Dynamic Positioning: Distribute and dynamically relocate functionality or assets (concluded on next page)		
Functional Relocation of Sensors (FRS): Relocate sensors, or reallocate responsibility for specific sensing tasks, to look for indicators of adversary activity, and to watch for adversary activities during recovery and evolution.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature with respect to tasking; immature with respect to relocation • **Tools**: Redundant services, SDN • **Standards**: OpenFlow [13] *Cyber Resiliency:* *Challenging to adopt. Technical and operational challenges with respect to agility, ensuring synergies with other techniques, and handling recovery and evolution.* • ***Process**: Task specific operators (users, administrators, defenders) to look for anomalous behavior during recovery*	Uses (AMgt) and supports (DReconf, DRA) Adaptive Response Supports Analytic Monitoring (M&DA) Uses FRA Uses Non-Persistence (NPS, NPC) Uses and supports Unpredictability	**Recon, Control, Execute, Maintain**: *Detect*: The likelihood of detection is increased by tailored sensing. **Control, Maintain**: *Degrade*: Tailored sensing makes adversary efforts to expand or maintain a persistent presence harder.
Functional Relocation of Cyber Assets (FRA): Change the location of assets that provide functionality (e.g., services, applications) or information (e.g., data stores), either by moving the assets or by transferring functional responsibility.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Performance: Mature in virtual environments. • **Tools**: Virtualization/containers • **Standards**: OpenFlow *Cyber Resiliency:* *Somewhat ready to adopt. Political, operational, and technical challenges largely relate to transitional status of MTD tools.* • ***Tools**: Some products characterized as MTD*	Uses (AMgt) and supports (DReconf, DRA) Adaptive Response Conflicts with Analytic Monitoring (M&DA) Supports Deception (Obfuscation, Sim) Uses Non-Persistence (NPS, NPC) Uses and supports Unpredictability	**Recon, Control, Execute, Maintain**: *Curtail*: The period in which adversary activities are effective against a given location or instance of an asset is limited. **Deliver**: *Divert*: The adversary's activity is diverted to a different target, as the intended target has moved. *Negate*: The adversary's activity fails, because the intended target has moved. **Control, Execute, Maintain**: *Expunge*: Compromised running software is deleted, if relocation involves re-instantiating software from a clean version. *Recover*: Mission capabilities are restored, and trust can also be restored when relocation involves re-instantiating software from a clean version.

© 2015 The MITRE Corporation. All Rights Reserved.

Dynamic Positioning (concluded)		
Asset Mobility (AM): Physically relocate physical assets (e.g., platforms or vehicles, mobile computing devices).		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Safety, Dependability: Mature in limited set of operational environments. • **Tools**: Wireless, VPN, hot swappable components • **Standards**: OpenFlow *Cyber Resiliency:* *Challenging to adopt. Technical challenges relate to understanding relationship between physical and logical accessibility; operational challenges relate to ensuring consistency and avoiding unanticipated consequences.*	Uses Adaptive Response (AMgt) Complicates Analytic Monitoring (MD&A, SF&A) Supports Deception (Obfuscation) Uses Non-Persistence (NPC) Uses and supports Unpredictability	**Recon, Control, Execute, Maintain**: Curtail: The period in which adversary activities are effective against a given location or instance of an asset is limited.
Distributed Functionality (DF): Distribute functionality (e.g., processing, storage, and communications) across multiple components.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Performance, Dependability: Extremely mature in many enterprise architectures. • **Tools**: Service oriented architecture (SOA), cloud computing • **Standards**: OpenStack *Cyber Resiliency:* *Somewhat ready to adopt. Technical challenges relate to determining what forms of distribution are effective in a contested environment; operational challenges relate to ensuring consistency and avoiding unanticipated consequences.*	Uses Adaptive Response (AMgt) Complicates Analytic Monitoring (MD&A, SF&A) Supports Deception (Obfuscation, Sim) Uses Diversity (C3) Uses Redundancy (Replication) Uses and supports Unpredictability	**Control, Execute, Maintain**: *Degrade* and *Delay*: The adversary must compromise more elements in order to deny or corrupt functionality. *Recover*: Mission functionality is available from a combination of elements.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 13. Dynamic Representation

Dynamic Representation: Construct and maintain current representations of mission posture in light of cyber events and cyber courses of action (concluded on next page)		
Dynamic Mapping and Profiling (DM&P): Maintain current information about resources, their status, and their connectivity.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Performance, Dependability: Mature Cyber security: Transitional • **Tools**: Tools referenced in Situational Awareness Reference Architecture (SARA) Guide [18] • **Process**: Define and maintain a Common Operational Picture (COP), including Cyber Security Situational Awareness *Cyber Resiliency:* *Somewhat ready to adopt. Technical and operational challenge of integrating cybersecurity assessment tools for different types of resources.*	Supports Adaptive Response Uses Analytic Monitoring (M&DA, SF&A) Uses Substantiated Integrity (BV)	**Control, Maintain**: *Detect*: Software and components that do not conform to policy requirements or that are behaving in unexpected ways are identified.
Dynamic Threat Modeling (DTM): Maintain current information about threat activities and characteristics (e.g., observables, indicators, TTPs).		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Immature-to-transitional • **Tools**: Modeling and simulation (M&S) and attack tree analysis tools for threat intelligence analysis (some with real-time or dynamic capabilities) • **Processes**: Threat information sharing, threat intelligence analysis • **Standards**: STIX, TAXII, CRITs *Cyber Resiliency: Somewhat ready to adopt.* *Operational challenges relate to how to model threats when an adversary is trying to deceive defenders, how to reflect different levels of confidence in shared threat information; technical challenges relate to harmonizing different models and standards.*	Uses Analytic Monitoring (M&FA)	**Recon, Control, Maintain**: *Analyze*: Patterns and trends in adversary behavior are revealed.

© 2015 The MITRE Corporation. All Rights Reserved.

Dynamic Representation (concluded)		
Mission Dependency and Status Visualization (MD&SV): Maintain current information about mission dependencies on resources, and the status of those resources with respect to threats.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Performance, Cyber security: Existing methods mature but too manually intensive to provide current information; immature-to-transitional w.r.t. threat representation. • **Tools**: CyCS, tools referenced in SARA Guide [18] • **Processes**: Crown Jewels Analysis (CJA) [15] [16], Mission-Based Analysis (MBA) [17] *Cyber Resiliency:* *Somewhat ready to adopt. Technical challenge of determining the trustworthiness of the picture when an adversary is trying to deceive defenders; technical and operational challenge of integrating cybersecurity and performance assessment tools for different types of resources.*	Supports Adaptive Response Uses Analytic Monitoring Supports Realignment (O/O, A/R)	**Execute**: *Detect*: Identify consequences of adversary execution as they occur. *Recover*: Recovery of mission capabilities from adversary activities is facilitated by knowledge of which resources were or will be needed.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 14. Non-Persistence

Non-Persistence: Generate and retain resources as needed or for a limited time (concluded on next page)		
Non-Persistent Information (NPI): Refresh information periodically, or generate information on demand, and delete it when no longer needed.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Performance: Mature for some technologies • **Tools**: Distributed databases with just-in-time generation • **Standards**: Open Archives Initiative Object Reuse and Exchange (OAI-ORE) Conventional security: Mature for some technologies • **Standards**: NIST SP 800-53R4 SC-4 control [19] *Cyber Resiliency:* *Somewhat ready to adopt. Technical and operational challenge of identifying mission dependencies on information (often indirect).*	Supports (DRA) and uses (AMgt) Adaptive Response Uses Substantiated Integrity (IQC)	**Execute**: *Curtail*: The period during which the adversary can acquire mission or control information is limited, as the information is deleted when no longer needed.
Non-Persistent Services (NPS): Refresh services periodically, or generate services on demand and terminate services after completion of a request.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Performance: Mature in some architectures (especially virtualized or cloud services) • **Tools**: Virtualization/containers, on-demand services *Cyber Resiliency:* *Somewhat ready to adopt. Technical and operational challenge of identifying mission dependencies on services (often indirect).* • ***Process**: Analyze long-running services, determine which if any need to be persistent, and set controls on others to ensure non-persistence*	Supports and uses Adaptive Response (DRA) Complicates Analytic Monitoring (M&DA) Supports Dynamic Positioning (FR, DF) Complicates Dynamic Representation (DM&P, MD&SV) Supports Unpredictability	**Exploit**: *Curtail*: The adversary's attempt to exploit a vulnerability is curtailed when the attacked service is terminated. **Control, Execute, Maintain**: *Curtail*: The period during which adversary activities are effective against a given instance of a service is limited. **Exploit, Control, Maintain**: *Expunge*: Compromised services are terminated when no longer needed; if re-instantiated from a clean version, new instances will not be compromised and malware will be deleted.

© 2015 The MITRE Corporation. All Rights Reserved.

Non-Persistence (concluded)		
Non-Persistent Connectivity (NPC): Establish connections on demand, and terminate connections after completion of a request or after a period of non-use.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Performance: Mature for some technologies; for others, designed-away. • **Tools**: Network QoS, configuration tools to set network connection / keep-alive (KA) timeouts *Cyber Resiliency:* *Ready to adopt. Technical and operational challenge of identifying mission dependencies on connectivity (sometimes indirect).* • ***Process**: Analyze long-term connections, determine which if any need to be persistent, and set controls on others to ensure non-persistence*	Supports and uses Adaptive Response (DRA) Complicates Analytic Monitoring (M&DA) Supports Dynamic Positioning Complicates Dynamic Representation (DM&P, MD&SV) Supports Unpredictability	**Recon**: *Degrade* and *Delay*: The adversary must re-establish connections in order to complete reconnaissance. **Deliver**: *Negate*: A connection is terminated before the adversary can take advantage of it to deliver malware. **Control, Execute, Maintain**: *Curtail*: The period during which the adversary can make use of a C3 channel is limited.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 15. Privilege Restriction

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 (concluded on next page)		
Privilege Management (PM): Define, assign, and maintain privileges associated with end users and cyber entities (e.g., systems, services, devices), based on established trust criteria, consistent with principles of least privilege.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Mature but often poorly applied or designed-away • **Tools**: Domain server, LDAP, Federated IdAM • **Process**: Organizational processes for defining and managing privileges, e.g., least privilege, split keys, white list management *Cyber Resiliency:* *Highly ready to adopt. Political challenge of demanding application of least privilege; operational challenge of determining trust criteria and privileges. Operational and technical challenge of hard-coded trust relationships and component-to-component privileges.*	Supports Adaptive Response (DReconfig, DRA based on trust criteria) Uses Coordinated Defense (C&CA) Supports Realignment (Purposing, O/O)	**Recon**: *Degrade* and *Delay*: The adversary must invest more time and effort in obtaining credentials, or concentrate on fewer targets with those credentials. **Exploit, Control, Execute, Maintain**: *Contain*: Privilege-based restrictions limit the adversary's activities to resources for which the credentials the adversary has obtained allow use. *Delay*: The adversary's lack of credentials delays access to restricted resources. Negate: The adversary's lack of valid credential prevents access to restricted resources.
Privilege-Based Usage Restrictions (PUR): Define, assign, maintain, and apply usage restrictions on cyber resources based on mission criticality and other attributes (e.g., data sensitivity).		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Mature but often poorly applied or designed-away • **Tools**: Role Based Access Control (RBAC) enabled products *Cyber Resiliency:* *Ready to adopt. Operational challenge of determining criticality, other attributes, and corresponding privilege restrictions. Operational and technical challenge of hard-coded trust relationships and component-to-component privileges.*	Supports Adaptive Response (DReconfig, DRA based on usage restrictions) Uses Coordinated Defense (C&CA) Supports Realignment (Purposing, O/O) [Could use Dynamic Representation (MD&SV) to determine mission criticality]	**Exploit, Control, Execute, Maintain**: Negate: Privilege-based usage restrictions prevent the adversary from accessing critical or sensitive resources. Contain: Privilege-based usage restrictions limit the adversary's activities to non-critical resources, or to resources for which the false credentials the adversary has obtained allow use. Degrade: The adversary's lack of credentials delays access to restricted resources or requires the adversary to invest more effort to circumvent access controls.

© 2015 The MITRE Corporation. All Rights Reserved.

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 (concluded)		
Dynamic Privileges: Elevate or deprecate privileges assigned to a user, process, or service based on transient or contextual factors.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Mature for some ICT environments • **Tools**: Risk Adaptable Access Control (RAdAC) implementations *Cyber Resiliency:* *Somewhat ready to adopt. Operational challenge of identifying contextual factors; technical challenges of observing contextual factors, changing privileges, enabling override.*	Supports Adaptive Response (DReconf, DRA based on usage restrictions) Uses Coordinated Defense (C&CA) Supports Realignment (A/R) Uses Substantiated Integrity (IQC, PT) [Could use Dynamic Representation to evaluate some contextual factors]	**Exploit, Control, Execute, Maintain**: *Delay*: The adversary must obtain additional privileges in order to perform activities.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 16. Realignment

Realignment: Align cyber resources with core aspects of mission/business functions (concluded on next page)		
Purposing: Ensure cyber resources are used consistent with critical mission purposes.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Enterprise Systems Engineering: Mature but often not applied; runs counter to trends toward cloud and converged architectures. *Cyber Resiliency:* *Challenging to adopt. Political and operational challenges to applying this principle, given general trends toward multi-use or reusable resources.* • ***Process**: Determine the mission purposes of resources, so that uses that increase risk without any corresponding mission benefit can be identified and eliminated*	Uses Dynamic Representation (DM&P, MD&SV) Supports Diversity (SCD) Conflicts with Adaptive Response (DReconfig, AMgt), particularly in conjunction with Redundancy (SC)	**Deliver, Exploit**: *Degrade* and *Delay*: The adversary cannot take advantage of unnecessarily risky uses of resources (e.g., exposure of services to the Internet without offsetting mission benefits).
Offloading/Outsourcing (O/O): Offload supportive but non-essential functions to a service provider that is better able to support the functions.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Enterprise Systems Engineering: Mature but often poorly applied; outsourcing more commonly driven by economics, with security implications poorly considered • **Tools**: Cloud computing • **Standards**: OpenStack *Cyber Resiliency:* *Challenging to adopt. Political and operational challenges to applying this principle, given general trends toward multi-use or reusable resources; political challenge of designating some functions as non-essential.* • ***Processes**: Mission flow analysis, mission dependency analysis, tabletop exercises, Red Teaming to uncover undocumented mission dependencies*	Uses Dynamic Representation (DM&P, MD&SV) Uses Privilege Restriction Conflicts with Adaptive Response (DReconfig, AMgt), particularly in conjunction with Redundancy (SC)	**Deliver, Exploit**: *Degrade* and *Delay*: The set of opportunities the adversary can take advantage of is reduced.

© 2015 The MITRE Corporation. All Rights Reserved.

Realignment (concluded)		
Restriction: Remove or disable unneeded risky functionality or connectivity, or add mechanisms to reduce the risk.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature but often not applied; runs counter to reliance on COTS / FOSS. • **Tools**: Software tracing/code path utilization, system/software hardening *Cyber Resiliency:* *Somewhat ready to adopt. Political and operational challenges to applying this principle, given general trends toward multi-use or reusable resources.*	Supports Coordinated Defense (DiD) Supports Privilege Restriction (PM, PUR) Conflicts with Diversity (C3) in conjunction with Redundancy (Replication)	**Recon:** *Degrade* and *Delay*: The adversary must work harder to probe external-facing systems. **Deliver, Control, Execute, Maintain**: *Negate*: The functionality or connectivity can no longer be used by the adversary. *Degrade*: The set of opportunities the adversary can take advantage of is reduced.
Replacement: Replace risky implementations with less-risky implementations.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature but often not applied; runs counter to reliance on COTS / FOSS. • **Process**: Custom development or re-development *Cyber Resiliency:* *Somewhat ready to adopt. Technical challenges with respect to ensuring consistency; economic challenges of applying (i.e., costs of replacement; ongoing management, training and maintenance).*	Supports (DiD) and conflicts with (C&CA) Coordinated Defense Supports Diversity (ADH, DDH)	**Weaponize**: *Negate*: The adversary lacks insight into critical customized components, and thus cannot develop exploits. *Degrade* and *Delay*: The adversary must develop exploits against customized components.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 17. Redundancy

Redundancy: Provide multiple protected instances of critical resources		
Protected Backup and Restore (PB&R): Back up information and software (including configuration data) in a way that protects its confidentiality, integrity, and authenticity, and to restore it in case of disruption or destruction.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Contingency Planning and COOP: Unprotected backup & restore is highly mature and widely used *Cyber Resiliency:* *Ready to adopt. Technical and operational challenges of managing risks during backup and restore activities.* • ***Tools**: Encrypted offsite backup services with integrity controls, monitoring of backup and restore activities*	Supports Adaptive Response Uses Deception (Obfuscation) Uses Diversity (ADH, DDH) Uses Substantiated Integrity (IQC, PT)	**Execute**: *Curtail*: The time during which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. *Recover*: Recovery from the effects of adversary activities is facilitated.
Surplus Capacity (SC): Maintain extra capacity for information storage, processing, and/or communications.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Contingency Planning, Performance: Mature and widely used • **Process**: Capacity planning *Cyber Resiliency:* *Ready to adopt. Technical and operational challenges involve leveraging other techniques effectively, to avoid increasing the attack surface.*	Uses Diversity (ADH, DDH, C3)	**Execute**: *Degrade*: The extent to which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. *Recover*: Recovery from the effects of adversary activities is facilitated.
Replication: Duplicate information and/or functionality in multiple locations and keep it synchronized.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Contingency Planning and COOP, Performance: Mature and widely used. • **Tools**: Hot/warm backups, database pools *Cyber Resiliency:* *Ready to adopt. Technical and operational challenges involve leveraging other techniques effectively, to avoid increasing the attack surface.*	Uses Diversity (ADH, DDH, C3) Supports Dynamic Positioning (DF) Uses Substantiated Integrity (IQC, PT)	**Execute**: *Degrade*: The extent to which the adversary causes mission functions (e.g., data retrieval, processing, communications) to cease or slow is limited. *Recover*: Recovery from the effects of adversary activities is facilitated.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 18. Segmentation / Isolation

Segmentation / Isolation: Define and separate (logically or physically) components on the basis of criticality and trustworthiness (concluded on next page)		
Predefined Segmentation (PS): Define enclaves, segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature and widely used in some environments; runs counter to trends toward converged architectures. • **Tools**: Physically isolated networks (with supporting logical separation), air gaps, VPN, DMZ, management network, management-only systems, sandboxes, virtualization/containers, firewalls, configuration: chroot • **Processes**: Define enclaves or sub-networks within an intranet; isolate an intranet from an extranet, and both from the Internet; separate inbound from outbound traffic, and separate requests from responses • **Standards**: OpenStack *Cyber Resiliency:* *Highly ready to adopt. Technical challenge of ensuring visibility across enclaves; political challenge of applying, given trends toward convergence of technologies and pervasive networking (e.g., Internet of Things).*	Supports Deception (Sim) Supports Privilege Restriction (PBUR) Can complicate Analytic Monitoring (M&DA, SF&A) by limiting visibility	**Recon, Control, Execute, Maintain**: *Contain*: The adversary's activities (e.g., perform network mapping, propagate malware, exfiltrate data or bring down servers) is restricted to the enclave on which the adversary has established a presence. **Deliver**: *Degrade*: The number of possible targets to which malware can easily be propagated is limited to the network segment. **Control, Execute**: *Detect*: Adversary activities involving C3 across network segments that violate policies enforced at barriers between segments are detected. **Control, Execute, Maintain**: *Delay* and *Degrade*: The adversary's ability to perform C3 is delayed or made more difficult, as the adversary must find ways to overcome barriers between network segments.

© 2015 The MITRE Corporation. All Rights Reserved.

Segmentation / Isolation (concluded)		
Dynamic Segmentation / Isolation (DSI): Change the definition of enclaves or protected segments, or isolate resources, while minimizing operational disruption.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber security: Mature and used in some environments; runs counter to trends toward converged architectures. • **Tools**: Virtualization/containers, SDN, firewalls • **Process**: Physically unplugging devices • **Standards**: OpenFlow, OpenStack *Cyber Resiliency:* *Ready to adopt. Technical challenge of ensuring visibility across enclaves; political challenge of applying, given trends toward convergence of technologies and pervasive networking (e.g., Internet of Things); operational challenge of avoiding unintended consequences on mission operations.*	Supports and uses Adaptive Response (DReconfig) Supports Deception (Sim) Supports Privilege Restriction (PBUR) Can complicate Analytic Monitoring (M&DA, SF&A) by limiting visibility	**Recon, Exploit, Control, Execute, Maintain**: *Contain*: The adversary's activities (e.g., observe characteristics of running processes, insert malware into running process, control compromised process, use compromised process to achieve mission objectives, maintain covert presence in running process) are limited to the set of processes or services within a segment (e.g., with a specific set of characteristics or context). **Deliver:** *Delay*: The adversary must find a delivery route into a newly defined enclave. **Execute**: *Recover*: A protected environment is provided, in which mission-essential capabilities can be reconstituted.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 19. Substantiated Integrity

Substantiated Integrity: Ascertain whether critical services, information stores, information streams, and components have been corrupted (concluded on next page)		
Integrity/Quality Checks (IQC): Apply and validate checks of the integrity or quality of information, components, or services.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Correct functionality / data quality: Mature and widely used for many technologies; immature for emerging technologies • **Tools**: Checksums, redundant calculations / validation • **Process**: Check that data conforms to its specified requirements, such as type or range, internal consistency • **Standards**: ISO 8000 Data Quality standards (under development) *Cyber Resiliency:* *Ready to adopt. Technical challenge of integrating with existing technologies; operational challenge of defining SOPs for when integrity / quality checks fail.* • ***Tools**: Tamper-evident technologies, cryptographic seals, trusted boot, attestation* • ***Processes**: Side-channel analysis, chip inspection*	Supports Adaptive Response (DReconf) Uses Analytic Monitoring (M&FA) to enable recovery to trusted state Uses Deception (Obfuscation), which makes adversary fabrication or modification harder Supports Diversity (InfoD) Supports Non-Persistence (NPI) Supports Privilege Restriction Supports Redundancy (PB&R, Replication)	**Deliver**: *Negate*: Malware payloads the adversary tries to deliver (e.g., counterfeit software updates, email attachments) or embed in apparently harmless objects (e.g., documents) are discarded or quarantined before the malware can exploit a vulnerability; adversary's assumption about exploiting the vulnerability are invalidated. *Detect*: The attempted delivery of malware payloads is detected. **Execute**: *Recover*: Contaminated data is removed, restoring mission or control data to a known good state. **Control, Maintain**: *Detect*: The presence of contaminated data or compromised software that the adversary seeks to maintain is detected.
Provenance Tracking (PT): Identify and track the provenance of data, software, and/or hardware elements.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Quality: Maturity varies depending on architectural layer and technology, but generally immature-to-transitional • **Tools**: Non-repudiation using cryptographic certificates/signatures, DBMS implementation of PROV specifications • **Processes**: SCRM, crowd-sourcing of reputational integrity • **Standard**: W3C provenance (PROV) family of specifications, Open Provenance Model (OPM) *Cyber Resiliency:* *Somewhat ready to adopt. Technical challenge of integrating with existing technologies; operational challenge of defining SOPs for when provenance checks fail.*	Supports Adaptive Response (DReconfig, DC) Supports Diversity (InfoD) Supports Privilege Restriction Supports Redundancy (PB&R, Replication)	**Deliver**: *Detect*: The adversary's attempts to deliver compromised data, software, or hardware are detected.

© 2015 The MITRE Corporation. All Rights Reserved.

Substantiated Integrity (concluded)		
Behavior Validation (BV): Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Dependability: Maturity varies depending on technology; adoption lags technical maturity. • **Tools**: Quality assurance, automated testing frameworks, fault injection • **Processes**: Analysis of behavior and trends; Red teaming *Cyber Resiliency:* *Somewhat ready to adopt. Technical challenge of integrating with existing technologies; operational challenge of defining SOPs for when behavior validation checks fail.* • ***Tools**: Anomaly detection, Byzantine quorum systems*	Supports Analytic Monitoring (M&DA) Supports Dynamic Representation (DM&P)	**Control, Execute, Maintain**: *Detect*: The presence of adversary-controlled processes is detected by peer cooperating processes. *Curtail*: Adversary-controlled processes are isolated or terminated by peer cooperating processes.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 20. Unpredictability

Unpredictability: Make changes randomly or unpredictably (concluded on next page)		
Temporal Unpredictability: Change behavior or state at times that are determined randomly or by complex functions.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Conventional security: Immature with regards to use for ICT, somewhat mature for physical defenses. • **Tools**: Pseudo-random number generators (integrated with other approaches) *Cyber Resiliency:* *Challenging to adopt. Technical challenges of integrating with existing technologies, avoiding unintended consequences.* • ***Processes**: Periodic forced shutdown and restart; periodic exercise of COOP*	Can be used in conjunction with Adaptive Response, Analytic Monitoring, Deception, Diversity, Dynamic Positioning, Non-Persistence, Privilege Restriction, and Segmentation / Isolation.	**Reconnaissance**: *Delay*: The unpredictable nature of the of the placement of defenses should cause the adversary to be more cautious and thus delay them getting an accurate view of the defender. **Exploit**: *Delay*: The inability to accurately time the defender's actions (e.g., when they will patch or upgrade out of cycle) delays the adversary's ability to exploit vulnerabilities. **Control:** *Delay*: The unpredictable timing of the deployment of defenses and sensors delays the adversary's ability to determine which future resources to target w/o being detected. *Detect*: The unpredictable timing of the defenses increases the likelihood that some advances will be detected. **Execute:** *Delay*: The inability to determine with confidence when defenses will be engaged/changed could cause the adversary to act more cautiously (slower) to ensure maximum effect of their attack. *Detect*: The unpredictable timing of placement of sensors and changes to defenses increase the chance that some of the attacks will be detected prematurely. **Maintain:** *Detect*: The unpredictable timing of placement of sensors and changes to defenses increases the chance that the long term activity of the adversary will be detected.

© 2015 The MITRE Corporation. All Rights Reserved.

Unpredictability (concluded)		
Contextual Unpredictability: Change behavior or state in ways that are determined randomly or by complex functions.		
Assessment & Examples	**Potential Interactions**	**Potential Effects on Adversary Activities**
Cyber Resiliency: *Challenging to adopt. Technical challenges of integrating with existing technologies, avoiding unintended consequences.* • ***Tools**: Functions that use system observations in the generation process* • ***Processes**: Integration of randomness (e.g., throws of dice) into operator / defender activities; random challenge / response*	Can be used in conjunction with Adaptive Response, Analytic Monitoring, Deception, Diversity, Dynamic Positioning, Non-Persistence, Privilege Restriction, and Segmentation / Isolation.	**Reconnaissance**: *Delay*: The unpredictable nature of the of the placement of defenses should cause the adversary to be more cautious and thus delay them getting an accurate view of the defender **Weaponize:** *Delay*: Because the triggering mechanisms of defenses may be based on random or complex functions, the adversary may be forced to be more cautious in their weaponry development to maximize effectiveness. **Deliver:** *Detect*: Changes in the algorithms of sensors and security mechanisms (e.g., conditions that detonations chambers or honeyclients may apply) increase the chance that delivery of malware may be detected. **Control:** *Detect*: Changing the sensors based on some random or contextual factors increases the chance that the adversary's lateral movement may be detected.

© 2015 The MITRE Corporation. All Rights Reserved.

Appendix B Supporting Definitions and Summaries

This appendix provides a summary of the ways that the cyber techniques could interact, based on the details presented in Appendix A. It also provides supporting definitions of potential effects on adversary activities at different stages in the cyber attack lifecycle, as well as of levels of maturity and ease of adoption.

B.1 Maturity and Ease of Adoption

Maturity consists of (1) functionality being integrated into commercial off-the-shelf (COTS) products, Government off-the-shelf (GOTS) solutions, or free and open source software (FOSS), (2) practices or processes being defined and broadly adopted, and ultimately (3) automation of those practices. With respect to functionality, technologies can be assessed in terms of technical readiness, for example by using Technology Readiness Levels (TRLs) [9]. However, using the functionality to achieve established objectives involves the definition of processes (and supporting governance structures) and practices (e.g., standard operating procedures (SOPs), playbooks). Documentation of processes and practices is part of maturing a technology or class of technologies. Finally, as roles for highly trained operational staff become harder to fill, automation of established practices is increasingly important. Because most approaches build on technologies and processes originally created for reasons other than cyber resiliency, maturity is assessed in the original context.

Table 21 identifies five levels of relative maturity.

Table 21. Levels of Maturity

Relative Maturity	Description
Highly Mature 5	The technology is available commercially or as GOTS or FOSS. The technology is in common use. Standards of good practice for its use, based on extensive experience, have been documented.
Mature 4	The technology is available commercially or as GOTS or FOSS. Operational experience and guidance have been documented. (Corresponds to TRL 8-9)
Transitional 3	Prototype or proof-of-concept technology is integrated into a representative demonstration or experimental environment or is in limited or experimental operational use. Corresponding processes or practices have been defined, and informally documented. (Corresponds to TRL 6-7)
Immature 2	Prototype or proof-of-concept technology has been developed. Demonstration processes or practices have been defined. (Corresponds to TRL 3-5)
Highly Immature 1	Key concepts and approaches are being explored or developed. (Corresponds to TRL 1-2)

Readiness for adoption for cyber resiliency takes two questions into consideration. First, how much experience exists with applying the technique or approach in a threat-informed environment? Second, to what degree are supporting procedures, operator time, and labor costs (including training) required for the technology to work in a threat-informed environment? Engineering and operations in threat-informed environments[14] tend to be less well-documented or more

[14] Examples of threat-informed environments include organizations that are at Cyber Prep level 3 or above [34], or at the Managed level or above in the B|A|H Cyber Operations Maturity Framework [28].

© 2015 The MITRE Corporation. All Rights Reserved.

labor- and expertise-intensive practices. Therefore, many cyber resiliency approaches currently are at best adoptable with caveats. However, some that are based on cyber security or COOP are more easily applied.

Table 22 identifies five levels of relative readiness for adoption. For each level, criteria for application and usability are identified; at least one of the criteria must be satisfied for an approach to be at that level of readiness. In addition, for each level, typical challenges to adoption are identified. Challenges are characterized using the POET (political (i.e., related to policy and governance), operational, economic, and technical) framework [10]. Additional challenges specific to the representative approaches are identified in the Appendix.

© 2015 The MITRE Corporation. All Rights Reserved.

Table 22. Relative Readiness for Adoption for Cyber Resiliency

Relative Readiness for Adoption	Description
Highly Ready to Adopt 5	Application: Use in a threat-informed environment is considered common practice. Standards of good practice have been documented (e.g., [8]). Usability: Use in a threat-informed environment is considered minimally costly and labor intensive, frequently because use is supported by automation. Typical challenges: Political (e.g., recognition by upper management that the environment needs to be threat-informed); operational (e.g., adaptation of SOPs to use effectively for cyber resilience)
Ready to Adopt 4	Application: Use in a threat-informed environment is growing in some sectors or types of organizations; however, use is considered leading-edge practice. Usability: Use in a threat-informed environment requires a non-trivial amount of effort and/or some degree of specialized expertise and training. Typical challenges: Political (e.g., recognition by upper management that the environment needs to be threat-informed, organizational willingness to push the state of the practice); Operational (e.g., development or modification of SOPs)
Somewhat Ready to Adopt 3	Application: Use in a threat-informed environment has been done for a limited set of organizations, missions, or types of systems. Usability: Use in a threat-informed environment requires considerable effort to develop supporting data or applications. *or* Considerable effort and/or significant skill is required to refine the technology or define supporting processes to ensure effectiveness. Typical challenges: Political (e.g., recognition by upper management that the environment needs to be threat-informed, organizational willingness to push the state of the practice); Operational (e.g., development of SOPs, integration of cyber resilience SOPs with security SOPs); Economic (e.g., commitment of resources); Technical (e.g., technology integration)
Challenging to Adopt *or* Applicable Only in Limited Environments 2	Application: Use in a threat-informed environment has been done in constrained situations (e.g., simulations, sandboxes) on a limited basis. Usability: Use in a threat-informed environment requires significant effort for operations; the technology has a significant procedural aspect to its application. *or* Significant effort and skill (or creativity) are required to refine the technology or define supporting processes to ensure effectiveness. Typical challenges: Political (e.g., recognition by upper management that the environment needs to be threat-informed, organizational willingness to push the state of the art); Operational (e.g., significant development of SOPs, integration of cyber resilience SOPs with security SOPs, significant skill and creativity required to use effectively); Economic (e.g., significant commitment of resources); Technical (e.g., significant technology integration)
Highly Challenging to Adopt 1	Application: Use in a threat-informed environment is largely constrained to paper studies and analysis; some very limited use in a constrained situation (e.g., simulations, sandbox) may be done to support the analysis. Usability: Use in a threat-informed environment has to date been largely procedural; costs of effort and expertise pose a major challenge. Significant effort, skill, and creativity are required to refine the technology or define supporting processes to ensure effectiveness. Typical challenges: Political (e.g., recognition by upper management that the environment needs to be threat-informed, organizational willingness to push the state of the art); Operational (e.g., significant development of SOPs, significant integration of cyber resilience SOPs with security SOPs); Economic (e.g., very significant and hard to estimate commitment of resources); Technical (e.g., significant technology development)

© 2015 The MITRE Corporation. All Rights Reserved.

B.2 Potential Interactions

Table 23 summarizes the potential interactions among cyber resiliency techniques, based on consideration of representative approaches in Appendix A.

Table 23. Potential Interactions Between Cyber Resiliency Techniques

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

Key:

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

© 2015 The MITRE Corporation. All Rights Reserved.

B.3 Effects on Adversary Activities

Table 24 describes the stages of the cyber attack lifecycle.

Table 24. Stages of the Cyber Attack Lifecycle

Stage	Description
Recon	The adversary identifies a target and develops intelligence to inform attack activities. The adversary develops a plan to achieve desired objectives.
Weaponize	The adversary develops or acquires an exploit (e.g., a "0-day"), places it in a form that can be delivered to and executed on the target device, computer, or network.
Deliver	The exploit is delivered to the target system. (e.g., tailored malware is included in a spearphishing email attachment or compromised components inserted in the supply chain are integrated into a target network).
Exploit	The initial attack on the target is executed. (e.g., A vulnerability is exploited, and malware is installed on an initial target system).
Control	The adversary employs mechanisms to manage the initial targets, perform internal reconnaissance, and compromise additional targets.
Execute	The adversary executes the plan and achieves desired objectives (e.g., exfiltration of sensitive information, corruption of mission-critical data, fabrication of mission or business data, degradation or denial of mission-critical services).
Maintain	The adversary ensures a sustained, covert presence on compromised devices, systems, or networks. To do so, the adversary may erase indications of prior presence or activities.

Table 25 identifies types of effects an organization might seek to have on adversary activities.[15] These effects can be achieved by defender actions, as enabled by tools and architectural decisions.

Table 25. Potential Effects on Cyber Adversary Activities

Defender Goal	Definition	Effect
Redirect (includes Deter, Divert, and Deceive)	*Direct adversary activities away from defender-chosen targets.*	*The adversary's efforts cease, or become mis-targeted or misinformed.*
Deter	Discourage the adversary from undertaking further activities, by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve intended effects (e.g., that targets exist).	The adversary ceases or suspends activities.
Divert	Lead the adversary to direct activities away from defender-chosen targets.	The adversary refocuses activities on different targets (e.g., other organizations, defender-chosen alternate targets). The adversary's efforts are wasted.
Deceive	Lead the adversary to believe false information about defended systems, missions, or organizations, or about defender capabilities or TTPs.	The adversary's perception of defenders or defended systems is false. The adversary's efforts are wasted.
Preclude (includes Negate and Preempt)	*Prevent specific adversary efforts from having an effect.*	*The adversary's efforts or resources cannot be applied or are wasted.*

[15] Table 25 updates Table 3 of [21].

© 2015 The MITRE Corporation. All Rights Reserved.

Defender Goal	Definition	Effect
Negate	Invalidate the premises on which the adversary's activity is based	The adversary's efforts are wasted, as the assumption on which the adversary based their attack are no longer valid and as a result the intended effects cannot be achieved.
Preempt	Ensure that the adversary cannot apply resources or perform activities.	The adversary's resources cannot be applied and/or the adversary cannot perform activities (e.g., because resources are destroyed or made inaccessible).
Impede (includes Degrade and Delay)	*Make the adversary work harder or longer to achieve intended effects.*	*The adversary achieves the intended effects, but only by investing more resources or undertaking additional activities.*
Degrade	Decrease the effectiveness of an adversary activity, i.e., the level of impact achieved.	The adversary achieves some but not all of the intended effects, or achieves all intended effects but only after taking additional actions.
Delay	Increase the amount of time needed for an adversary activity to achieve its intended effects.	The adversary achieves the intended effects, but may not achieve them within the intended time period. (The adversary's activities may therefore be exposed to greater risk of detection and analysis.)
Detect	*Identify adversary activities or their effects by discovering or discerning the fact that an adversary activity is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur.*	*The adversary's activities become susceptible to defensive responses.*
Limit (includes Contain, Curtail, Recover, & Expunge)	*Restrict the consequences of adversary efforts by limiting the damage or effects of adversary activities in terms of time, cyber resources, and/or mission impacts.*	*The adversary's effectiveness is limited.*
Contain	Restrict the effects of the adversary activity to a limited set of resources.	The value of the activity to the adversary, in terms of achieving the adversary's goals, is reduced.
Curtail	Limit the duration of an adversary activity.	The time period during which the adversary's activities have their intended effects is limited.
Recover	Roll back adversary gains, particularly with respect to mission impairment.	The adversary fails to retain mission impairment due to recovery of the capability to perform key mission operations.
Expunge	Remove adversary-directed malware, repair corrupted data, or damage an adversary-controlled resource so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.	The adversary loses a capability for some period of time.
Expose (includes Analyze and Publicize)	*Remove the advantages of stealth from the adversary by developing and sharing threat intelligence.*	*The adversary loses advantages, as defenders are better prepared.*
Analyze	Understand the adversary better, based on analysis of adversary activities, including the artifacts (e.g., malware) and effects associated with those activities and correlation of activity-specific observations with observations from other activities (as feasible).	The adversary loses the advantages of uncertainty, confusion, and doubt; the defender can recognize adversary TTPs.

© 2015 The MITRE Corporation. All Rights Reserved.

Defender Goal	Definition	Effect
Publicize	Increase awareness of adversary characteristics and behavior across the stakeholder community (e.g., across all CSIRTs that support a given sector, which might be expected to be attacked by the same actor(s)).	The adversary loses the advantage of surprise and possible deniability; the adversary's ability to compromise one organization's systems to attack another organization is impeded.

© 2015 The MITRE Corporation. All Rights Reserved.