Cyber Resiliency Engineering Framework (CREF)

Richard Graubart

RDG@MITRE.ORG

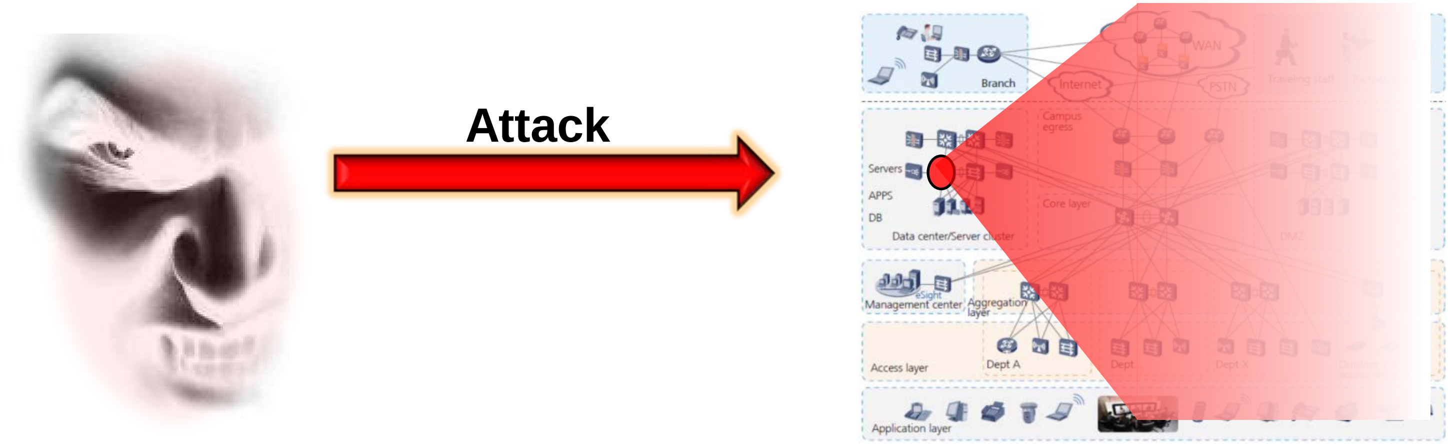
November 17, 2015

MITRE

Cyber Resiliency: The Bottom Line

Why	**The bad guys *will* get in**
What	**Keep the mission going**
How	**Architect for resilience** **Change how we respond to attacks** **Integrate organizational structures**
When	***Now* – build on existing people, processes, and products**

Why Cyber Resiliency is Needed: Hypothetical Attack



Attacker uses zero-day exploit focused on common browser

Malware spreads after 1st host compromised; user accounts compromised

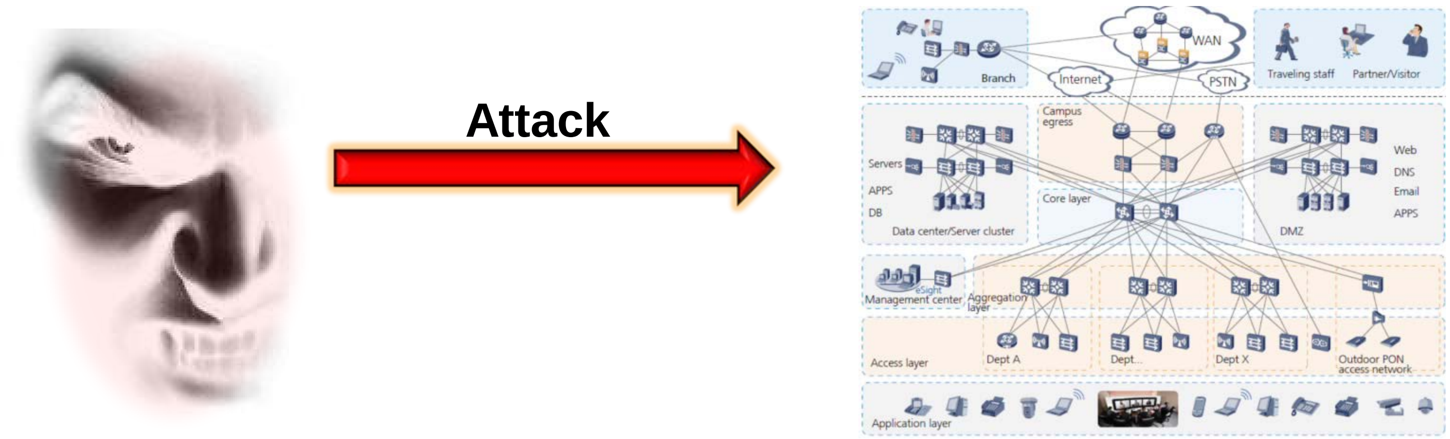
Malware takes advantage of homogeneous browser environment

Static host environment enables attacker to maintain foothold

Traditional defenses (boundary protection and patching) are insufficient!

A new approach is needed: resiliency

Attack Revisited: Cyber Resiliency Applied



Resiliency enables enterprises to complete missions *despite* successful attacks.

- **<u>Diversity</u>: run IE, Chrome, Firefox, etc** → ***Negates adversaries assumptions***
- **<u>Unpredictability</u>: ASLR, randomizing compiler, …** → ***Delays attack progression***
- **<u>Non-persistence</u>: reimaging software periodically** → ***Foothold lost (malware expunged)***
- **<u>Segmentation</u>: distinct internal enclaves** → ***Adversary's advance contained***
- **<u>Deception</u>: detonation chambers, honeynets** → ***Malware detected, adversary diverted***

<u>Knowledge of specific attack not required!</u>

Resilience: Many Definitions, But a Few Key Concepts

- **Many definitions tied to specific scope**
- **Common themes**
  - Disruption, adversity, faults, challenges
  - Need to provide and maintain acceptable capabilities
- **Broad goals**
  - Recover (aka Restore)
  - Withstand (aka Maintain or Continue)
  - Adapt (aka Evolve)
  - Anticipate (aka Prepare)

Scope	Definition
Nation	"The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption" (White House, 2010)
Critical Infrastructure	"Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event." (NIAC, 2010)
Defense Critical Infrastructure	"The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change." (DoD, 2008)
Critical Infrastructure Security and Resilience	"…the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." (White House, 2013)
Organization (Operational Resilience)	"The ability of the organization to achieve its mission even under degraded circumstances" "The organization's ability to adapt to risk that affects its core operational capacities. Operational resilience is an emergent property of effective operational risk management, supported and enabled by activities such as security and business continuity. A subset of enterprise resilience, operational resilience focuses on the organization's ability to manage operational risk, whereas enterprise resilience encompasses additional areas of risk such as business risk and credit risk." (CERT Program, 2010)
Network	"The ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation." (Sterbenz, et al., 2006)
Resiliency Engineering	"The ability to build systems that are able to anticipate and circumvent accidents, survive disruptions through appropriate learning and adaptation, and recover from disruptions by restoring the pre-disruption state as closely as possible." (Mandi, 2009)

Cyber Resiliency: Definition

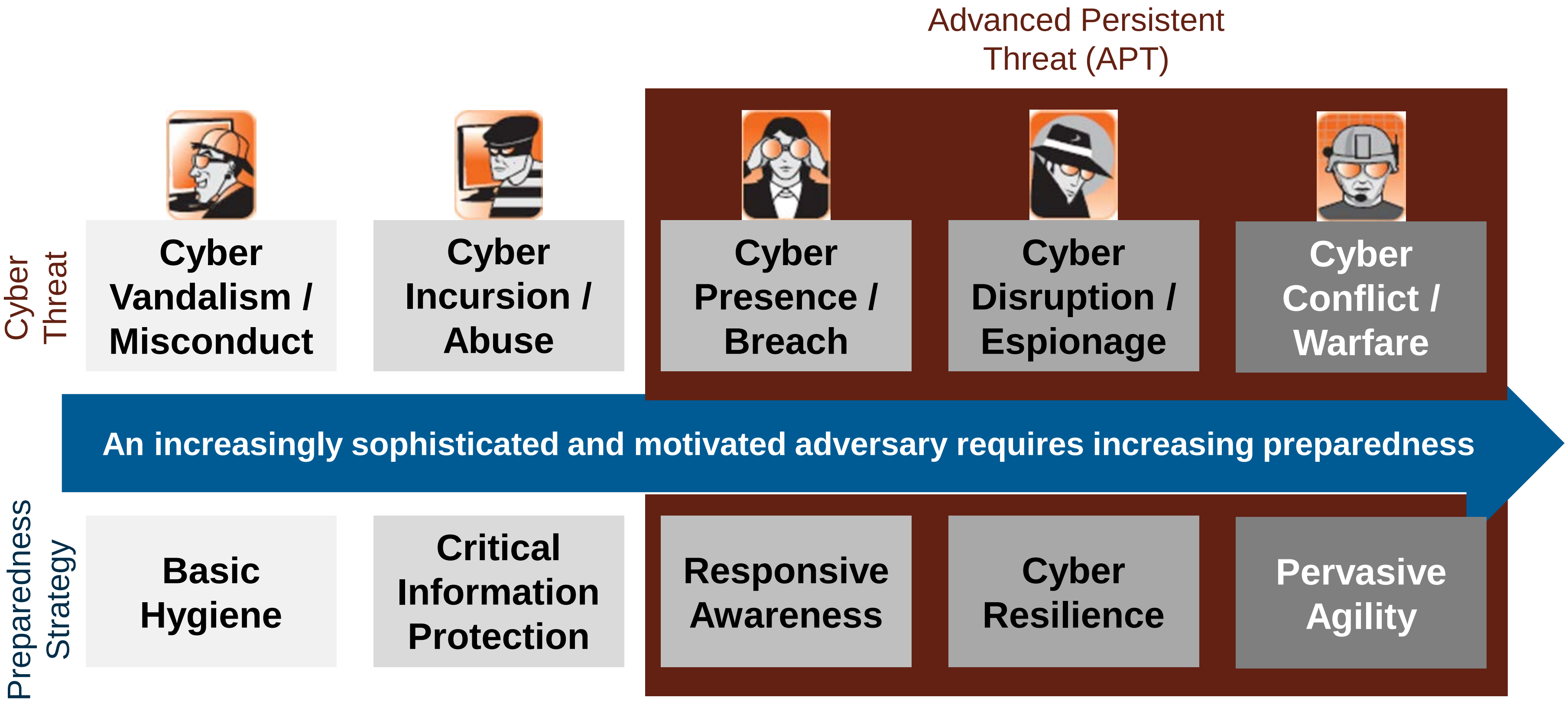
The ability of cyber systems and cyber-dependent missions to

- **anticipate,**
- **continue to operate in the face of,**
- **recover from, and**
- **evolve to better adapt to**

advanced cyber threats

PR-15-1334, Cyber Resiliency Engineering Aid –The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, Deb Bodeau, Rich Graubart, Bill Heinbockel, Ellen Laderman, May 2015; http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

Cyber Resiliency Takes the APT into Consideration



Advanced Persistent Threat (APT)

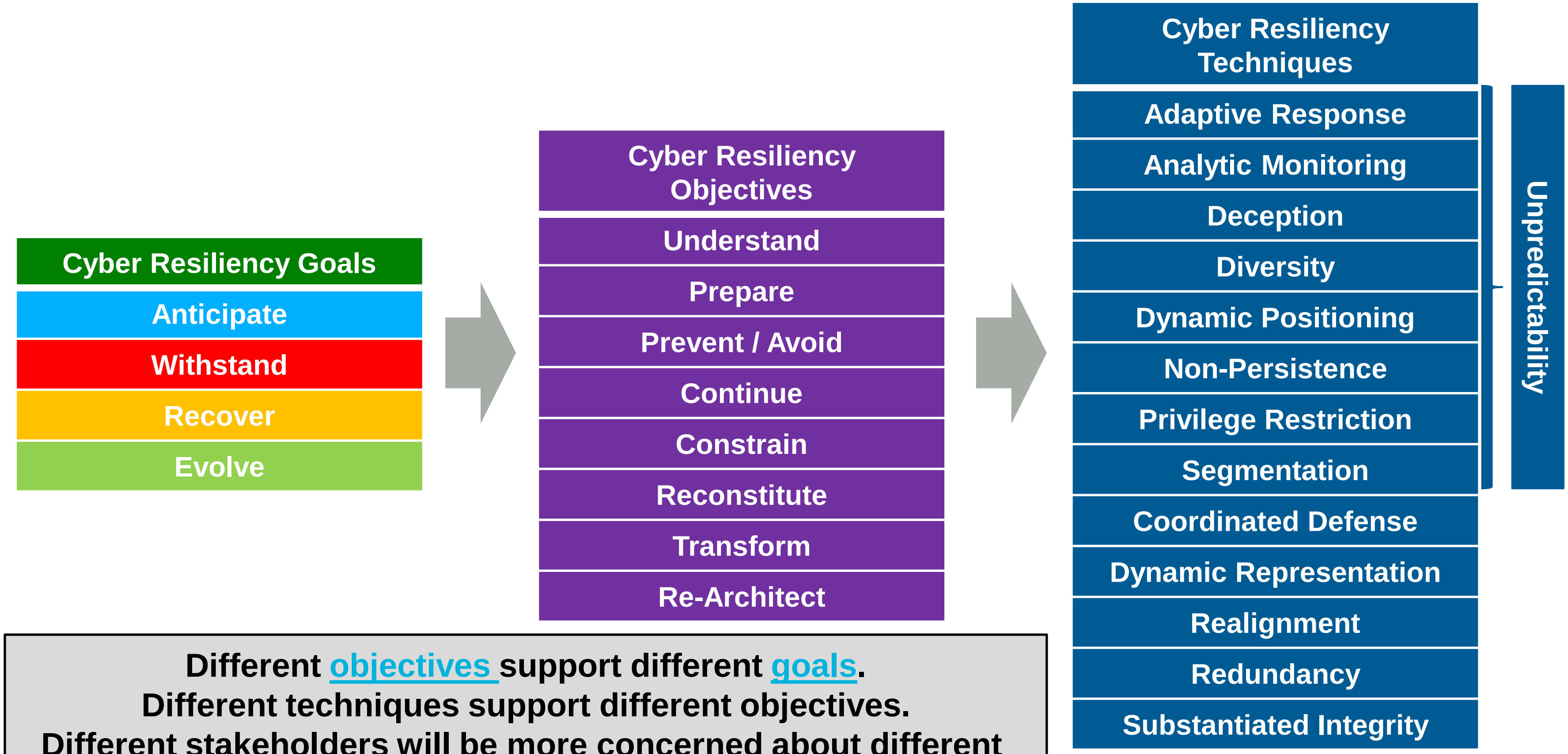
Cyber Threat	Cyber Vandalism / Misconduct	Cyber Incursion / Abuse	Cyber Presence / Breach	Cyber Disruption / Espionage	Cyber Conflict / Warfare
Preparedness Strategy	Basic Hygiene	Critical Information Protection	Responsive Awareness	Cyber Resilience	Pervasive Agility

An increasingly sophisticated and motivated adversary requires increasing preparedness

APT disrupts traditional resiliency (non-cyber) assumptions:

- **Stealthy, embedded APT => multi-occurrence events**
- **Intelligent adversary => attack evolves in response to defender actions**

Cyber Resiliency Engineering Framework (CREF): Mapping the Landscape



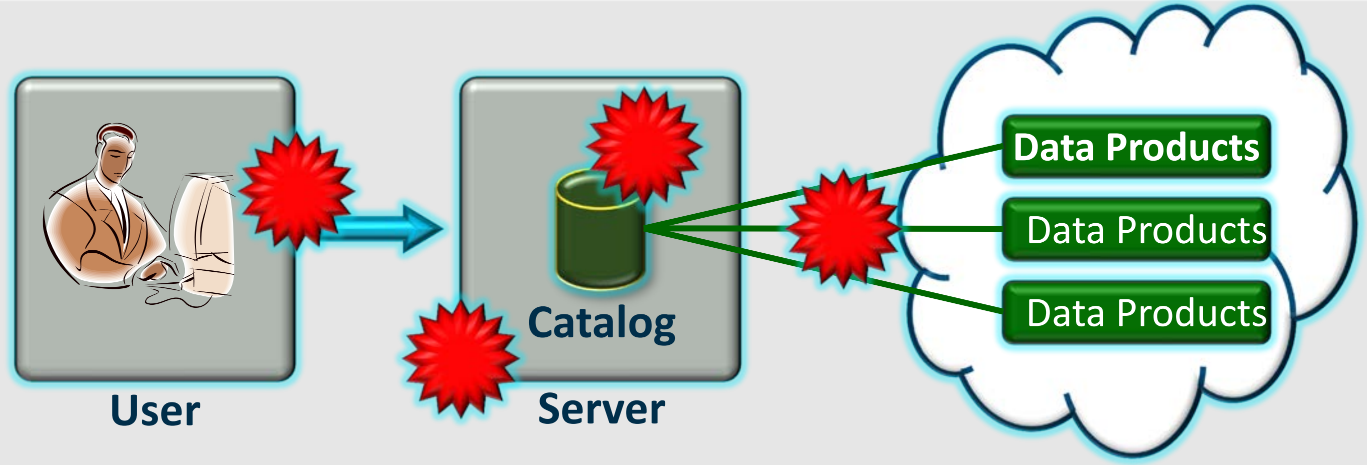
Cyber Resiliency Goals
- Anticipate
- Withstand
- Recover
- Evolve

Cyber Resiliency Objectives
- Understand
- Prepare
- Prevent / Avoid
- Continue
- Constrain
- Reconstitute
- Transform
- Re-Architect

Cyber Resiliency Techniques
- Adaptive Response
- Analytic Monitoring
- Deception
- Diversity
- Dynamic Positioning
- Non-Persistence
- Privilege Restriction
- Segmentation
- Coordinated Defense
- Dynamic Representation
- Realignment
- Redundancy
- Substantiated Integrity

**Different objectives support different goals.
Different techniques support different objectives.
Different stakeholders will be more concerned about different goals & objectives.
Techniques vary in maturity, applicability to architectural layers, and suitability to operational environments – no system can (or should) apply them all.**

Framework – Example



Goal	Objective	Technique	Technology	800-53
Withstand	Constrain	Deception	Deception network	SC-30 (4)
		Segmentation	Hardware trusted path	SC-11
		Privilege Restriction	Dual Authorization	AC-3 (2)
Recover	Reconstitute	Redundancy	Distributed DBMS	SC-36
		Adaptive Response	Alt. Security Mech.	CP-13
	Continue	Substantiated Integrity	Crypto bindings	SI-7 (6)

Engineering Considerations for Selecting Techniques to Apply

- **Neither desirable nor feasible to apply all cyber resiliency techniques to an architecture**
  - Limited resources
  - Legacy components / interoperability with legacy
  - Implementation of some techniques makes implementations of others more difficult
- **Take the Advanced Persistent Threat into consideration**
  - Apply techniques to affect adversary activities throughout the cyber attack lifecycle
- **As feasible leverage existing capabilities, developed for other purposes (e.g., performance, stability, security)**

Factors to Considerations in Selecting Resiliency Techniques

- Maturity and Application of Techniques
- Time Frame
- Political, Operational, Economic, and Technical Factors
- Environmental Considerations
- Cyber Resiliency Effects on Adversary

Cyber Resilience: The Bottom Line

Why

The bad guys *will* get in

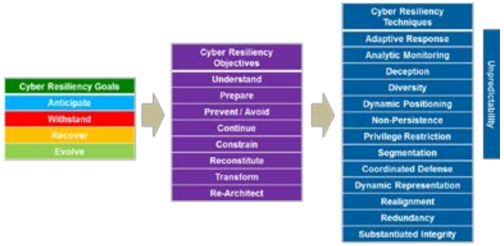
→ Critical Missions Fail When Attacked!

What

Keep the mission going

Provide resilience of critical cyber resources, mission, business process or organization in the face of cyber threats

How



Cyber Resiliency Goals
- Anticipate
- Withstand
- Recover
- Evolve

Cyber Resiliency Objectives
- Understand
- Prepare
- Prevent / Avoid
- Continue
- Constrain
- Reconstitute
- Transform
- Re-Architect

Cyber Resiliency Techniques
- Adaptive Response
- Analytic Monitoring
- Deception
- Diversity
- Dynamic Positioning
- Non-Persistence
- Privilege Restriction
- Segmentation
- Coordinated Defense
- Dynamic Representation
- Realignment
- Redundancy
- Substantiated Integrity

Unpredictability

Architect for resilience

Change how we respond to attacks

Integrate organizational structures

- Adopt the Cyber Resiliency Engineering Framework
- Design, build, and integrate cyber resiliency techniques into systems
- Define policies & practices to promote resilience

Cyber Resilience: The Bottom Line

When

Now! Apply cyber resiliency via the CREF lens throughout the system lifecycle and across enterprise architecture, policy and operational procedures

Result

Critical missions complete successfully despite effective cyber attacks against underlying technology

Conclusion

- **Cyber Resiliency Engineering Framework serves as an analytic tool to identify appropriate cyber resiliency mitigations to counter the APT**
  - Use Goals and Objectives to orient to the resiliency landscape
  - Use Objectives to establish relative priorities
- **Use Cyber Resiliency Techniques in a threat-informed way to identify “quick wins” and move toward a more resilient future**
  - Select and apply techniques judiciously, not desirable or practical to apply all techniques
  - Resiliency controls (~150) supporting cyber resiliency techniques are already in NIST 800-53, can be used to enhance existing baselines

MITRE Publically Released Cyber Resiliency Publications

- PR10-3301 Building Secure, Resilient Architectures for Cyber Mission Assurance, Harriet Goldman, 2010; http://www.mitre.org/sites/default/files/pdf/10_3301.pdf
- PR11-4436, Cyber Resiliency Engineering Framework Version 1.0, Deb Bodeau, Rich Graubart, September 2011; http://www.mitre.org/sites/default/files/pdf/11_4436.pdf
- PR11-3023; Resiliency Research Snapshot, June 2011; Rich Pietravalle, Dan Lanz; June 2011; http://www.mitre.org/sites/default/files/pdf/11_3023.pdf
- 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
- PR12-3795.Cyber Resiliency Assessment: Overview of the Architectural Assessment Process, June 2013; http://www.mitre.org/sites/default/files/publications/cyber-engineering.pdf
- PR12-3795, Cyber Resiliency Assessment, Enabling Architectural Improvement, May 2013: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf
- PR12-2226, Cyber Resiliency Metrics version 1.0, Rev 1.0; Deb Bodeau, Rich Graubart, Len LaPadula, Peter Kertzner, Arnie Rosenthal, Jay Brennan; April 2012; https://register.mitre.org/sr/12_2226.pdf
- PR12-4821; Second Annual Secure and Resilient Cyber Architectures Workshop; https://registerdev1.mitre.org/sr/2012/2012_resiliency_workshop_report.pdf
- PR13-4210, Third Annual Secure and Resilient Cyber Architectures Workshop; http://www.mitre.org/sites/default/files/publications/13-4210.pdf
- PR13-3513; Resiliency techniques for systems-of-systems: Deb Bodeau, John Brtis, Richard Graubart, John Salwen, September 2013; http://www.mitre.org/sites/default/files/publications/13-3513-ResiliencyTechniques_0.pdf
- PR13-4047; Cyber Resiliency and NIST 800-53 Rev 4 Controls, September 2013, Deb Bodeau, Rich Graubart; http://www.mitre.org/sites/default/files/publications/13-4047.pdf
- PR13-4173, Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment, Deb Bodeau, Rich Graubart, November 2013; http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf
- PR13-4174, Mapping the Cyber Terrain, Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility; Deb Bodeau, Rich Graubart, Bill Heinbockel, November 2013; http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf
- PR 14-0500, A Measurable Definition of Resiliency Using 'Mission Risk' as Resiliency as a Metric", Musman, S, et. al., February, 2014: https://www.mitre.org/sites/default/files/publications/resiliency-mission-risk-14-0500.pdf
- PR 15 0704, Fourth Annual Secure and Resilient Cyber Architectures Invitational; http://www.mitre.org/cyberworkshop
- PR-15-1334, Cyber Resiliency Engineering Aid –The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, Deb Bodeau, Rich Graubart, Bill Heinbockel, Ellen Laderman, May 2015; http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

?

Backup Slides

Cyber Resiliency Goals

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

Cyber Resiliency Objectives

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 successful execution of 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	🟨 🟩

Cyber Resiliency Objectives Provide Basis for Defining Cyber Resiliency MOEs

Objective	Representative Examples of MOEs
Understand	• Time to map network, % of network mapped • Time to assess health of network nodes, % assessed
Prepare	• % mission functions for which criticality is known • Time between ingest of threat intelligence and development or selection of cyber course of action
Prevent / Avoid	• % of network nodes, services with up-to-date patches & configuration settings
Continue	• % of mission-critical functions operating at acceptable level
Constrain	• Time between alert and successful change to network configuration
Reconstitute	• % of mission-essential functions restored to acceptable level of functioning within [specified] time
Transform	• % of contingency plans that consider cyber attack as a source or complicating factor
Re-Architect	• % of mission-critical components that have been designed, implemented, and configured to address advanced threats

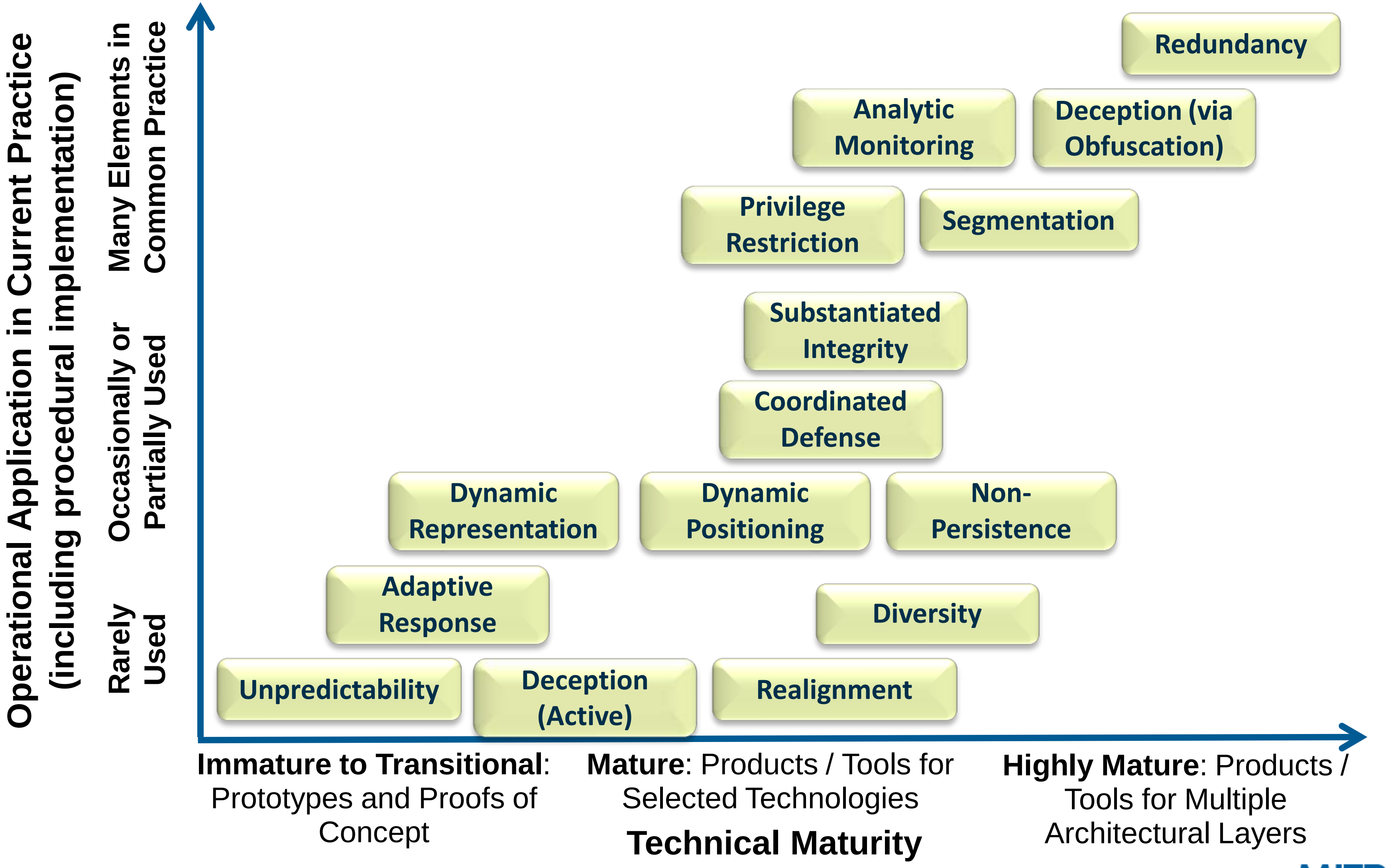
Cyber Resiliency Techniques (1 of 2)

Adaptive Response	Implement nimble cyber courses of action (CCoAs) to manage risks
Analytic Monitoring	Gather, fuse, and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities, and damage
Coordinated Defense	Manage multiple, distinct mechanisms in a non-disruptive or complementary way
Deception	Mislead, confuse, or hide critical assets from, the adversary
Diversity	Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities
Dynamic Positioning	Distribute and dynamically relocate functionality or assets
Dynamic Representation	Construct and maintain current representations of mission posture in light of cyber events and cyber courses of action

Cyber Resiliency Techniques (2 of 2)

Non-Persistence	Generate and retain resources as needed or for a limited time
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
Realignment	Align cyber resources with core aspects of mission/business functions
Redundancy	Provide multiple protected instances of critical resources
Segmentation	Define and separate (logically or physically) components on the basis of criticality and trustworthiness
Substantiated Integrity	Ascertain whether critical services, information stores, information streams, and components have been corrupted
Unpredictability	Make changes randomly or unpredictably

Cyber Resiliency Techniques From a Practice and Maturity Perspective



Operational Application in Current Practice (including procedural implementation)

Many Elements in Common Practice

Occasionally or Partially Used

Rarely Used

Redundancy

Analytic Monitoring

Deception (via Obfuscation)

Privilege Restriction

Segmentation

Substantiated Integrity

Coordinated Defense

Dynamic Representation

Dynamic Positioning

Non-Persistence

Adaptive Response

Diversity

Unpredictability

Deception (Active)

Realignment

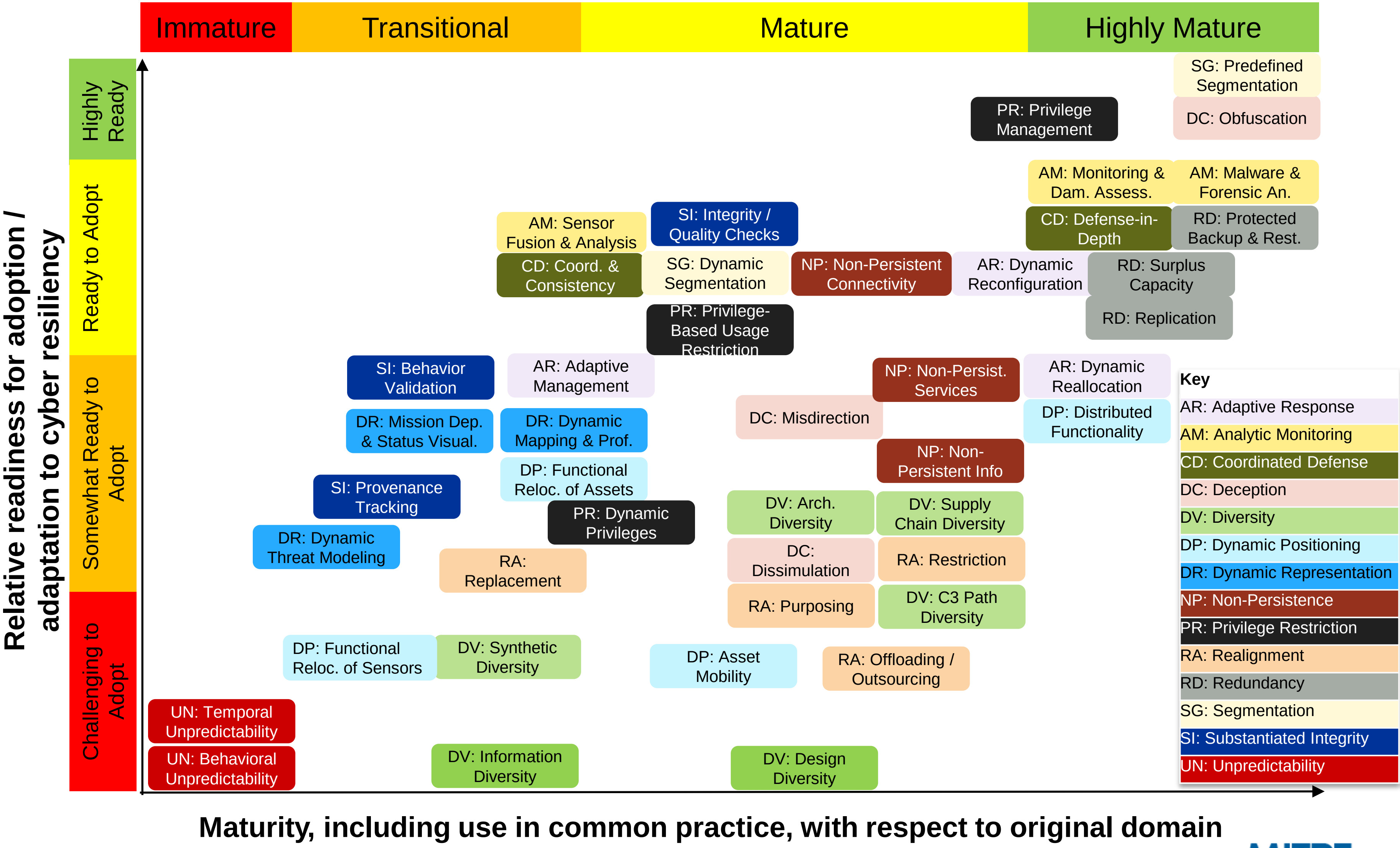
Immature to Transitional: Prototypes and Proofs of Concept

Mature: Products / Tools for Selected Technologies

Highly Mature: Products / Tools for Multiple Architectural Layers

Technical Maturity

Approaches Vary in Relative Maturity and Relative Readiness for Adoption / Adaptation to Cyber Resiliency



Immature

Transitional

Mature

Highly Mature

Relative readiness for adoption / adaptation to cyber resiliency

Highly Ready

Ready to Adopt

Somewhat Ready to Adopt

Challenging to Adopt

Maturity, including use in common practice, with respect to original domain

SG: Predefined Segmentation

PR: Privilege Management

DC: Obfuscation

AM: Monitoring & Dam. Assess.

AM: Malware & Forensic An.

SI: Integrity / Quality Checks

AM: Sensor Fusion & Analysis

CD: Defense-in-Depth

RD: Protected Backup & Rest.

CD: Coord. & Consistency

SG: Dynamic Segmentation

NP: Non-Persistent Connectivity

AR: Dynamic Reconfiguration

RD: Surplus Capacity

PR: Privilege-Based Usage Restriction

RD: Replication

SI: Behavior Validation

AR: Adaptive Management

NP: Non-Persist. Services

AR: Dynamic Reallocation

DC: Misdirection

DR: Mission Dep. & Status Visual.

DR: Dynamic Mapping & Prof.

DP: Distributed Functionality

NP: Non-Persistent Info

DP: Functional Reloc. of Assets

SI: Provenance Tracking

DV: Arch. Diversity

DV: Supply Chain Diversity

PR: Dynamic Privileges

DR: Dynamic Threat Modeling

DC: Dissimulation

RA: Restriction

RA: Replacement

RA: Purposing

DV: C3 Path Diversity

DP: Functional Reloc. of Sensors

DV: Synthetic Diversity

DP: Asset Mobility

RA: Offloading / Outsourcing

UN: Temporal Unpredictability

UN: Behavioral Unpredictability

DV: Information Diversity

DV: Design Diversity

Key

AR: Adaptive Response

AM: Analytic Monitoring

CD: Coordinated Defense

DC: Deception

DV: Diversity

DP: Dynamic Positioning

DR: Dynamic Representation

NP: Non-Persistence

PR: Privilege Restriction

RA: Realignment

RD: Redundancy

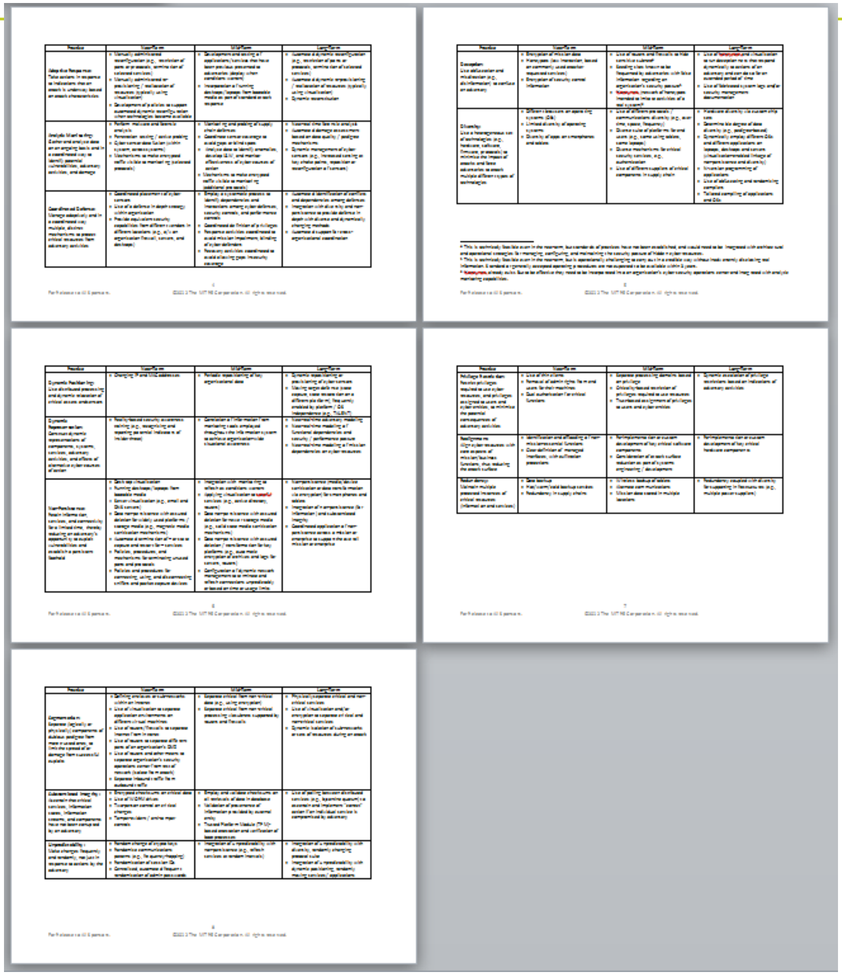
SG: Segmentation

SI: Substantiated Integrity

UN: Unpredictability

Time Frame View of Resiliency Techniques

Examined cyber resiliency techniques from a near, mid and long term perspective

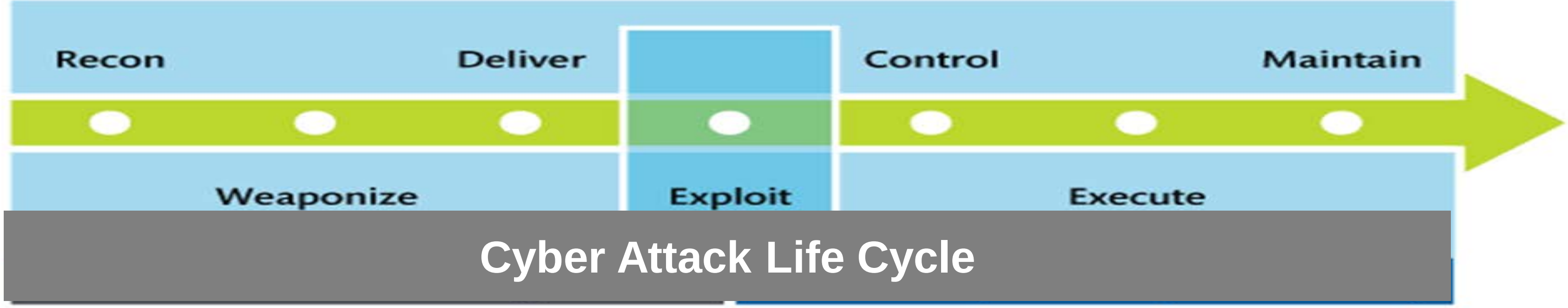


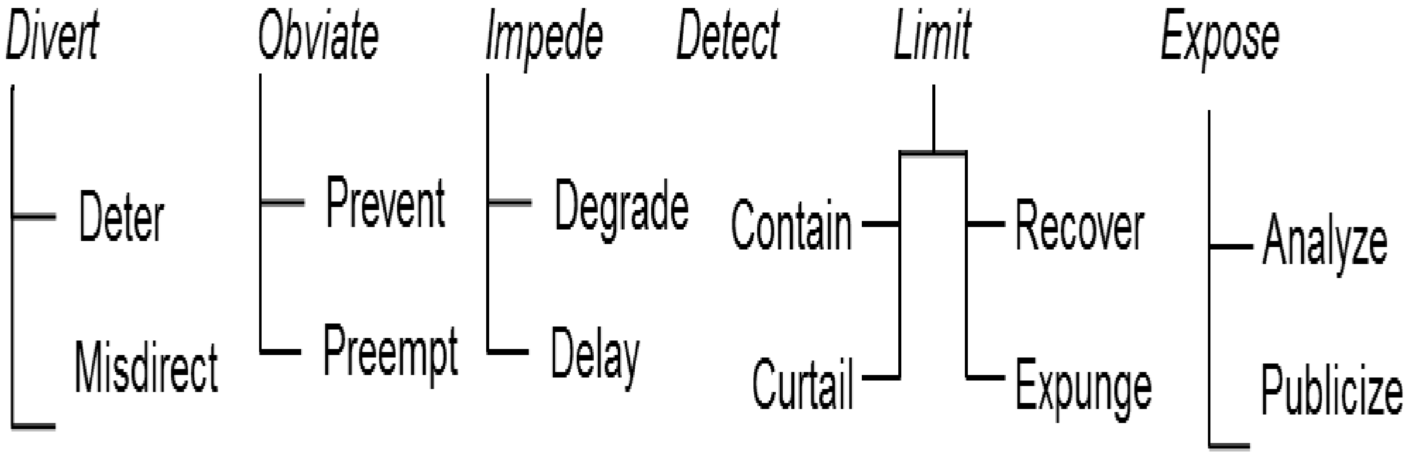
Time Frame Example: Diversity

Use a heterogeneous set of technologies, communications paths, suppliers, and data sources to minimize the impact of attacks and force adversaries to attack multiple different types of technologies

Examples		
Near-Term	Mid-Term	**Long-Term**
• Different browsers on operating systems (OSs) • Limited diversity of operating systems • Diversity of apps on smartphones and tablets	• Use of different protocols / communications diversity (e.g., over time, space, frequency) • Diverse suite of platforms for end users (e.g., some using tablets, some laptops) • Diverse mechanisms for critical security services, e.g., authentication • Use of different suppliers of critical components in supply chain	• Hardware diversity via custom chip sets • Determinable degree of data diversity (e.g., pedigree-based) • Dynamically employ different OSs and different applications on laptops, desktops and servers (virtualization-enabled linkage of non-persistence and diversity) • Use of obfuscating and randomizing compilers • Tailored compiling of applications and OSs

Defender’s Goals wrt Adversary and Cyber Attack Life Cycle

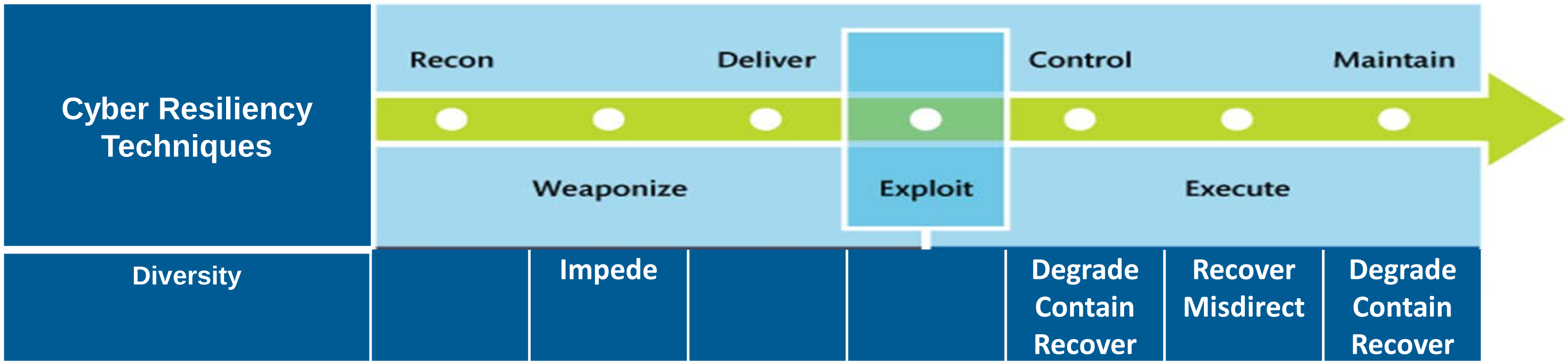




Notional Effects of Cyber Resiliency Techniques on Adversary Activities Across the Cyber Attack Lifecycle

Cyber Resiliency Techniques	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Adaptive Response	X	X	X	X	X	X	X
Analytic Monitoring	X		X	X	X	X	X
Coordinated Defense		X		X	X	X	X
Deception	X	X	X	X	X	X	X
Diversity		X			X	X	X
Dynamic Positioning	X				X	X	X
Dynamic Representation					X	X	X
Non-Persistence				X	X	X	X
Privilege Restriction				X	X	X	X
Realignment		X	X	X	X	X	X
Redundancy						X	
Segmentation	X		X	X	X	X	X
Substantiated Integrity			X		X	X	X
Unpredictability	X				X		

Notional Effect of Diversity on Adversary Across the Cyber Attack LifeCycle



Cyber Resiliency Techniques	Recon	Weaponize	Deliver	Exploit	Control	Execute	Maintain
Diversity		Impede			Degrade Contain Recover	Recover Misdirect	Degrade Contain Recover

POET Framework

Political

- Policies, laws, regulations
- Relationships and commitments
- Governance
- Risks and risk tolerance
- Organizational culture
- Investment strategy

Operational

- Mission priorities
- Mission impacts
- Operational constraints
- Impacts on supporting processes
- Flexibility/agility

Economic

- Costs
- Benefits
- Perceived value
- Incentives

Technical

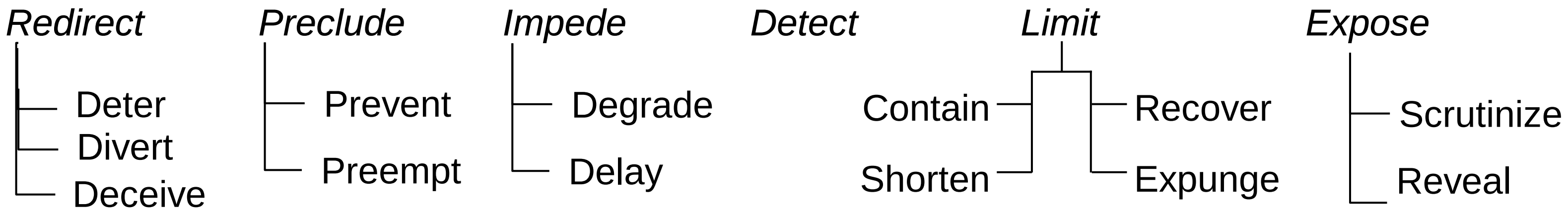
- Standards
- Performance
- Legacy investments
- Interoperability
- Infrastructure

Sample POET Considerations and Restrictions on Scope

Cyber Resiliency Technique	Representative Reasons for Restricting Consideration
Adaptive Response	Liability concerns (e.g., responses that violate SLAs, cause collateral damage)
Analytic Monitoring	Policy concerns related to collecting, aggregating, and retaining data (e.g., sensitivity / classification, privacy)
Coordinated Defense	Governance and CONOPS issues (e.g., overlapping or incompletely defined roles and responsibilities, no clear responsibility for defining cyber courses of action)
Deception	Legal, regulatory, contractual, or policy restrictions Concern for reputation
Diversity	Policy or programmatic restrictions (e.g., organizational commitment to a specific product or product suite) Life-cycle cost of developing or acquiring, operating, and maintaining multiple distinct instances
Dynamic Positioning	Technical limitations due to policy or programmatic restrictions (e.g., organizational commitment to a specific product or product suite which does not accommodate repositioning)
Dynamic Representation	Governance issues / information sharing constraints in the context of systems-of-systems
Non-Persistence	Technical limitations that prevent refresh functions from meeting Quality of Service (QoS) requirements
Privilege Restriction	Governance and CONOPS issues (e.g., inconsistencies or gaps in definitions of roles, responsibilities, and related privileges; operational impetus to share roles)
Realignment	Organizational and cultural impacts (e.g., eliminating functions that personnel are used to employing, impact on morale of relocating staff)
Redundancy	Costs of maintaining multiple, up to date and secure instantiations of data and services
Segmentation	Cost and schedule impacts of re-architecting; cost of additional routers, firewalls
Substantiated Integrity	Cost and schedule impacts (e.g., of incorporating and managing cryptographic checksums on data)
Unpredictability	Operational and cultural issues (e.g., adverse impact on planned activities, adverse impact on staff expectations of how to operate)

Effects of Cyber Resiliency Techniques On Adversary

- **Cyber defenders and system architects can work to achieve a variety of effects on adversary activities**



Redirect

Deter

Divert

Deceive

Preclude

Prevent

Preempt

Impede

Degrade

Delay

Detect

Limit

Contain

Shorten

Recover

Expunge

Expose

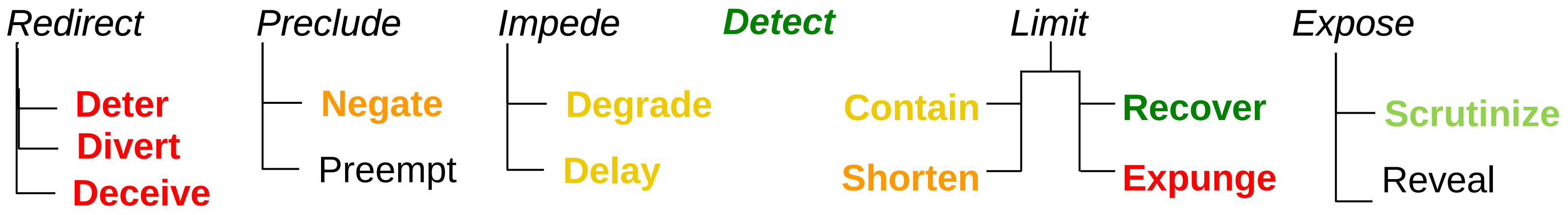
Scrutinize

Reveal

- **Cyber resiliency techniques have different effects**
  - Some techniques have multiple effects
  - Some techniques have only two effects others as much as eight
- **Engineering challenge: Select enough different techniques to have the broadest possible effect on the adversary**

Effects of Cyber Resiliency Techniques On Adversary (2 of 2)

- **In terms of the effects on the adversary the resiliency controls in the baselines can roughly be characterized as**
  - Well addressed: Detect and Recover
  - Addressed: Analyze
  - Partially addressed: Contain, Degrade and Delay
  - Marginally addressed: Curtail, Negate
  - Missing: any control having the effect of Deterring, Deceiving or Diverting the adversary, or Expunging the adversary



Redirect
Deter
Divert
Deceive

Preclude
Negate
Preempt

Impede
Degrade
Delay

Detect

Limit
Contain
Shorten
Recover
Expunge

Expose
Scrutinize
Reveal

Limiting control selection to those controls only in the baselines has the potential of preventing an organization from fully and successfully engaging the adversary and disrupting the adversary's attack.

Vocabulary for Effects on Adversary (1 of 4)

Intended Effect	Definition	Result
Redirect	*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	*Prevent specific adversary efforts from having an effect.*	*The adversary's efforts or resources cannot be applied or are wasted.*
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).

Vocabulary for Effects on Adversary (2 of 4)

Defender Goal	Definition	Effect
Impede	*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.*

Vocabulary for Effects on Adversary (3 of 4)

Defender Goal	Definition	Effect
Limit	*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.

Vocabulary for Effects on Adversary (4 of 4)

Defender Goal	Definition	Effect
Expose	*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.
Publicize / Share	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.