Cyber Risk to Mission: Assessment Methodology

presented to

14th NATO Operations Research and Analysis Conference

"Emerging and Disruptive Technology"

Dr. David S. Alberts
Senior Fellow
Institute for Defense Analyses
Alexandria, Virginia

Chair, NATO SAS-143

Agenda

- Significance of Cyber and Cyber-Enabled Capabilities
- Cyber Risk to Mission
- Managing CRM
- Summary

Prevalence and Significance of Cyber

- Network Centric Warfare signaled the beginning of an era of increasing dependence on ‘Cyber’* to provide the robustly networked force that has dramatically increased force effectiveness
- It is now hard to imagine any military operation that will not depend upon cyber or cyber-enabled capabilities
- Military operational domains now not only the physical domains of Land, Maritime, Air, and Space; but also the virtual domain of Cyberspace
- Given the contested nature of Cyberspace, all missions now multi-domain inherently including the need for Cyberspace Operations

*At the time the term used was ‘information and communications technologies’

Network Centric Warfare[1]

Network Centric Warfare (NCW) is the military response to the opportunities created by the Information Age.

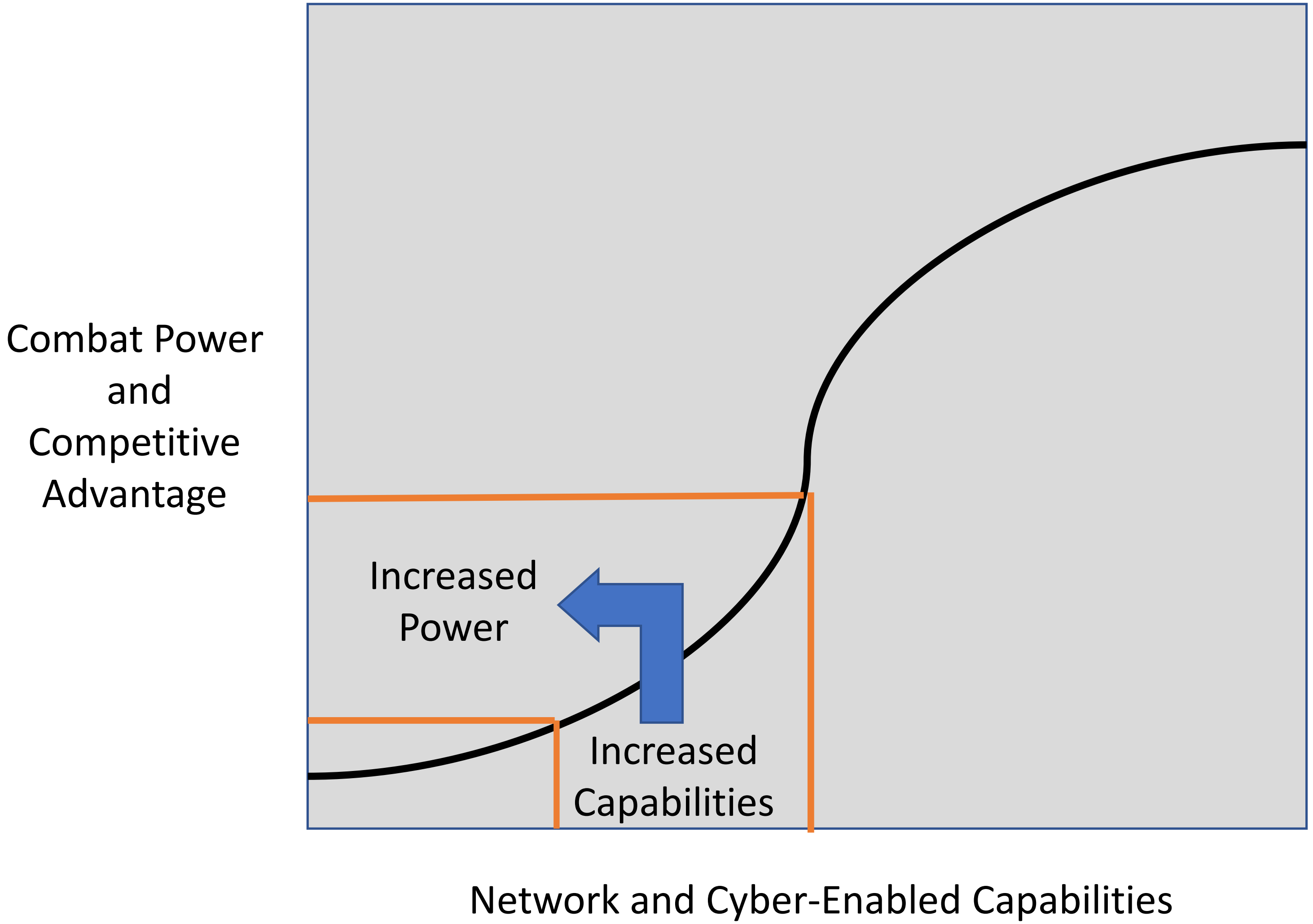
The term network-centric warfare provides a useful shorthand for describing a broad class of approaches to military operations that are enabled by the networking of the force.

“Networking the Force” entails much more than providing connectivity among force components. It involves the development of distributed collaboration processes designed to ensure that all pertinent available information is shared and that all appropriate assets can be brought to bear to by commanders to employ dominant maneuver, precision engagement, full-dimensional protection, and focused logistics.

In recent years, cyber-enabled capabilities have been integrated into our platforms and systems to further leverage the power of information.

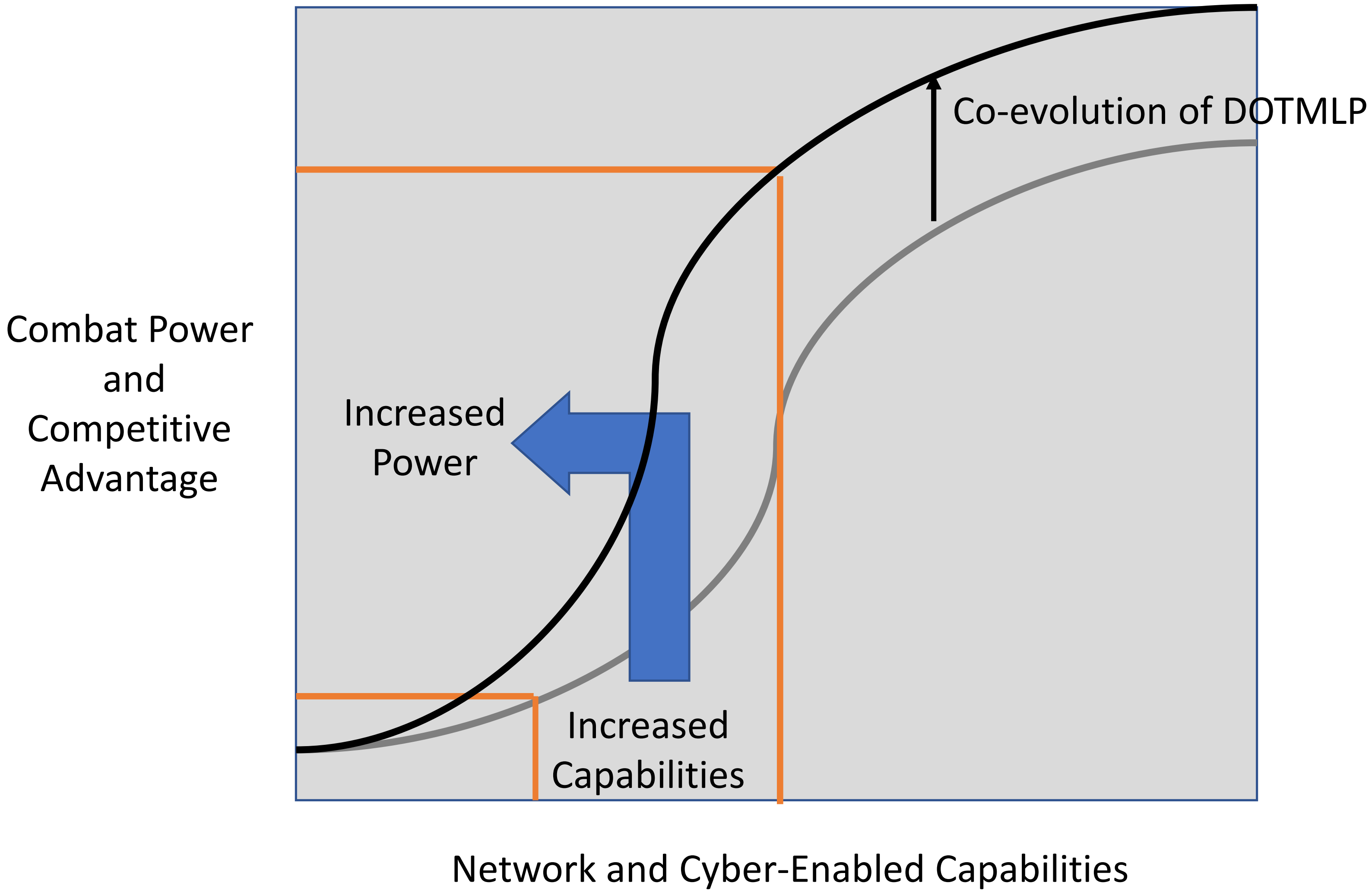
[1] DoD Report to the Congress on Network Centric Warfare, 2001

Power of Cyber and Cyber-Enabled Capabilities



Power of NCW

Co-evolved Doctrine, Organization, C2, Processes = Force Multiplier


Co-evolution of DOTMLP
Combat Power and Competitive Advantage
Increased Power
Increased Capabilities
Network and Cyber-Enabled Capabilities

Cyber Risk to Mission (CRM)

- **Cyber Risk to Mission is present whenever the cyber or cyber-enabled capabilities that a commander depends upon fail to match operational expectations**
- CRM is not about why one's cyber and cyber-enabled capabilities do not satisfy mission requirements; it is about the consequence to mission effectiveness that results from adversely impacted cyber capabilities
- Cyber Risk to Mission is an <u>"All Hazard" </u>Risk; a shortfall in cyber and/or cyber-enabled capability can result from a variety of causes (not only as a result of cyberattacks but could be a result of a kinetic attack or an accident)
- A measure of Cyber Risk to Mission is the likelihood that, as a result of adversely impacted cyber or cyber-enabled capabilities (from any cause), one or more critical mission performance metrics will be less than their minimally acceptable levels for a significant period of time and thus the mission may be unsuccessful

Sources of Cyber Risk

- Threats to the availability, functionality, performance, assurance, security of, and/or our confidence in, our cyber capabilities come from many sources, including the following:

  - Adversary actions
  - Collateral damage from defending against real or imagined adversary actions
  - Characteristics / Complexities of Cyber Capabilities
  - Unanticipated behavior of systems, 'intelligent' software, and decision aids
  - Volatility of the Cyber Environment
  - Collateral damage from cyberattacks on others
  - Mistakes, Accidents, Poor Cyber Hygiene
  - Critical infrastructure Damage, Degradation, Disruption, Denial, Destruction

- These threats are present throughout the competition continuum including below the threshold of armed conflict.

Managing Cyber Risk

- Managing risk to mission requires “actions taken to remediate or mitigate risk or reconstitute capability in the event of loss or degradation”[(1)] [(2)]

  - Remediation - Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified[(1)]

  - Mitigation - Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure[(1)]

  - Another response would be to “Accept” the risk, if deemed appropriate. If accepted, monitor the risk and address when appropriate.

(1) DoDD 3020.40 Mission Assurance replaces Critical infrastructure Directive

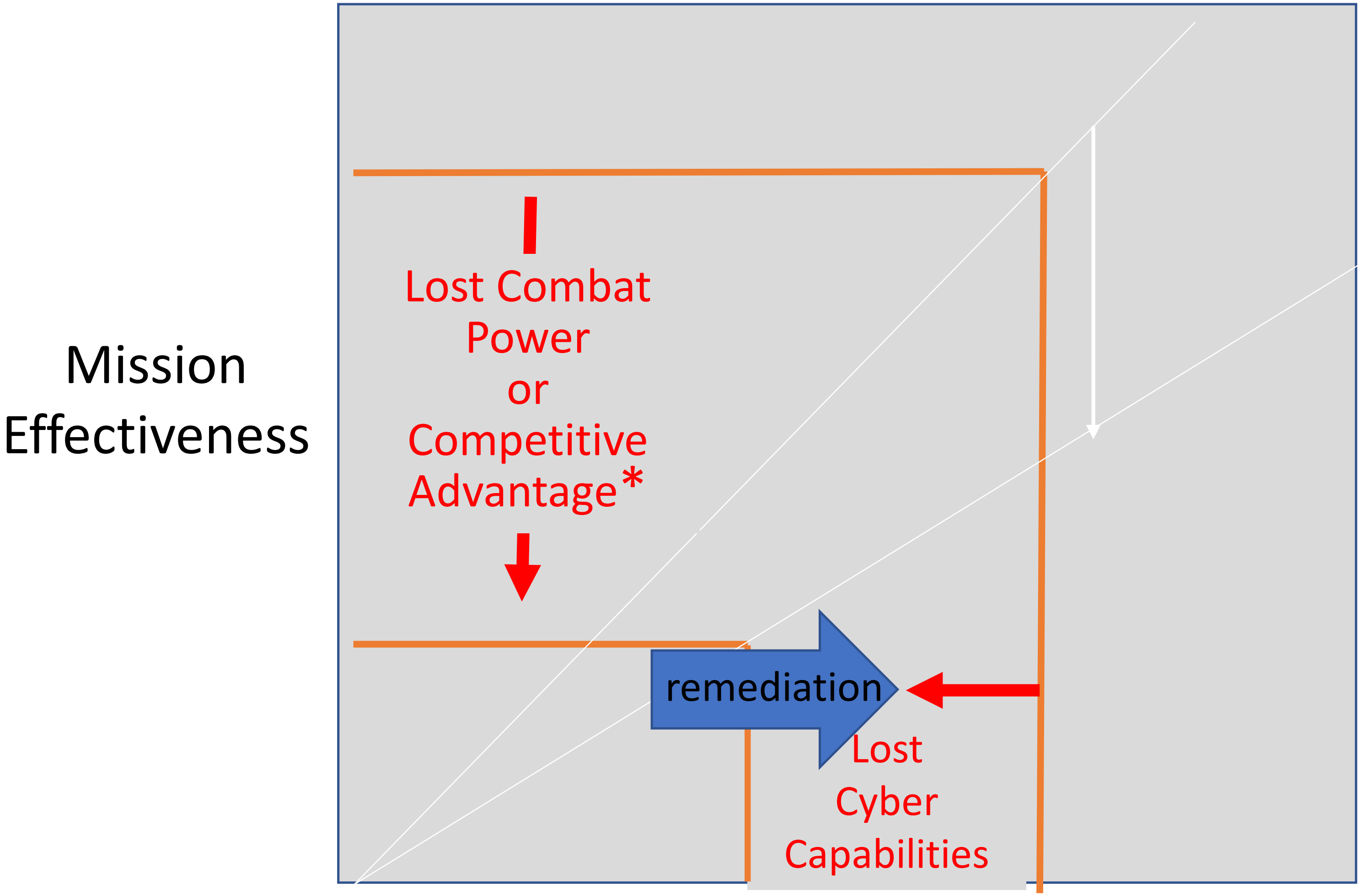
(2) DoDI 3020.45 Mission Assurance Construct, August 14, 2018

Remediation v. Mitigation

Remediation	Mitigation
prevent or reduce the likelihood of a loss	ensure mission succeeds despite a loss
eliminates vulnerabilities and corrects weakness	manages the adverse consequences resulting from a loss
limits the extent and duration of a loss should it occur	limits the extent and duration of the loss after it occurs
actions taken before a loss can occur	actions taken after a loss occurs (or after a warning in anticipation of a loss)
establishes a new baseline	deviates from baseline
seeks to fully satisfy all mission metrics	seeks to hold metrics at or above minimally acceptable levels

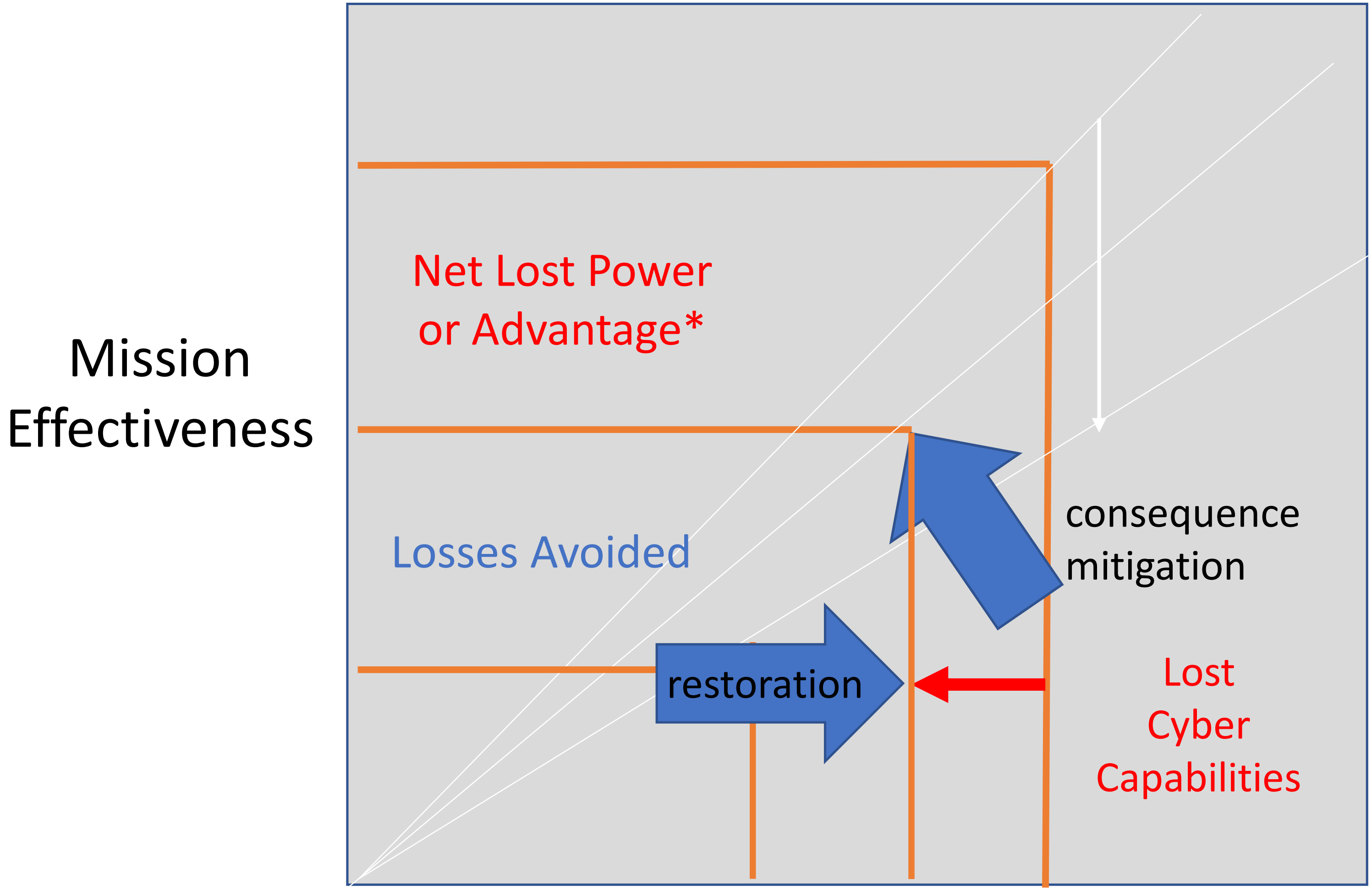
Remediation

Remediation eliminates vulnerabilities and weaknesses that an adversary could have exploited reducing the likelihood of an event that could have an adverse impact on cyber capabilities

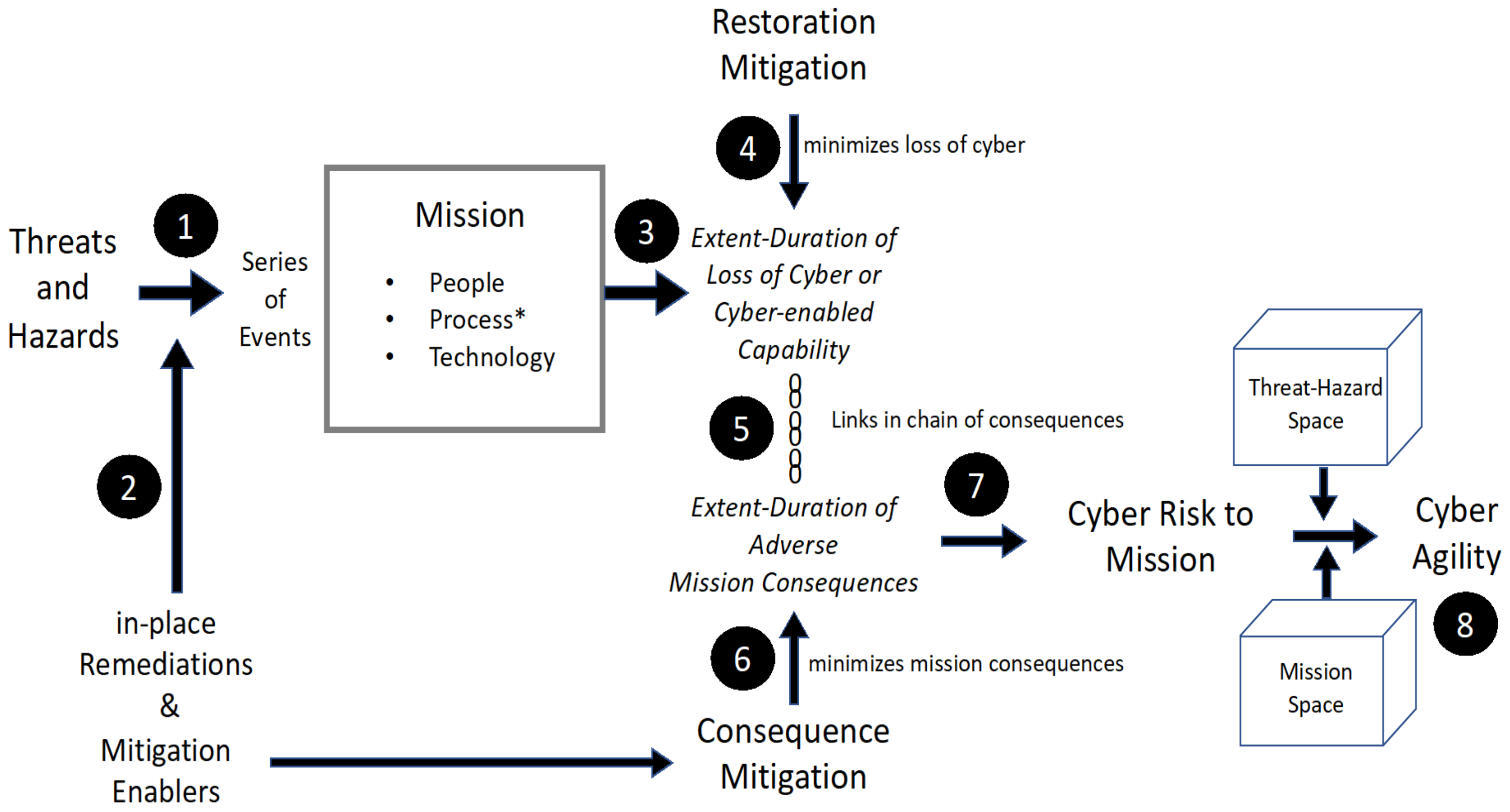


Mitigation

Mitigations eliminate or reduce the consequences of a loss of cyber capabilities



Conceptual Model of CRM



Threats and Hazards

1

Series of Events

2

in-place Remediations & Mitigation Enablers

Mission

- People
- Process*
- Technology

3

Restoration Mitigation

4

minimizes loss of cyber

Extent-Duration of Loss of Cyber or Cyber-enabled Capability

5

Links in chain of consequences

Extent-Duration of Adverse Mission Consequences

6

minimizes mission consequences

Consequence Mitigation

7

Cyber Risk to Mission

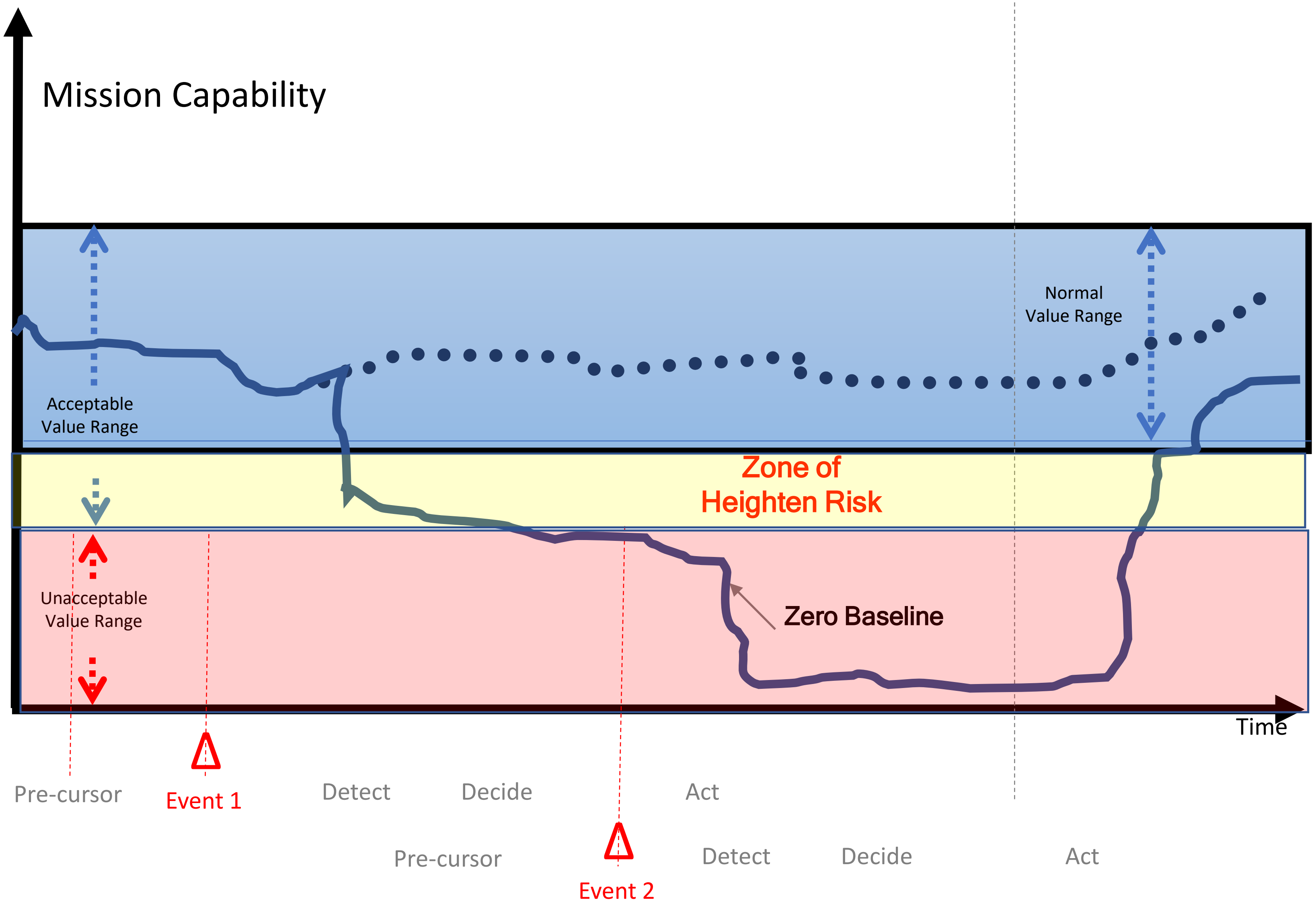
Threat-Hazard Space

Mission Space

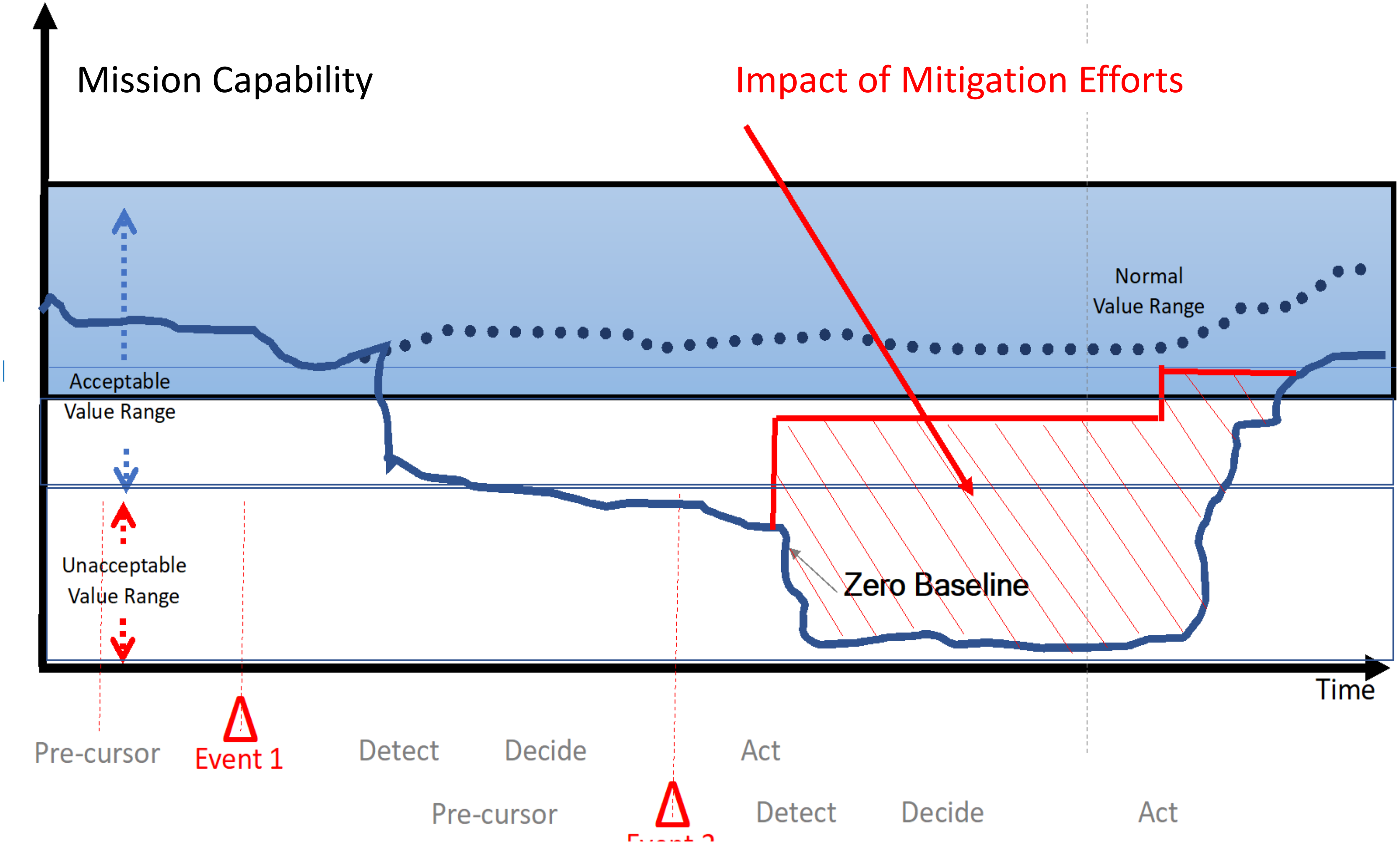
Cyber Agility

8

Cyber Risk to Mission Zones



Impact of Mitigation



Cyber State v. Mission State

	Zero Baseline	with Mitigations
Cyber State	🟥	🟧
Mission State	🟥	🟩

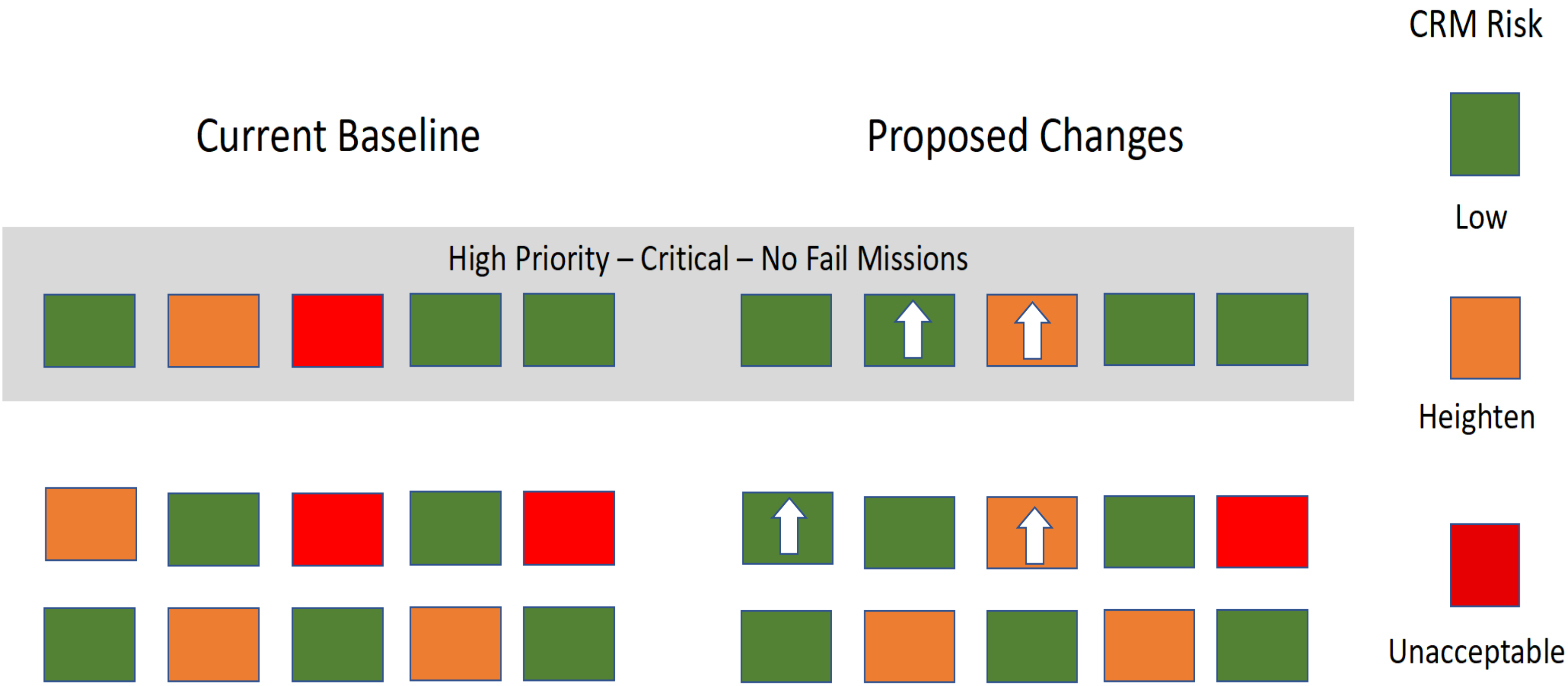
Cyber State
or
Mission State

🟩 Normal

🟧 Significant Loss or Consequences

🟥 Unacceptable

Impact of Changes to Remediation-Mitigation



Current Baseline	Proposed Changes
High Priority – Critical – No Fail Missions	
🟩 🟧 🟥 🟩 🟩	🟩 🟩⬆ 🟧⬆ 🟩 🟩
🟧 🟩 🟥 🟩 🟥	🟩⬆ 🟩 🟧⬆ 🟩 🟥
🟩 🟧 🟩 🟧 🟩	🟩 🟧 🟩 🟧 🟩

CRM Risk

🟩 Low

🟧 Heighten

🟥 Unacceptable

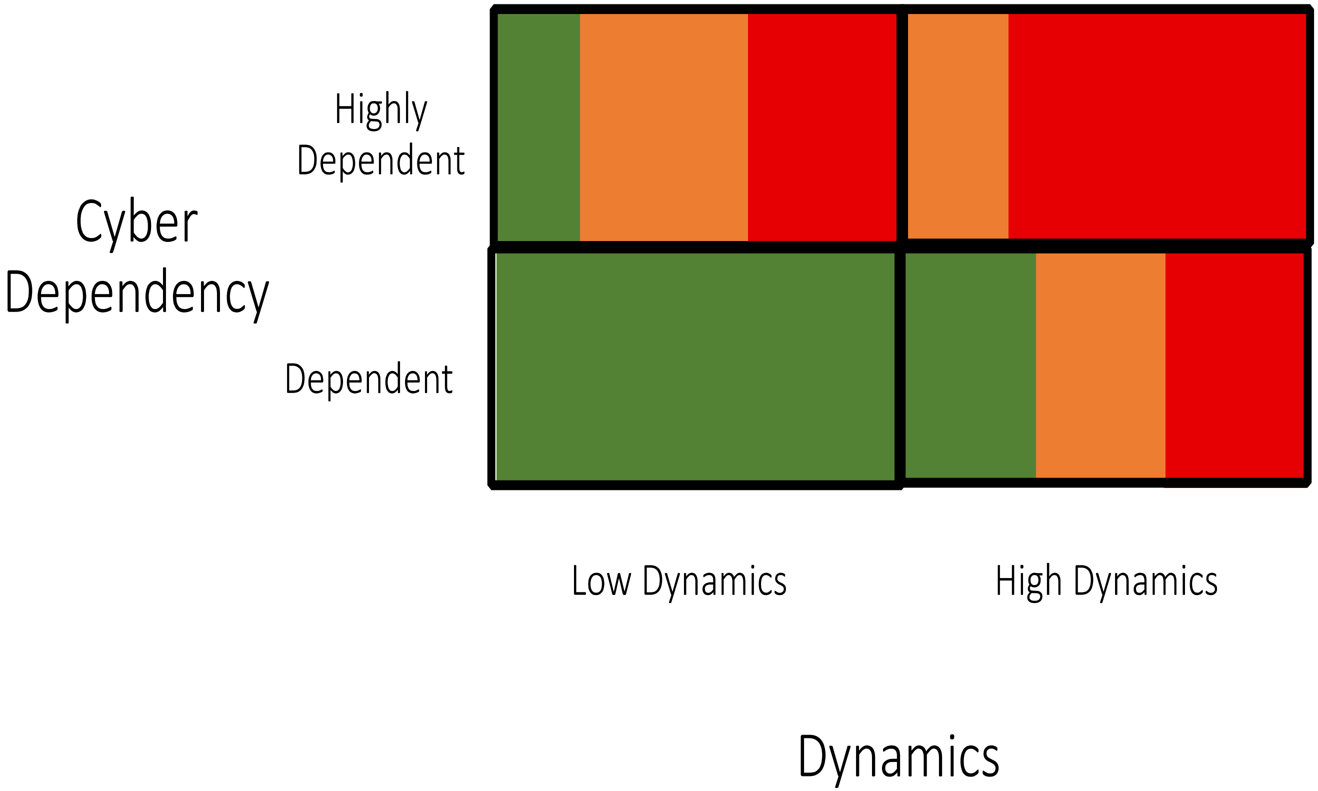
Mission Space

Cyber Dependency

	Low Dynamics	High Dynamics
Highly Dependent	Less Tolerance of Loss	Most Exposure to CRM
Dependent	Least Exposure to CRM	Less Tolerance of Loss with Short Durations

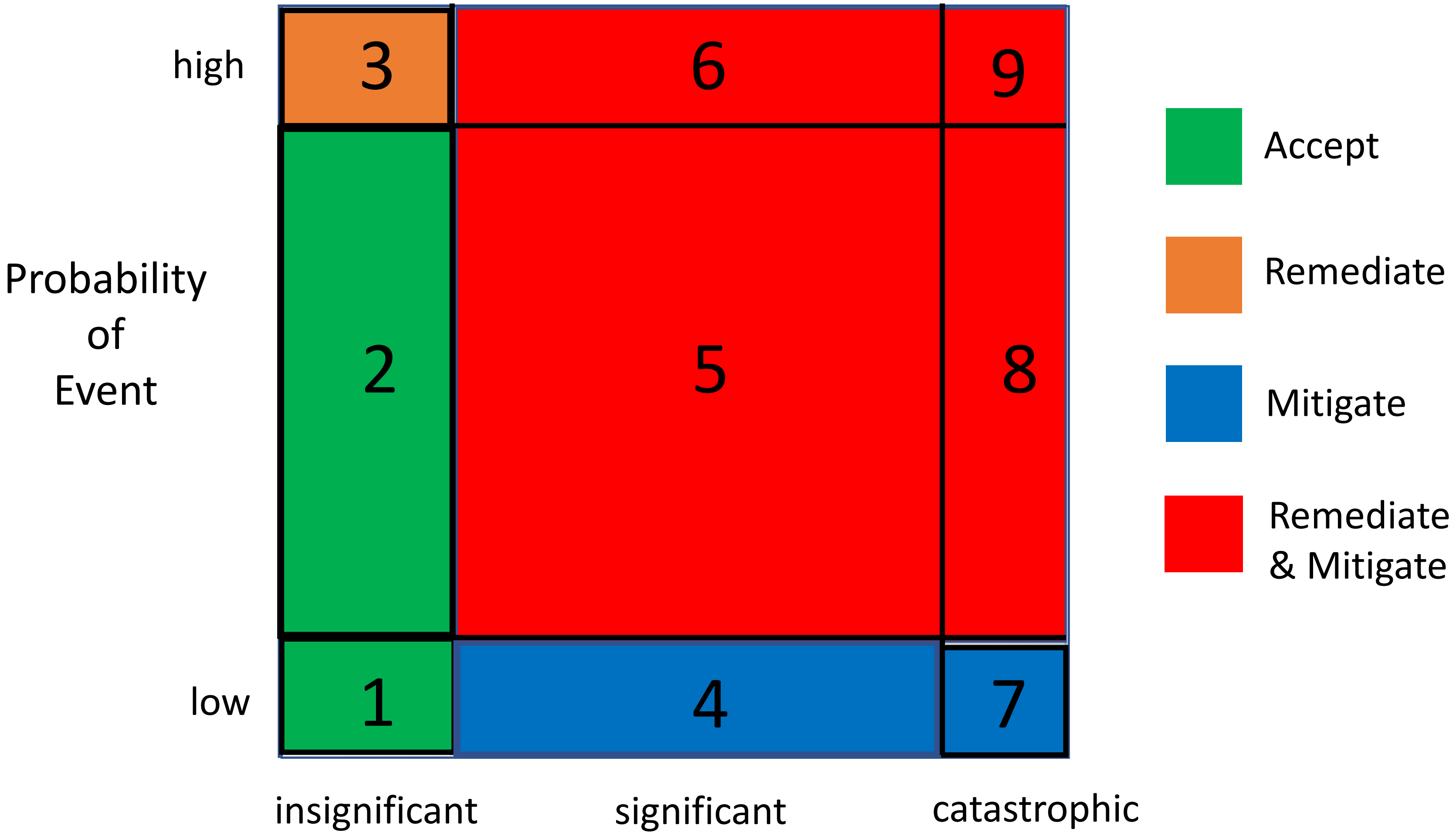
Dynamics

CRM and Regions of the Mission Space



Managing CRM by Type of Risk

Different types of risk are more amenable to different approaches to managing the risk



high

3 6 9

Probability of Event

2 5 8

low

1 4 7

insignificant significant catastrophic

Severity of Adverse Consequences

🟩 Accept

🟧 Remediate

🟦 Mitigate

🟥 Remediate & Mitigate

Summary

- This paper presents a methodology and set of metrics that can be applied to a variety of Cyber Risk to Mission assessments.
  - expands the focus from looking at just losses of cyber capability to the consequences for missions.
  - enables a balanced approach to managing CRM as it provides an opportunity to understand the tradeoffs between remediation and mitigation.
- As with any methodology, its value will depend upon an ability to populate it with credible data
- Given the importance of cyber capabilities and the existence of a contested cyber environment, efforts to better understand CRM are urgently needed