SAND2020-5263PE

Cyber Deterrence and Resilience Strategic Initiative

PRESENTED BY

Eva Uribe and Michael Minner

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Cyber Deterrence and Resilience

Problem: Perfect cyber defense is not possible

“The unfortunately reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States’ ability to defend and adequately strengthen the resilience of its critical infrastructures.”

—Defense Science Board Taskforce on Cyber Deterrence (2017)

Solution: Deterrence of cyber adversaries

Desired end-states:

1. "A continued absence of cyber attacks that constitute a use of force" (No cyber Pearl Harbor)
2. "Reduction in destructive, disruptive, or destabilizing cyber activities against U.S. interests below the threshold of the use of force" (No death by 1000 cuts)
   National Security Council's Recommendations to the President on Deterring Cyber Adversaries (2018)
3. Global strategic stability

What is deterrence?

Deterrence involves creating conditions that dissuade adversaries from taking unwanted actions, because they perceive that the costs exceed the benefits.

- Involves the entire spectrum of government and private sector influence and power.

- **Deterrence by punishment** Perception of unacceptable costs
- **Deterrence by denial** perception of insufficient benefits

Deterrence of cyber adversaries is U.S. policy

National Security Strategy (2017)

Priority actions include "deter and disrupt malicious cyber actors."

National Cyber Strategy (2018)

Strengthen U.S.'s ability "to deter and if necessary punish those who use cyber tools for malicious purposes."

Sec. 1636 of the Defense Authorization Act (2019)

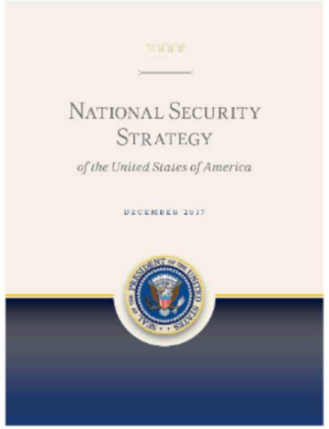
The U.S. should "deter if possible, and respond to when necessary" all cyber attacks and activities that target vital U.S. interests.

2017 Presidential Executive Order mandated high-level cabinet members to deliver a report to the President on the Nation's strategic options for deterring adversaries in cyberspace.

Cyberspace Solarium Commission Report (2020)

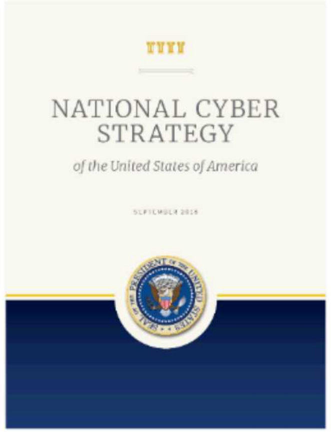
Advocates "a new strategic approach to cybersecurity: layered cyber deterrence

1. Shape behavior (e.g. norm building)
2. Deny benefits (e.g. resilient critical infrastructure)
3. Impose costs (e.g. defend forward)


NATIONAL SECURITY STRATEGY

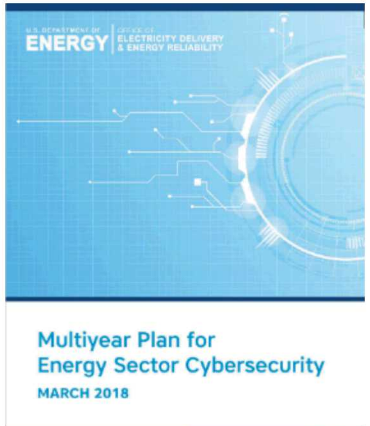
of the United States of America

DECEMBER 2017


NATIONAL CYBER STRATEGY

of the United States of America

SEPTEMBER 2018


U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

Multiyear Plan for Energy Sector Cybersecurity

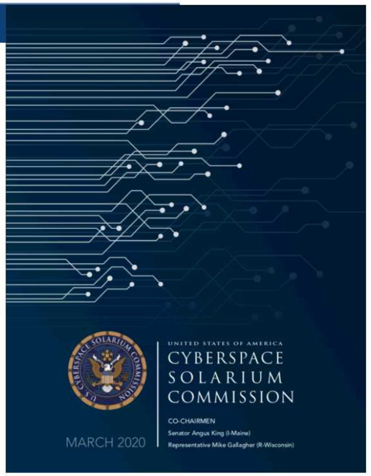
MARCH 2018

U.S. DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY STRATEGY

May 15, 2018

Vision: By 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnerships with other federal and nonfederal entities.


UNITED STATES OF AMERICA

CYBERSPACE SOLARIUM COMMISSION

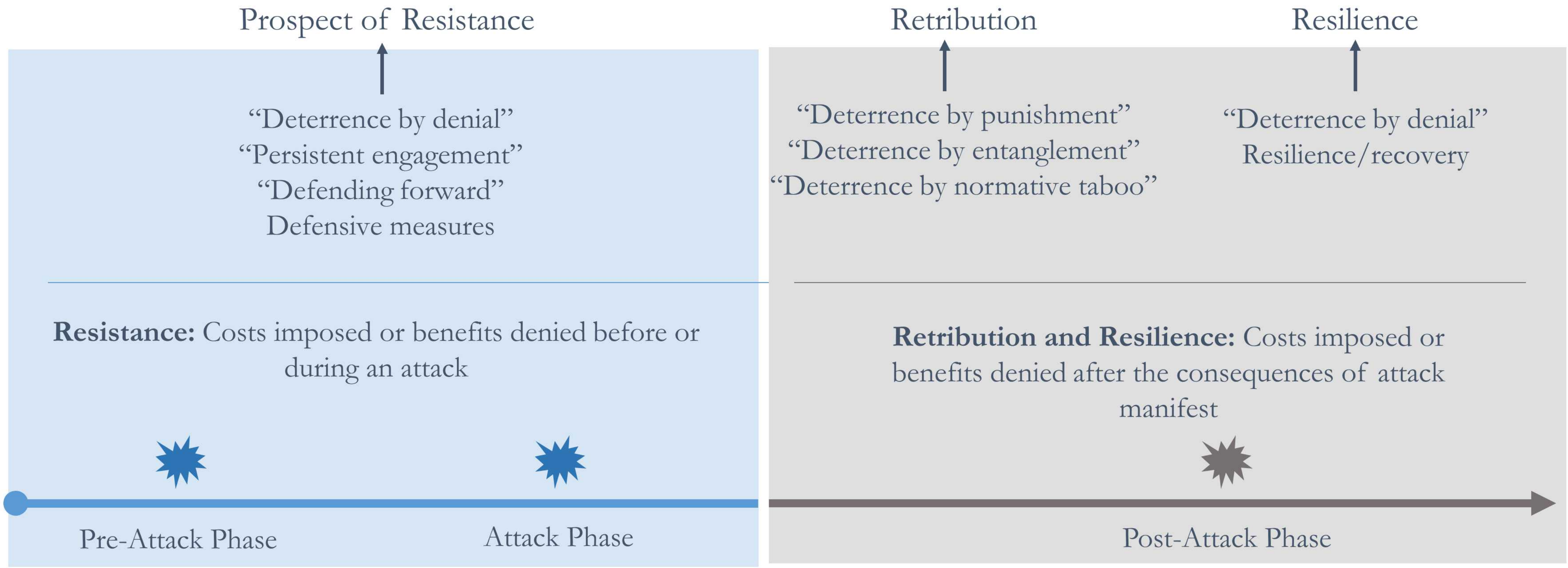
CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)

MARCH 2020

There are many different strategies to deter cyber adversaries



Prospect of Resistance

"Deterrence by denial"
"Persistent engagement"
"Defending forward"
Defensive measures

Resistance: Costs imposed or benefits denied before or during an attack

Retribution

"Deterrence by punishment"
"Deterrence by entanglement"
"Deterrence by normative taboo"

Resilience

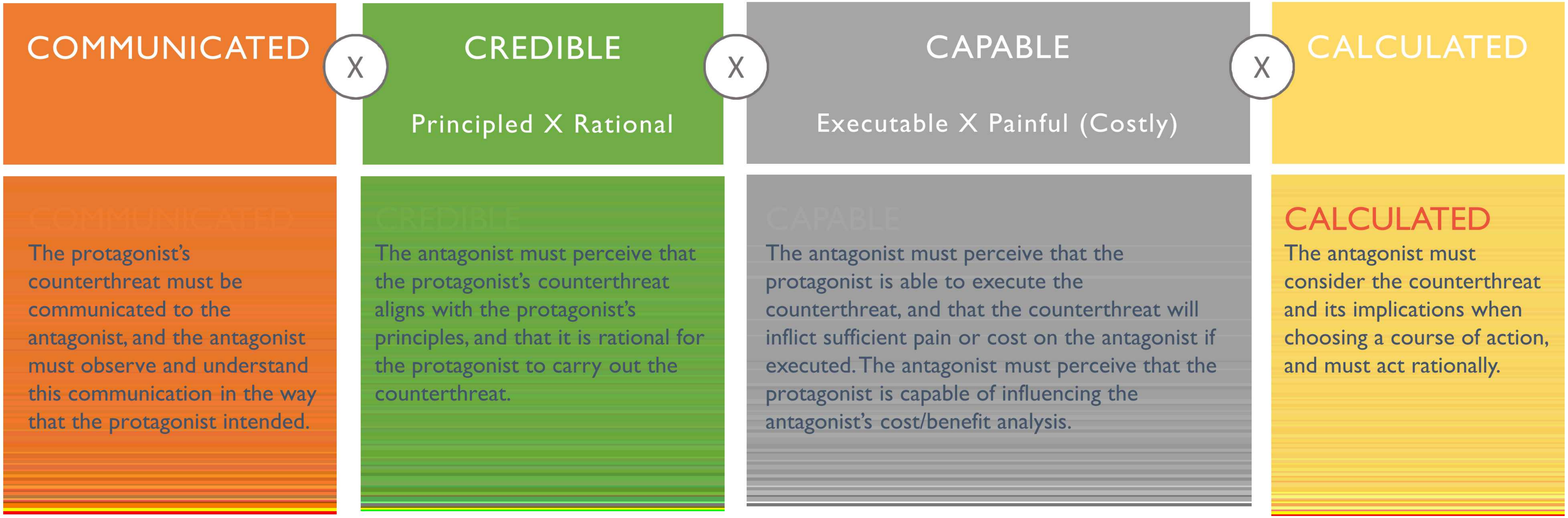
"Deterrence by denial"
Resilience/recovery

Retribution and Resilience: Costs imposed or benefits denied after the consequences of attack manifest

For all deterrence options, capabilities can (and in many cases should) be developed, demonstrated, and communicated well before an attack takes place.
What separates these strategies is the point in time at which costs will be imposed on the adversary.

What makes deterrence counterthreats effective?

A distillation of deterrence theory literature shows how deterrence counterthreats fail. An effective deterrence counterthreat must have all of the following components:



COMMUNICATED X CREDIBLE X CAPABLE X CALCULATED

Principled X Rational

Executable X Painful (Costly)

COMMUNICATED

The protagonist's counterthreat must be communicated to the antagonist, and the antagonist must observe and understand this communication in the way that the protagonist intended.

CREDIBLE

The antagonist must perceive that the protagonist's counterthreat aligns with the protagonist's principles, and that it is rational for the protagonist to carry out the counterthreat.

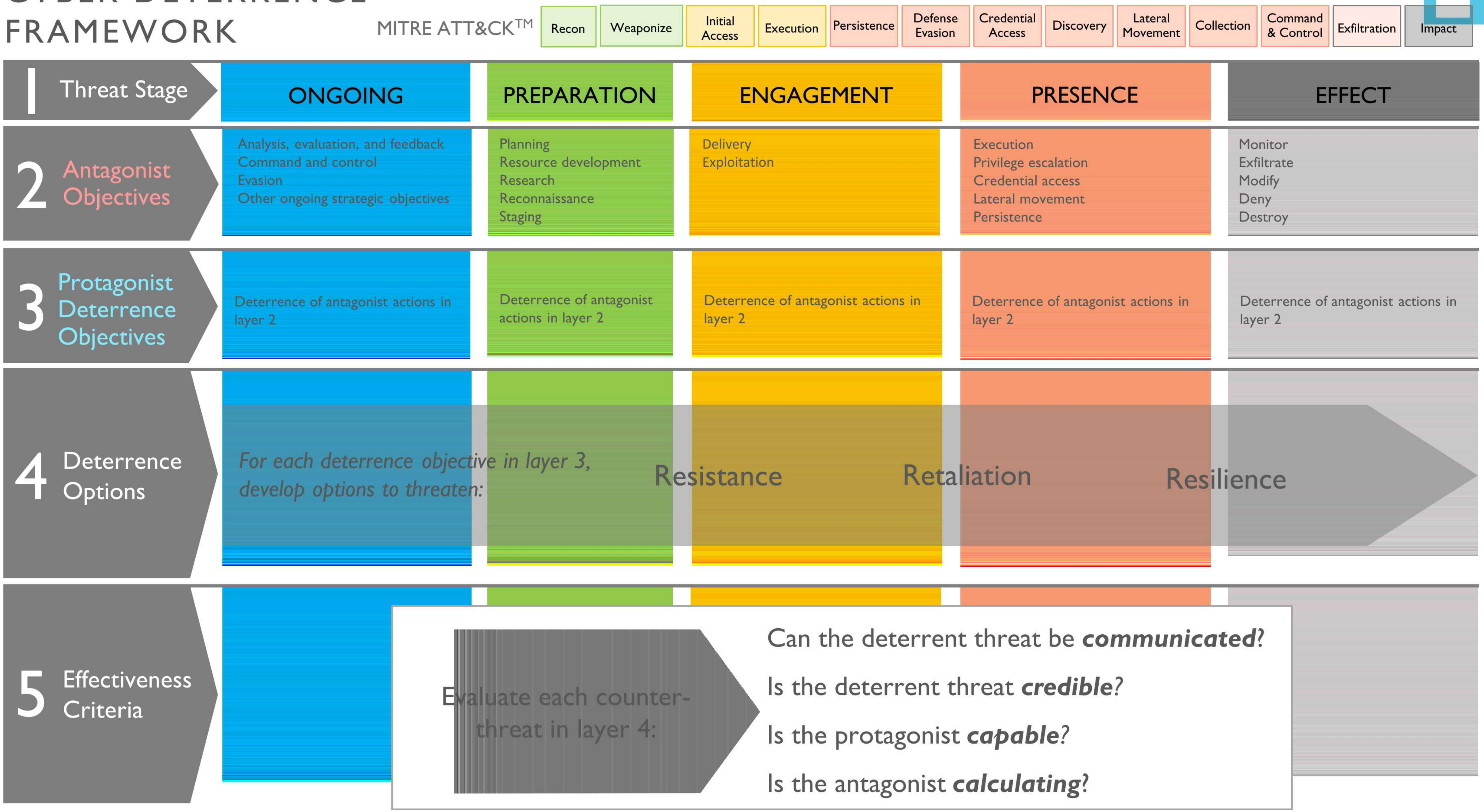
CAPABLE

The antagonist must perceive that the protagonist is able to execute the counterthreat, and that the counterthreat will inflict sufficient pain or cost on the antagonist if executed. The antagonist must perceive that the protagonist is capable of influencing the antagonist's cost/benefit analysis.

CALCULATED

The antagonist must consider the counterthreat and its implications when choosing a course of action, and must act rationally.

CYBER DETERRENCE FRAMEWORK



MITRE ATT&CK™

Recon	Weaponize	Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact

1 Threat Stage	ONGOING	PREPARATION	ENGAGEMENT	PRESENCE	EFFECT
2 Antagonist Objectives	Analysis, evaluation, and feedback Command and control Evasion Other ongoing strategic objectives	Planning Resource development Research Reconnaissance Staging	Delivery Exploitation	Execution Privilege escalation Credential access Lateral movement Persistence	Monitor Exfiltrate Modify Deny Destroy
3 Protagonist Deterrence Objectives	Deterrence of antagonist actions in layer 2	Deterrence of antagonist actions in layer 2	Deterrence of antagonist actions in layer 2	Deterrence of antagonist actions in layer 2	Deterrence of antagonist actions in layer 2

4 Deterrence Options

For each deterrence objective in layer 3, develop options to threaten:

Resistance

Retaliation

Resilience

5 Effectiveness Criteria

Evaluate each counter-threat in layer 4:

Can the deterrent threat be ***communicated***?

Is the deterrent threat ***credible***?

Is the protagonist ***capable***?

Is the antagonist ***calculating***?

CYBER DETERRENCE FRAMEWORK

MITRE ATT&CK™

Recon	Weaponize	Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact

1 Threat Stage	ONGOING	PREPARATION	ENGAGEMENT	PRESENCE	EFFECT
2 Antagonist Objectives	Analysis, evaluation, and feedback Command and control Evasion Other ongoing strategic objectives	Planning Resource development Research Reconnaissance Staging	Delivery Exploitation	Execution Privilege escalation Credential access Lateral movement Persistence	- Destroy hardware - Delete software and backup files - Disrupt physical industrial processes (ICS attack) at desired level of effect
3 Protagonist Deterrence Objectives	Deterrence of antagonist actions in layer 2	Deterrence of antagonist actions in layer 2	Deterrence of antagonist actions in layer 2	Deterrence of antagonist actions in layer 2	- Deter Antagonist from destroying hardware, deleting software and backup files - Deter Antagonist from future attempts to disable electric grid
4 Deterrence Options	*For each deterrence objective in layer 3, develop options to threaten:*	**Threat of Resistance** • Establish an air gap • Intrusion detection (IDS, IPS, SEIM) • Disable/destroy. Machines from which malware launch order could originate		**Threat of Retribution** • Name & shame • Military cyber retaliation • Military kinetic retaliation	**Threat of Resilience** • Manual override operations • Ensure redundancy (backup hardware, swappable systems)
5 Effectiveness Criteria	**Effectiveness Criteria** Option: Manual override operations Overall Score: YES	Overt statement. Historical precedent.	Principled: Yes Rational: Yes – worth cost to Blue	Executable: Yes, provided manual systems are still intact Painful/costly: Maybe – depends on adversary's commitment	**We assume adversary perceives costs and benefits of action, and that, given enough information, we can influence their perception.**

Strategic Foresight

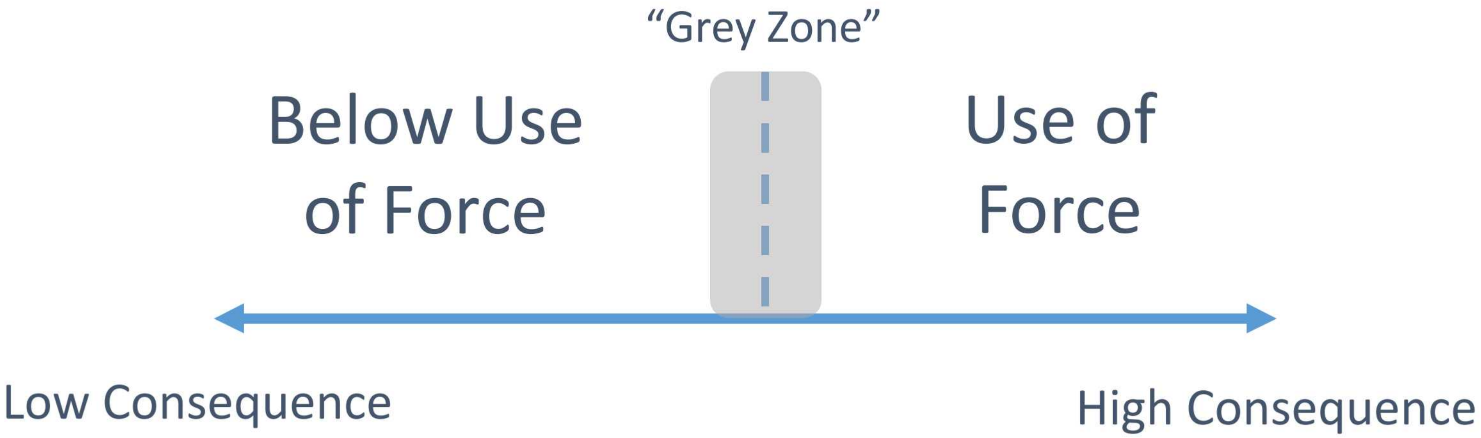
Applications of the Framework

- The team is currently pursuing options to engage internal and external stakeholders with this framework.
- We are also exploring ways to refine the effectiveness analysis and add additional rigor.

- What is the viability of this framework for strategic foresight?
- We have walked through a simple example scenario. What if we analyze a set of scenarios, what insight can we gain?
- Additionally, thresholds are a critical focus area in many circles, for obvious reasons, what advances can the framework contribute?

Thresholds

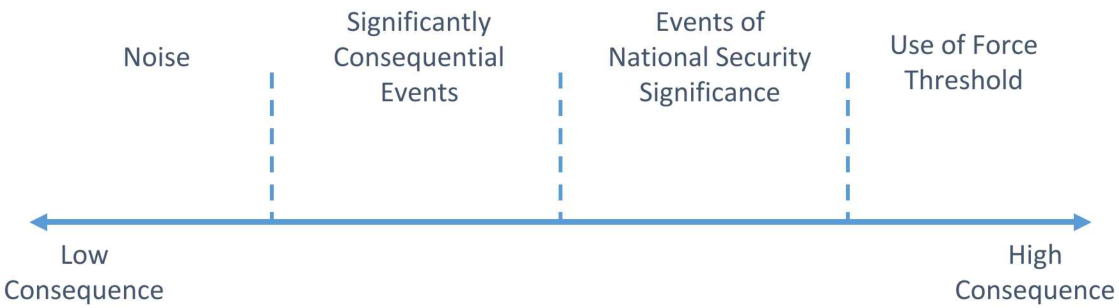
The current approach to thresholds in cyber scenarios lacks nuance…

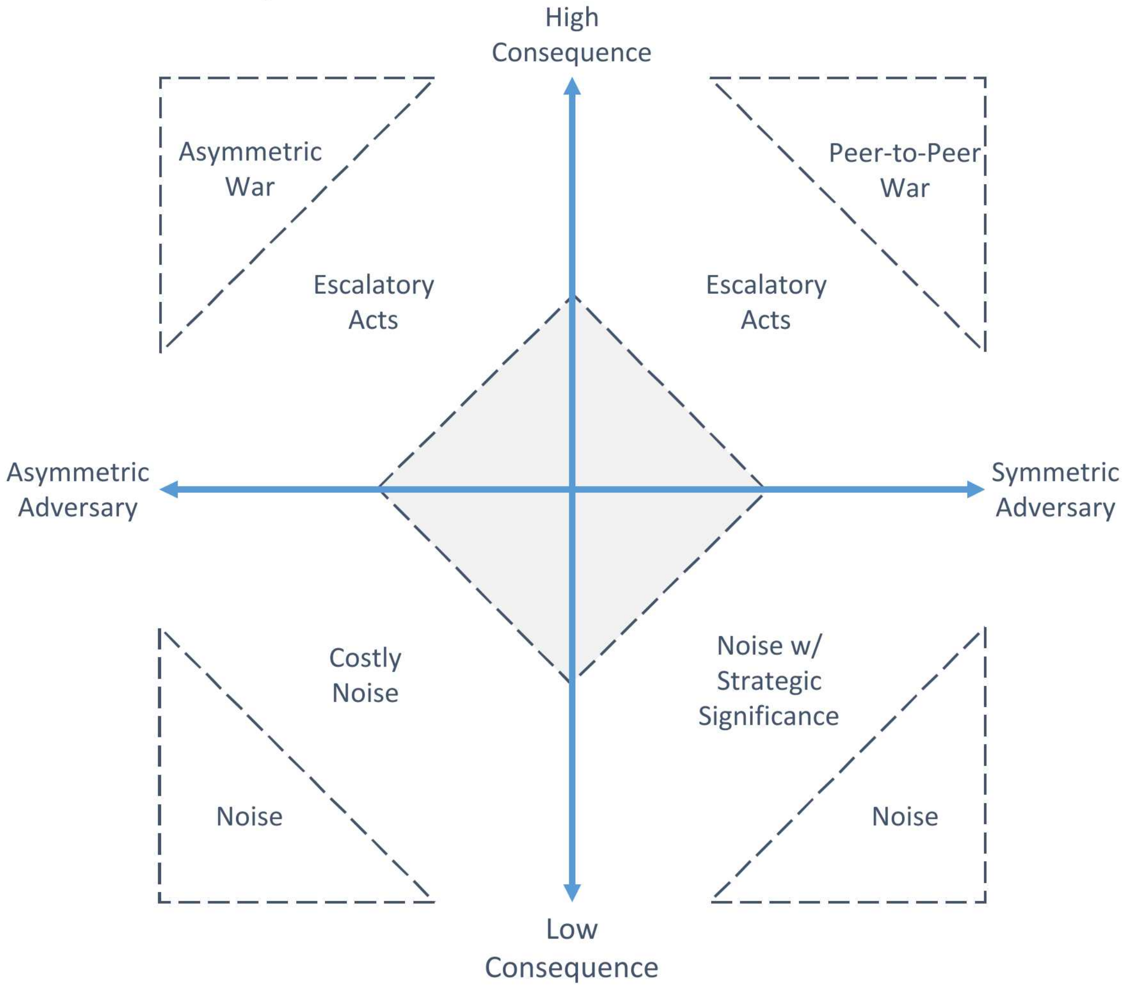


U.S. CYBERCOM Command Vision (2018)
"Adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages."

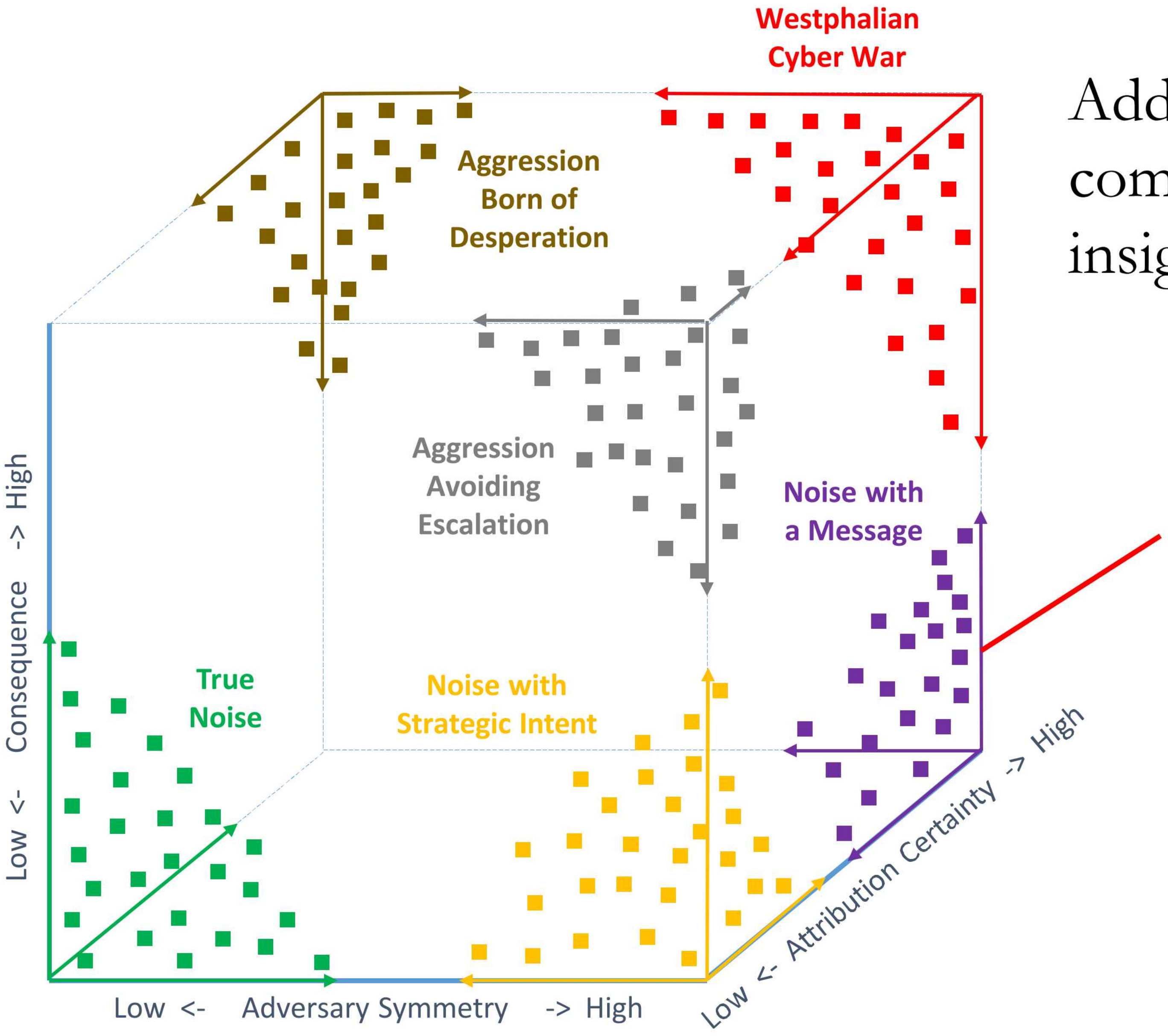
Thresholds-based Analyses

Cyber conflict scenarios can be characterized along many dimensions; existing literature draws its conclusions based only on a handful.


Noise
Significantly Consequential Events
Events of National Security Significance
Use of Force Threshold
Low Consequence
High Consequence



Multi-dimensional Analysis


Westphalian Cyber War
Aggression Born of Desperation
Aggression Avoiding Escalation
Noise with a Message
True Noise
Noise with Strategic Intent
Low <- Consequence -> High
Low <- Adversary Symmetry -> High
Low <- Attribution Certainty -> High

Additional dimensions add analytical complexity, but also potentially greater insight.

Our location in the n-dimensional scenario space has direct bearing on options for deterrence.

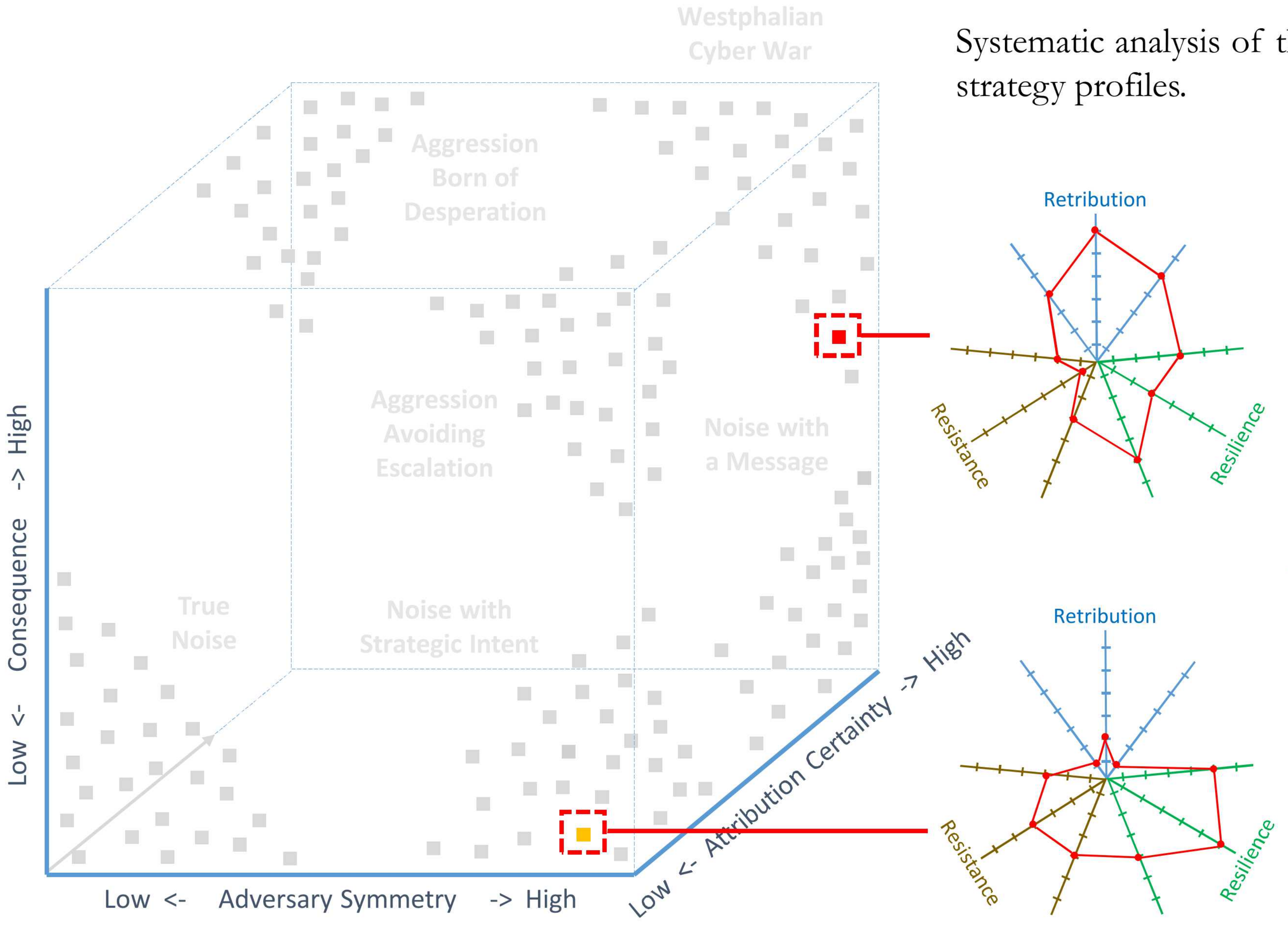
For example, in an environment characterized by low consequence action, symmetry of power, and high attribution certainty:

- The magnitude of any retaliatory threat is potentially limited/complicated by proportionality considerations.
- The peer-to-peer dynamic raises concerns regarding escalatory potential.
- The adversary is not obscuring their intentions, so communication of our threat is potentially less complicated.

Strategy Profiles

NOTIONAL PROFILES

Systematic analysis of the scenario space can help us arrive at strategy profiles.


Westphalian Cyber War
Aggression Born of Desperation
Aggression Avoiding Escalation
Noise with a Message
True Noise
Noise with Strategic Intent
Low <- Consequence -> High
Low <- Adversary Symmetry -> High
Low <- Attribution Certainty -> High
Retribution
Resistance
Resilience
Retribution
Resistance
Resilience

Strategy Emphasis	• Retribution, supported by resilience
Enabling Capabilities	• Offensive cyber tools • Precision kinetic options • Redundant & survivable C&C supporting cyber ops • Resilient infrastructure that can absorb adversary cyber attacks
Stakeholders	• DOD (retribution) • DHS (resiliency support/coordination) • Sector-specific agencies (resiliency implementation)

Strategy Emphasis	• Resilience & resistance, with secondary retribution options
Enabling Capabilities	• Defensive cyber measures for targeted infrastructure • Investigatory resources supporting attribution and retribution
Stakeholders	• DHS (resiliency support/coordination) • Sector-specific agencies (resiliency implementation) • DOJ/FBI (supporting retribution through investigatory resources)

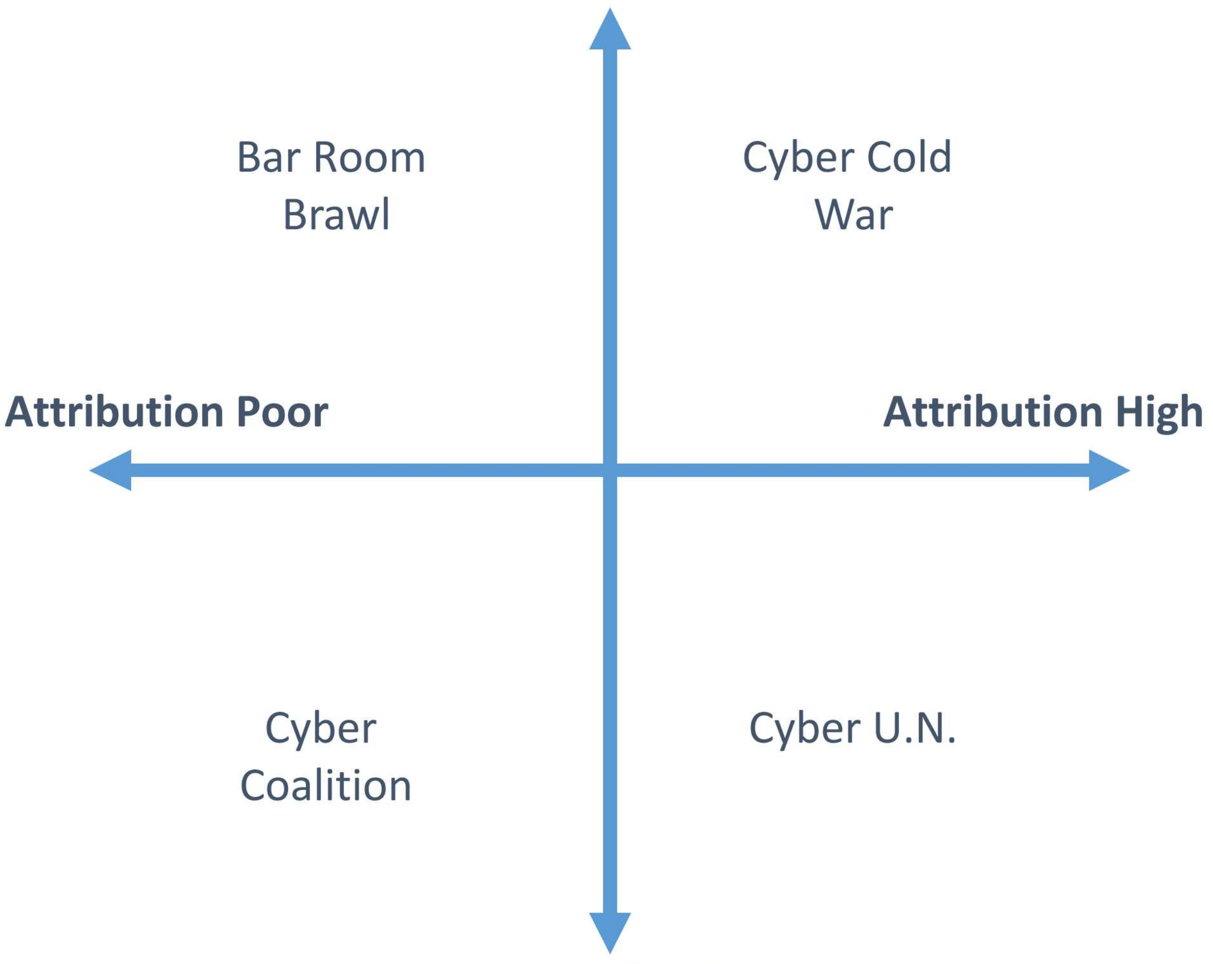
Critical Uncertainties

- Obviously, it's impossible to fully predict the future, but if you can identify critical uncertainties in the current world and how they might shape the world 10-20 years from now, then you can create specific scenarios corresponding to those drivers.
- We can't prepare for every possible future, but we *can* prepare for a few potential futures.
- As part of the team's past efforts, correspondents (experts and/or participants at workshops) were asked questions to validate scenario choices and to help refine possible futures.

Example Drivers

- Autonomy in Offense and Defense
- Regulation
- Connectivity of Systems
- Industry Cyber Posture
- Homogeneity of Systems
- Centralization of Data
- Data Collection
- Liability for Cyber Incident
- Detection Capabilities
- Attribution Capabilities
- International Relations

International Relations Adversarial



International Relations Peaceful

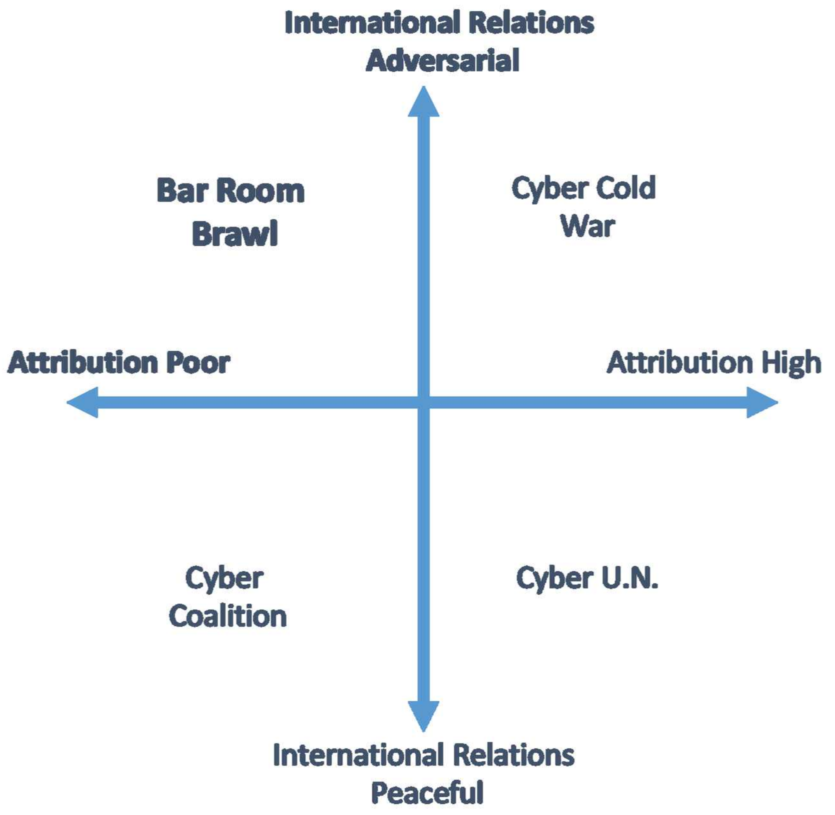
Draft Example

What does it mean for GOV ORG to operate in a future state where attribution is degraded and international relations are weakened?

The .gov and CI environments would suffer attacks more frequently, and of higher severity.

Depending on the GOV ORG's roles and responsibilities (and authorities), the organization can explore options across the three R's, resistance, resilience, and retribution.

- Develop a strategy for communicating capabilities to adversaries. (All R's)
- Invest in R&D for cybersecurity capability enhancements due to increased frequency and severity of attacks. (All R's)
- When developing/deploying services, assets, or other functions, build in resilience by design to allow for operation in degraded state. (Resilience)
- The potential implementation of or transition to a more secure network architecture (such as Zero Trust) will pose unique challenges to each organization but can reduce risk overall. (Resistance)
- Where appropriate, explore opportunities to improve attribution techniques through coordination, information sharing, and technologies to better identify malicious actors. (Retribution)



International Relations Adversarial

Bar Room Brawl

Cyber Cold War

Attribution Poor

Attribution High

Cyber Coalition

Cyber U.N.

International Relations Peaceful

Looking Ahead

Options?

1. Strict Thresholds
   - Lack of rigor is limiting
2. Multi-dimensional Strategies
   - Need more data to better inform outcomes
3. Scenario Planning
   - Must identify the critical drivers of concern
4. Something else?
   - Likely to depend on target audience…

We are looking for feedback.

Other approaches, tools, resource that we should consult?

Conclusion

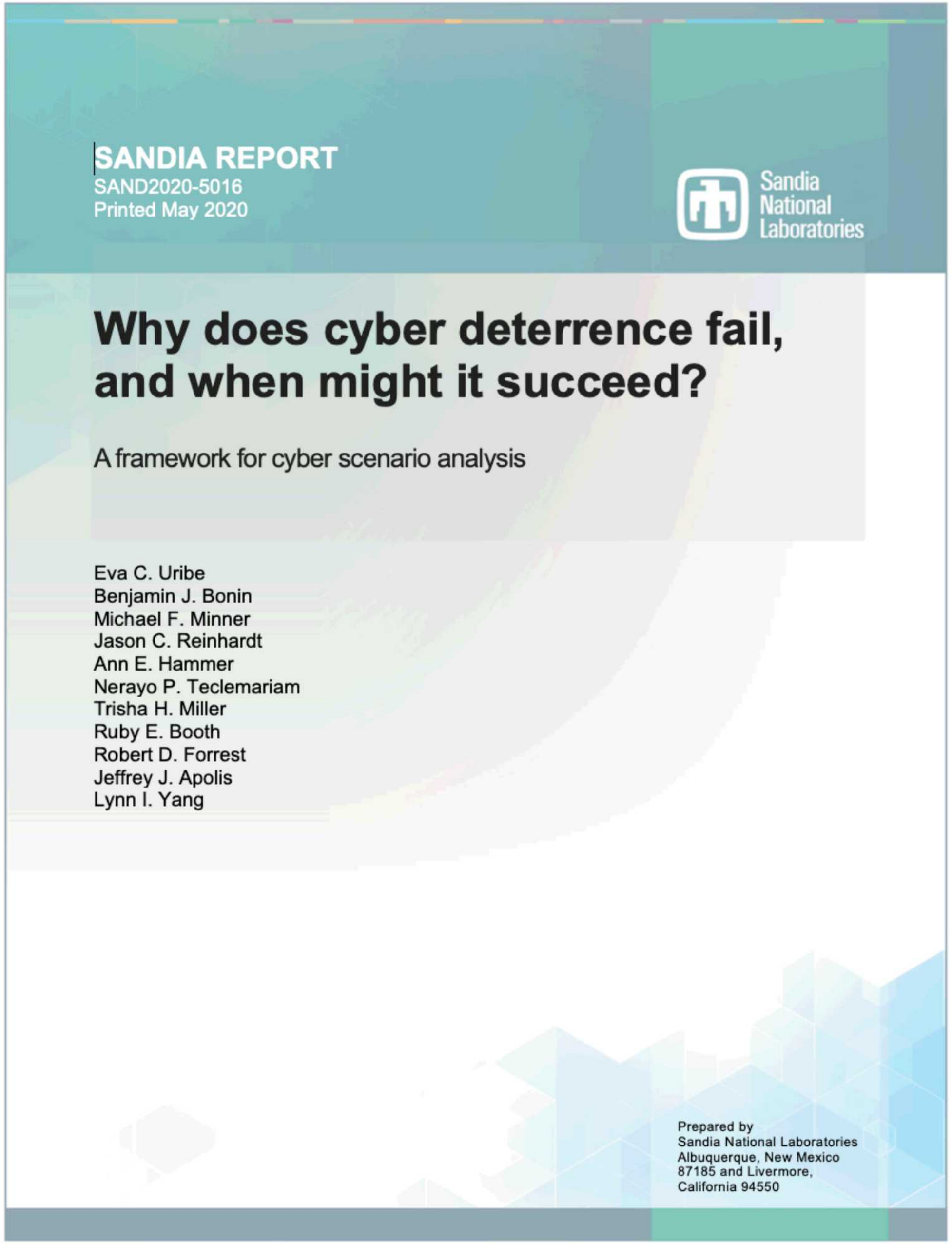
Thank you for your time!

We have a UUR report that we are preparing for external publication.

Emails:

euribe@sandia.gov

mfminne@sandia.gov



SANDIA REPORT
SAND2020-5016
Printed May 2020

Sandia National Laboratories

Why does cyber deterrence fail, and when might it succeed?

A framework for cyber scenario analysis

Eva C. Uribe
Benjamin J. Bonin
Michael F. Minner
Jason C. Reinhardt
Ann E. Hammer
Nerayo P. Teclemariam
Trisha H. Miller
Ruby E. Booth
Robert D. Forrest
Jeffrey J. Apolis
Lynn I. Yang

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Deterrence of cyber adversaries presents unique challenges

1 Cyberspace is a domain of *constant contact* (many actors interacting with unprecedented speed, remoteness, and scale)

2 Attribution of attacks and intrusions is difficult

3 Detection of attacks and intrusions is often delayed

4 Cross-domain deterrence may be escalatory

5 The U.S. is asymmetrically vulnerable in cyberspace

6 There is a lack of domestic norms and laws for responding to cyber incidents

7 There is a lack of international norms and law for conflict and behavior in cyberspace

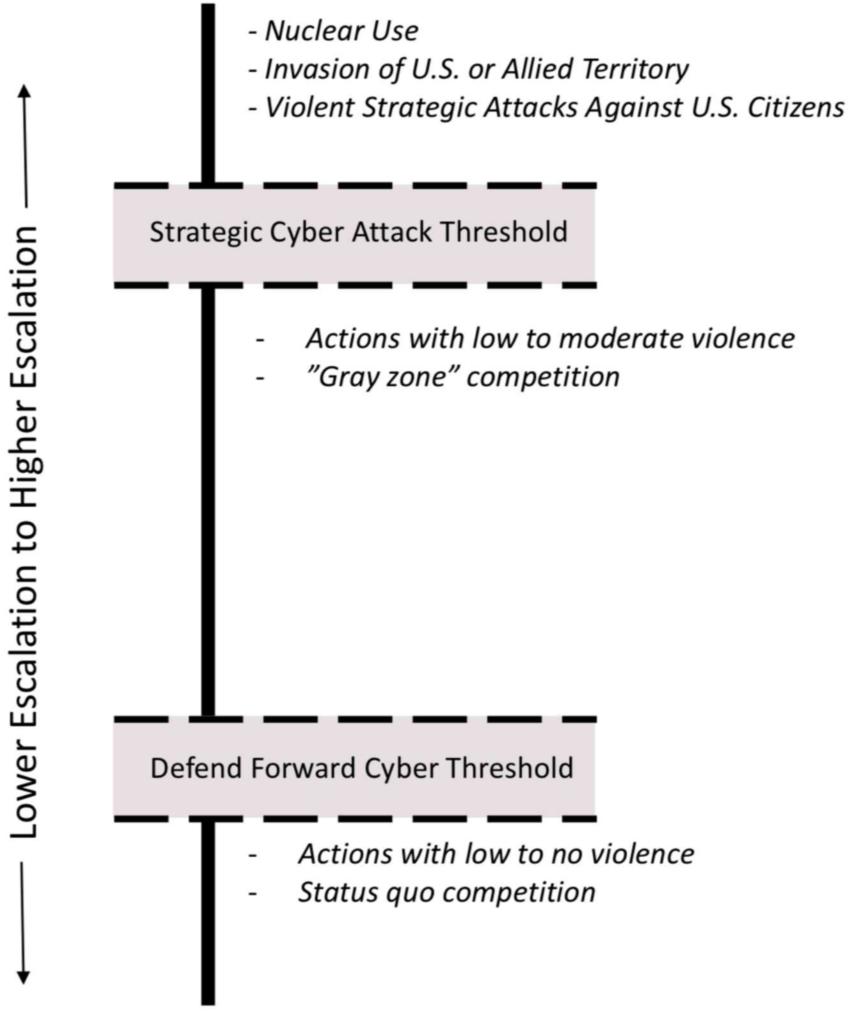
8 The effects of cyber weapons are uncertain

9 Offensive and defensive cyber operations are difficult to distinguish

10 Greater potential for technological surprise that rapidly alters conflict asymmetries

11 Greater tension in the reveal/conceal dilemma (defense is relatively easy)

Single Axis Thresholds



- Nuclear Use
- Invasion of U.S. or Allied Territory
- Violent Strategic Attacks Against U.S. Citizens

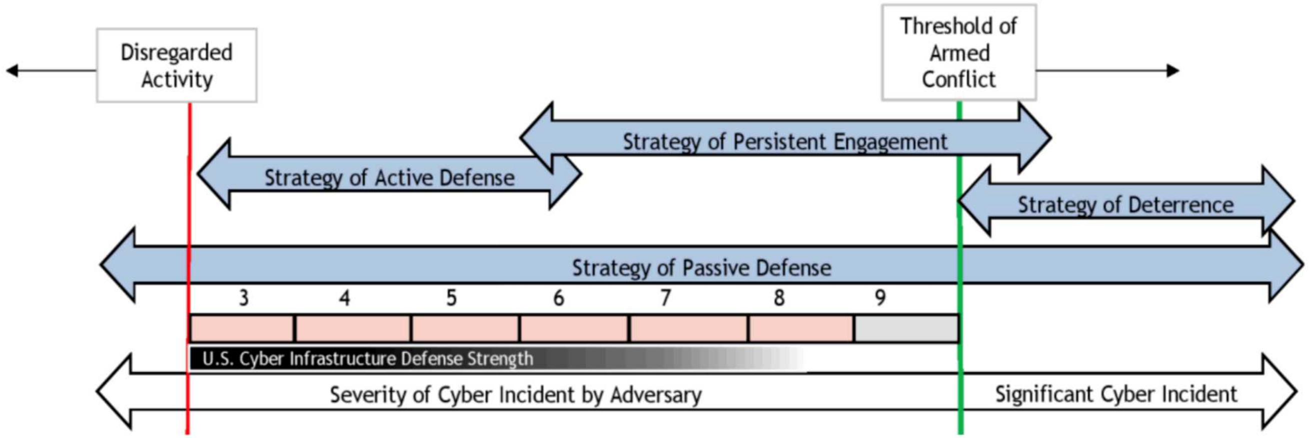
Strategic Cyber Attack Threshold

- *Actions with low to moderate violence*
- *"Gray zone" competition*

Defend Forward Cyber Threshold

- *Actions with low to no violence*
- *Status quo competition*

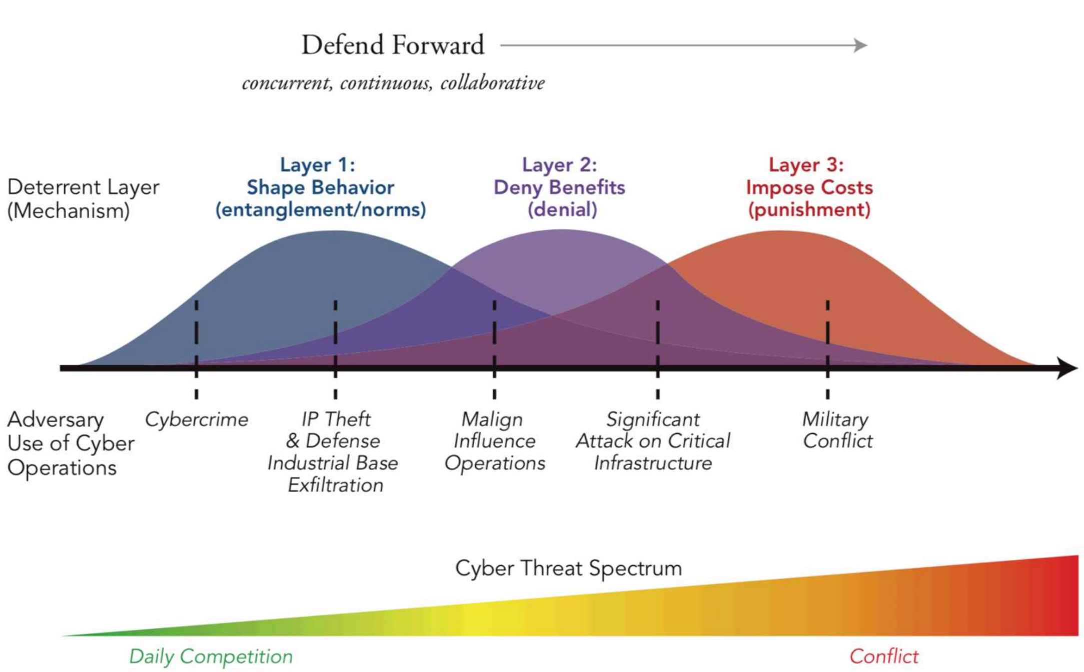
Jacquelyn Schneider's "Cyber Threshold Problem"



Disregarded Activity
Threshold of Armed Conflict
Strategy of Persistent Engagement
Strategy of Active Defense
Strategy of Deterrence
Strategy of Passive Defense
3
4
5
6
7
8
9
U.S. Cyber Infrastructure Defense Strength
Severity of Cyber Incident by Adversary
Significant Cyber Incident

The Strategic Integrated Cyber Influence Model (Texas A&M)

Layered Cyber Deterrence



Cyberspace Solarium Commission