SAND2021-3776PE

Energy & Homeland Security

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 (CyDaR) Strategic Initiative

Presented by Michael Minner

April 5, 2021

Energy &
Homeland Security

Why should Sandia be concerned with the deterrence of cyber adversaries?

WHAT THREATS DO WE FACE IN CYBERSPACE?

Major U.S. Public-Sector Cyber Threats

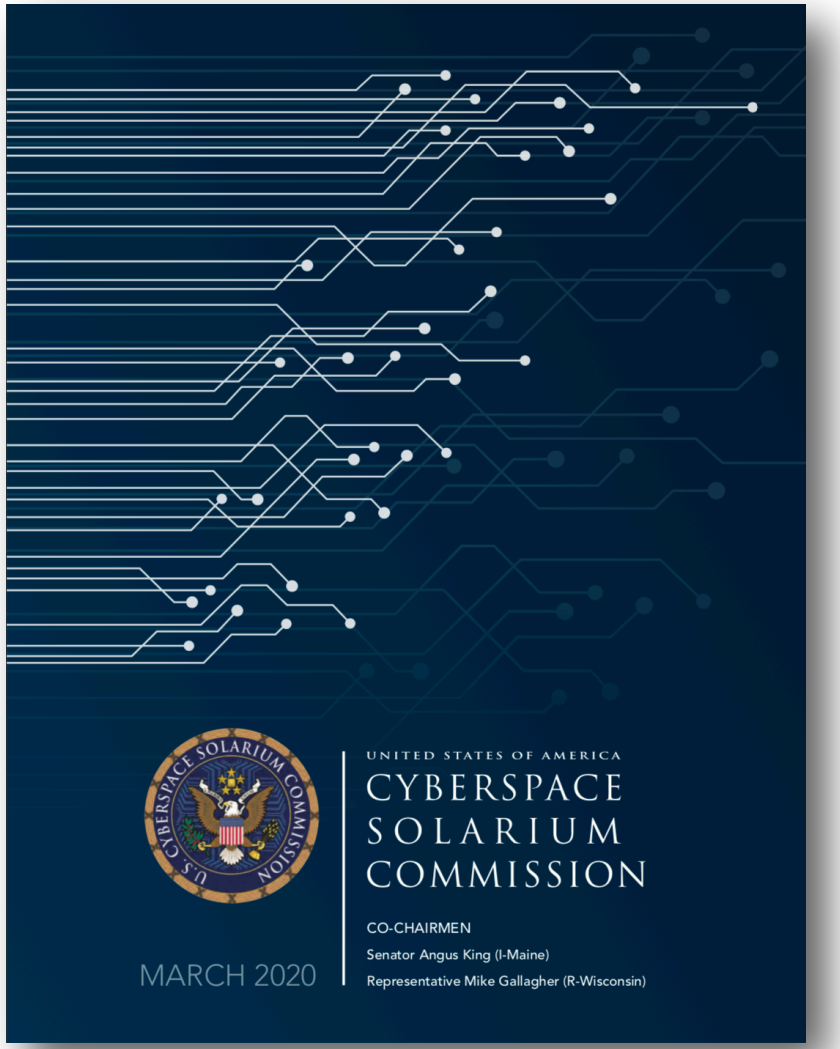
- Attacks on election processes and other democratic institutions
- Espionage to undermine military capabilities
- Targeting civilian agencies for intelligence collection
- Loss of leadership in research and development of key technologies

Major U.S. Private-Sector Cyber Threats

- Cybercrime and ransomware for financial gain
- Intellectual property theft that hinders growth and innovation
- Holding private-sector critical infrastructure at risk to influence leaders during crises

Examples

- 2012 Malware hits Saudi Aramco, resulting in 30,000 computers rendered unusable
- 2013 IP Commission Report estimates IP theft leads to business losses of $300 billion annually
- 2015 Phishing emails with malicious code grant unauthorized access to South Korean nuclear power plant
- 2014-15 Office of Personnel Management is breached, exposing sensitive information on 21 million federal employees
- 2015-16 Cyber incidents targeting Ukrainian energy companies disrupt power for millions
- 2017 Equifax breach results in theft of personal information of over 145 million



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)

PROBLEM: PERFECT CYBER DEFENSE IS NOT POSSIBLE

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

DETERRENCE OF CYBER ADVERSARIES IS U.S. POLICY

National Security Strategy

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)

DISCUSSION

Given this context, why should Sandia be involved in this space?

WHY SANDIA?

PROBLEM

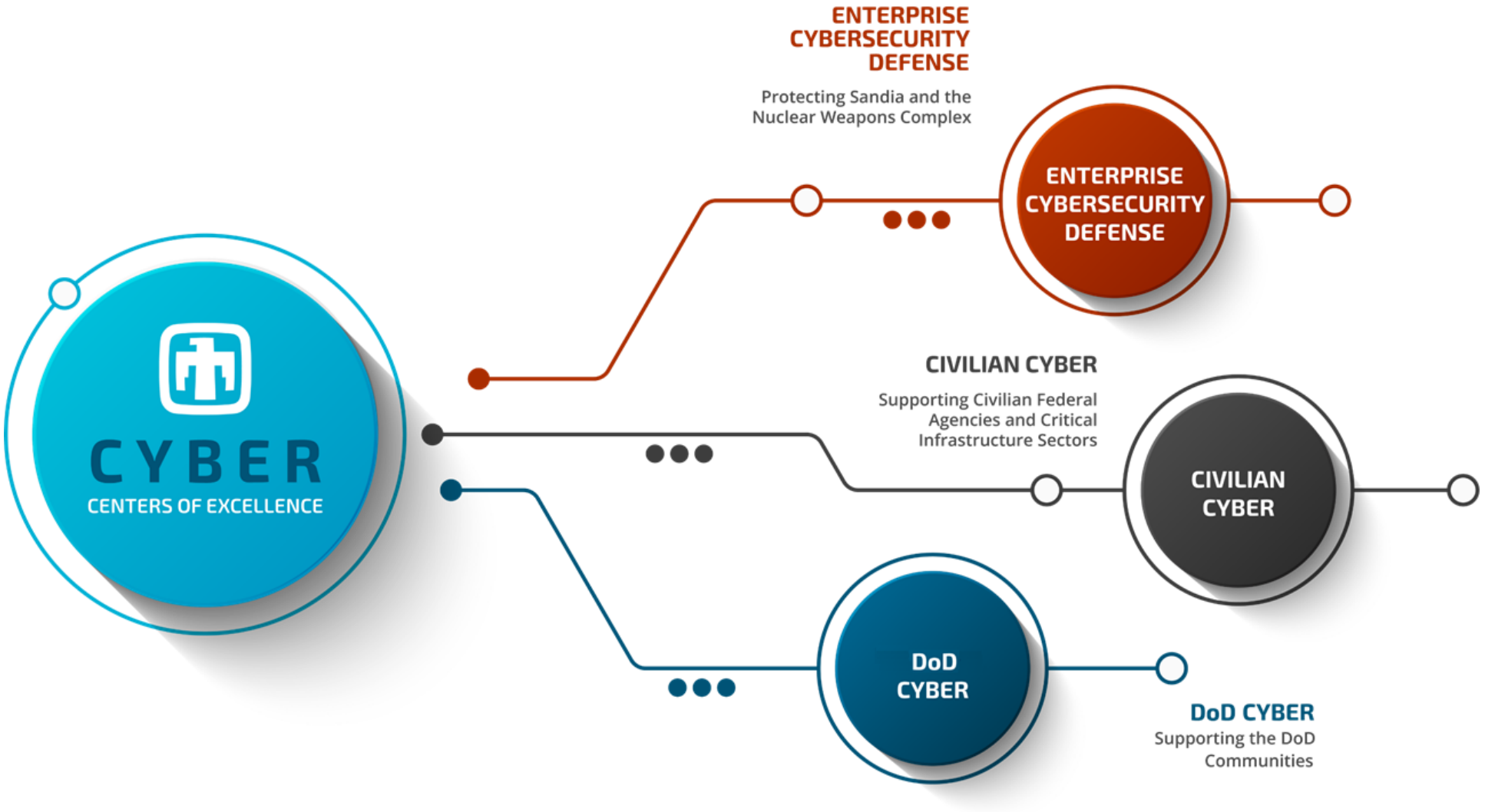
The need and policy for cyber deterrence is evident, but there is lacking a clear set of frameworks, tools, and metrics to enable the community to operationalize cyber deterrence.

SOLUTION

Sandia is the helping to bring a holistic approach to the complex issue with our expertise in deterrence theory and practice, deep and broad R&D capabilities, and world-class threat-informed cyber and critical infrastructure knowledge.



CYBER DETERRENCE WORK COMPLEMENTS SANDIA'S CYBER PROGRAMS



Energy &
Homeland Security

What is cyber deterrence?

DISCUSSION

How would you define deterrence?

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 THREATS RAISE COST OR DECREASE BENEFITS OF ADVERSARY

Hypothesis: An adversary is dissuaded from action when

$$Value_{action} < Value_{inaction}$$

$$(B_{action} - C_{action}) < (B_{inaction} - C_{inaction})$$

- C_{action}= costs of action
- $C_{inaction}$= costs of inaction

B_{action} = benefits of action

$B_{inaction}$ = benefits of inaction

DISCUSSION

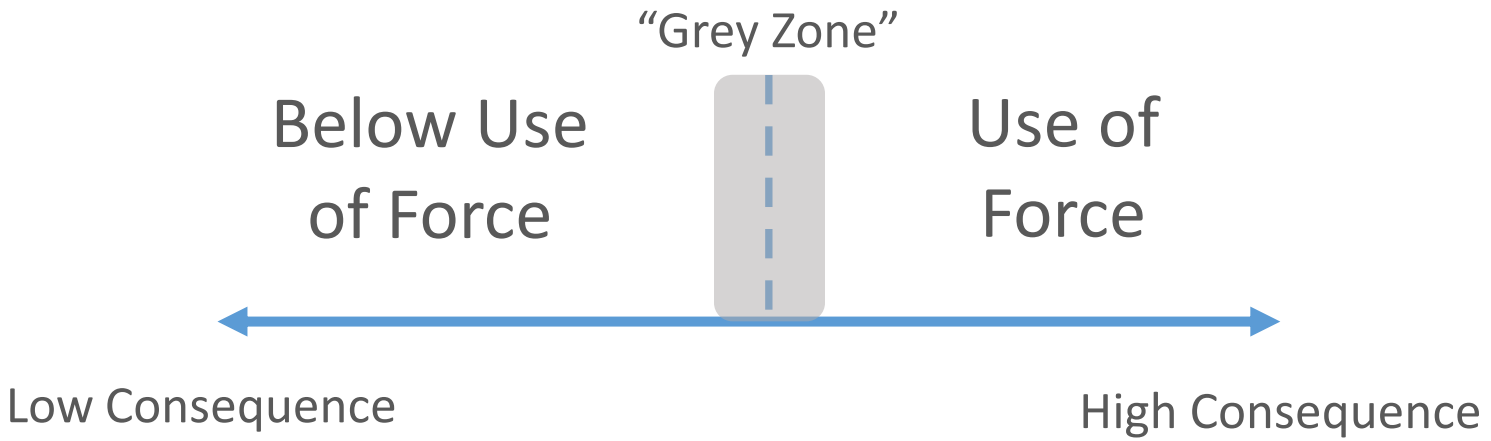
What elements of cyber make deterrence of cyber adversaries unique or challenging?

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

THRESHOLDS

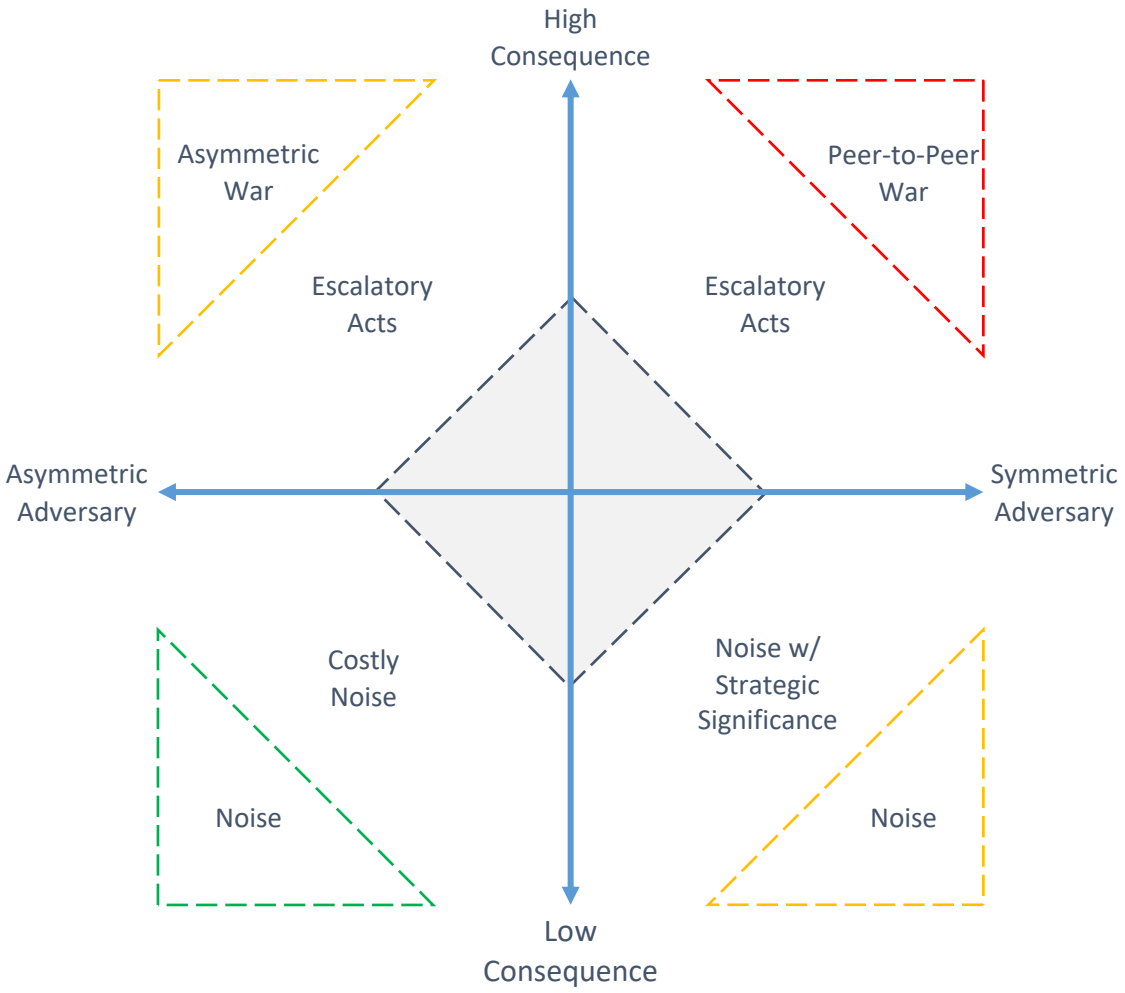
The current approach to thresholds in cyber scenarios lacks nuance…



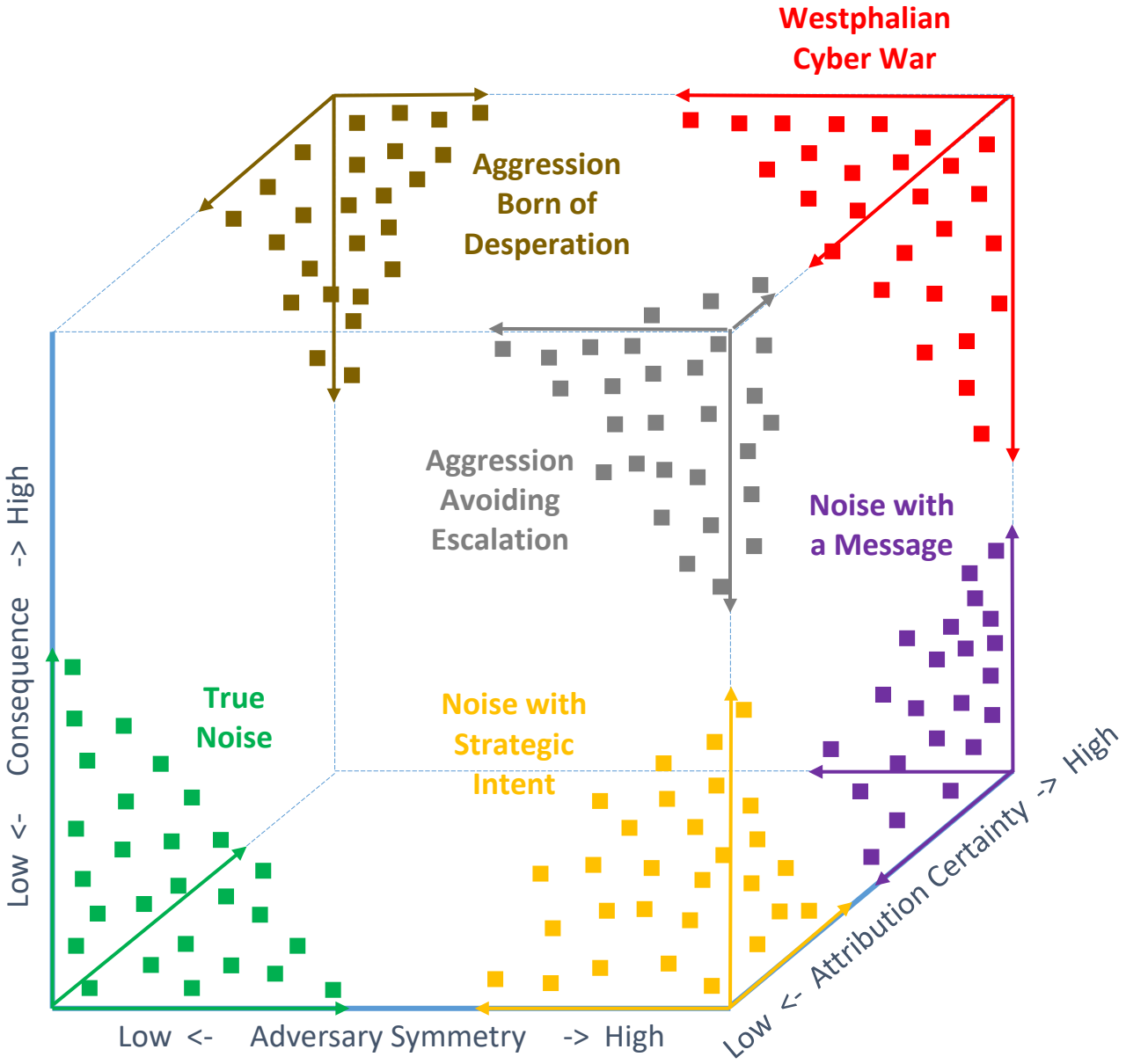
U.S. CYBERCOM Command Vision (2018)
"Adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages."

THRESHOLDS-BASED ANALYSES

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



MULTI-DIMENSIONAL ANALYSIS



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

Energy &
Homeland Security

How can we analyze this space systematically?

EXAMPLE DETERRENCE MECHANISMS

DENIAL

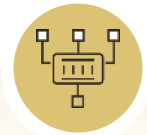
Antagonist is dissuaded from action; perceived benefits of action reduced or eliminated

ENTANGLEMENT

Simultaneous costs to both protagonist and antagonist due to interdependencies

NORMS

Damage to antagonist's reputation is perceived to outweigh benefits



CYBER PERSISTENCE

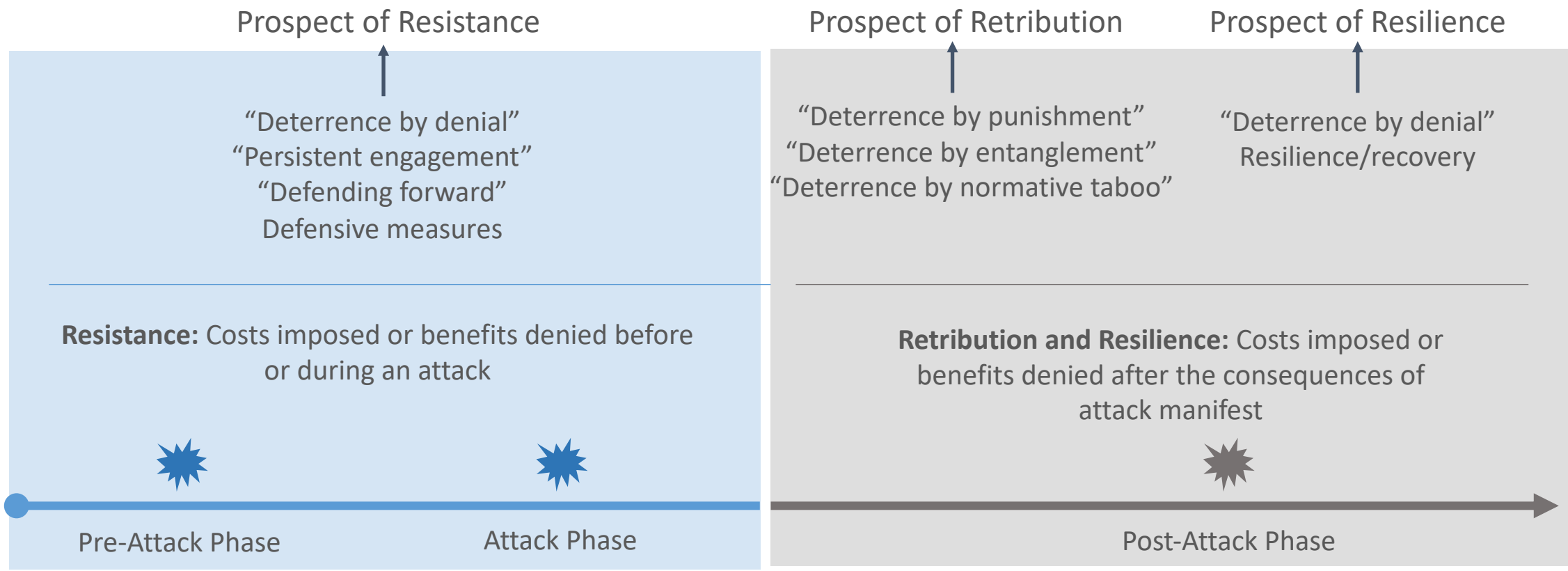
Through threats and regular use of force, antagonist establishes norms and conditions that reduce incentives

PUNISHMENT

Preventing an action by fear of the consequences

Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, **41,** *3* (2017), 44-71.
Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies,* **40**, *1-2* (2015) 92-117.
Lucas Kello, *The Virtual Weapon and International Order*, Yale University Press (New Haven, CT, 2017).
Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is not a credible strategy for cyberspace," *Orbis*, **61,** *3* (2017) 381-393.
Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command, United States Cyber Command, 2018.

THERE ARE MANY DIFFERENT STRATEGIES TO DETER CYBER ADVERSARIES



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 follow 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.

Energy &
Homeland Security

The Cyber Deterrence Framework and Example Scenario

A NOTE ON TERMINOLOGY…

Red vs. *Blue*

(upset status quo) *(maintain status quo)*

THE CYBER DETERRENCE FRAMEWORK HELPS US TO UNDERSTAND:

1. Which strategies can Blue employ to deter or dissuade Red from attacking in the first place?

2. Which deterrence actions are feasible for Blue to implement?

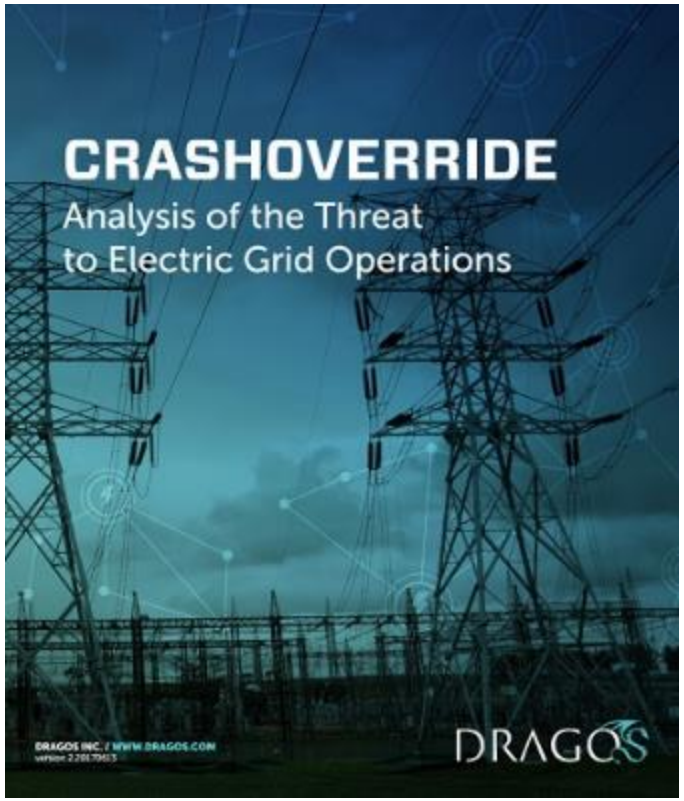
3. Which deterrence actions can influence Red cost/benefit analysis?

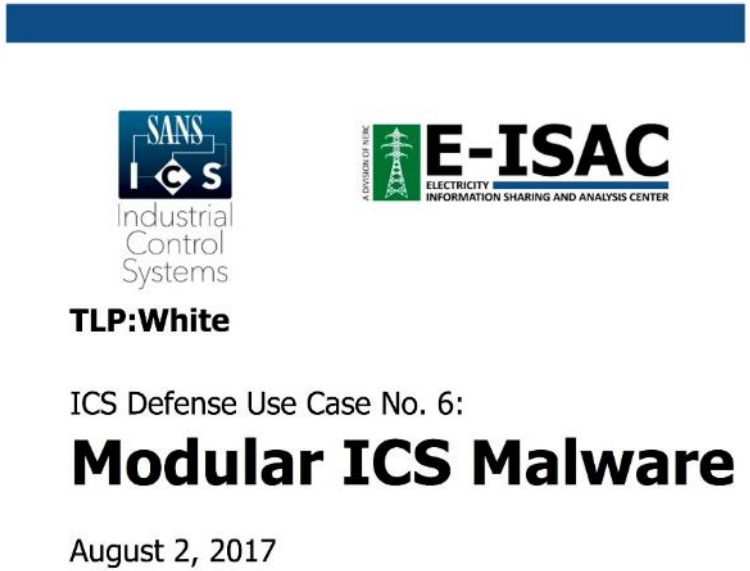
CYBER DETERRENCE FRAMEWORK

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***?			

OPEN SOURCE RESOURCES FOR TRIAL SCENARIO





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					
5 Effectiveness Criteria					

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	Threat of Retribution	Threat of Resilience
• Establish an air gap	• Name & shame	• Manual override operations
• Intrusion detection (IDS, IPS, SEIM)	• Military cyber retaliation	• Ensure redundancy (backup hardware, swappable systems)
• Disable/destroy. Machines from which malware launch order could originate	• Military kinetic retaliation	

5 Effectiveness Criteria

Effectiveness Criteria

Option:
Manual override operations

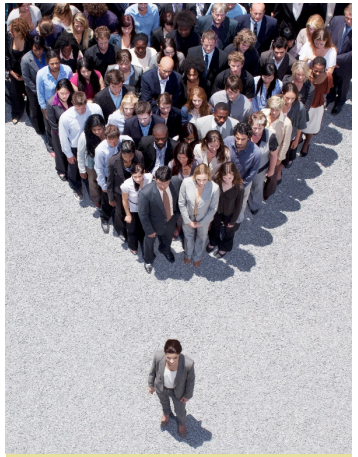
Overall Score: YES

COMMUNICATED	CREDIBLE Principled X Rational	CAPABLE Executable X Painful (Costly)	CALCULATED
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.**

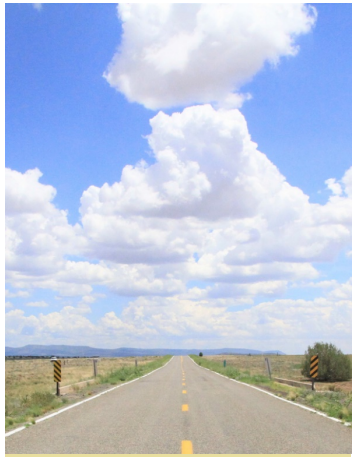
FRAMEWORK ENABLES SUPPORT FOR VARIOUS STAKEHOLDERS

Thought leadership in cyber deterrence

Analysis results to inform policy & operations



Understanding various roles of stakeholders



R&D Gaps & Roadmaps

Program Development Opportunities

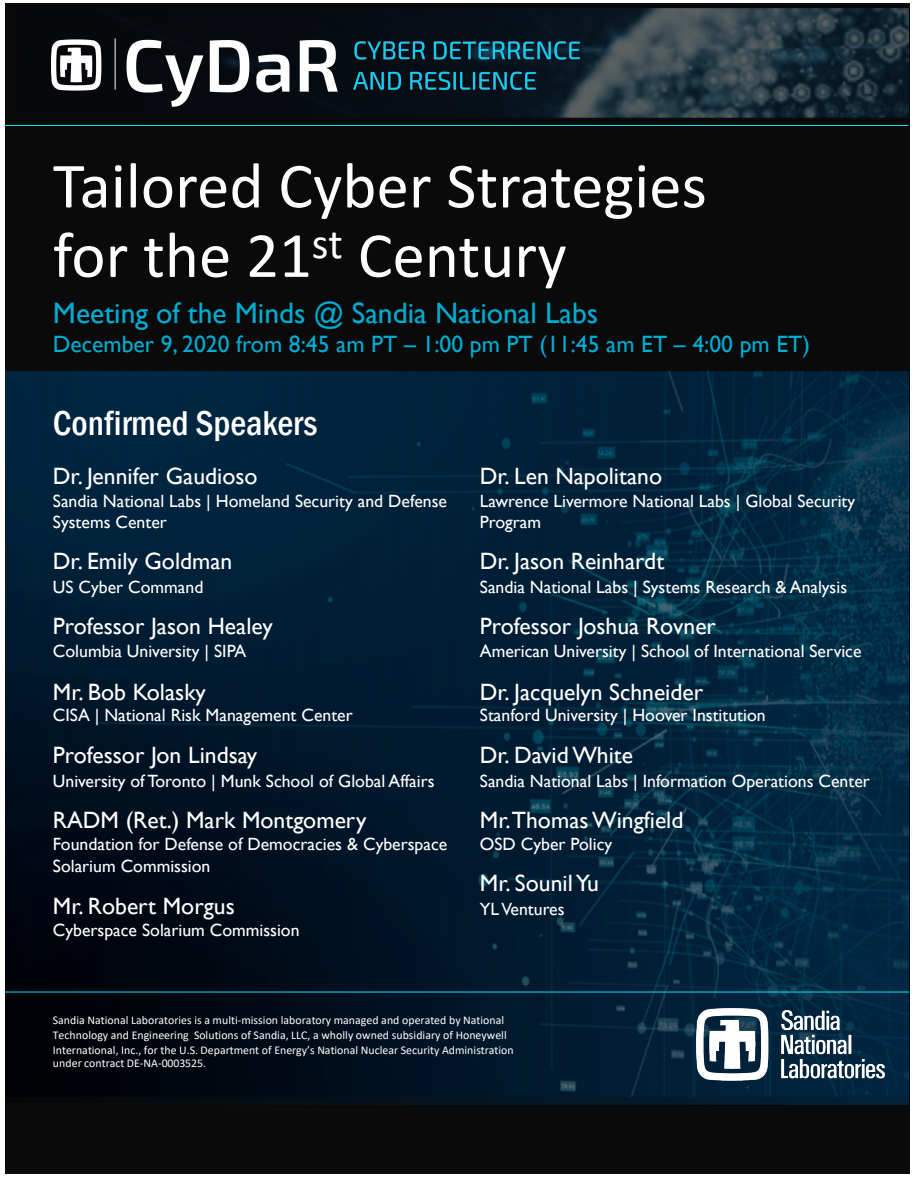
Understanding Alignment of Sandia Programs & Organizations

External - Focus

Internal - Focus

MEETING OF THE MINDS

- We hosted a Meeting of Minds focused on cyber strategies in December of 2020.
- Key takeaways from that meeting will be shared soon.
- Please keep an eye out for a future Meeting of the Minds.



CONCLUSION

Thank you for your time!

We have a UUR report.

We are preparing external publications.

We are also preparing a SharePoint page for broader access to materials and resources:

https://sharepoint.sandia.gov/sites/CyDaR

Email: mfminne@sandia.gov