



SAND2020-6702PE

Cyber Deterrence and Resilience Strategic Initiative: Intern Briefing



PRESENTED BY

Eva Uribe and Michael Minner

SAND #:##



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.



Why should Sandia care about deterrence of cyber
adversaries ?



What threats do we face in cyberspace?

Major U.S. Public-Sector Cyber Threats

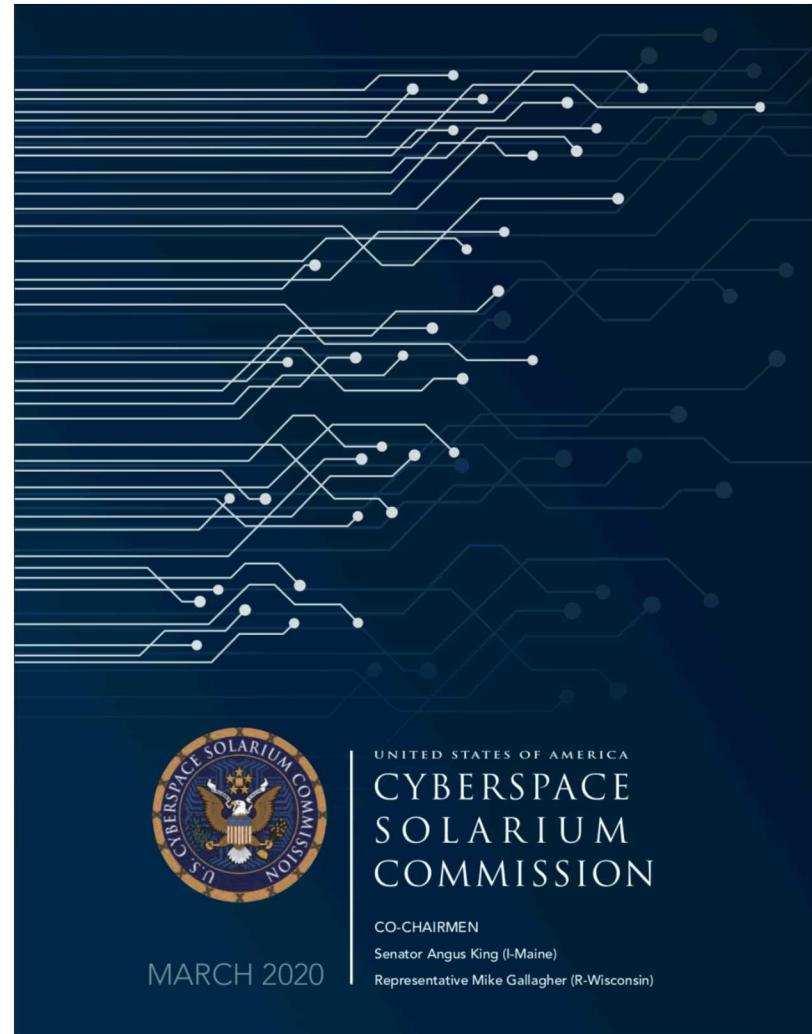
- Attacks on election processes and other democratic institutions
- Espionage to undermine military capabilities
- Targeting civilian agencies for intelligence collection
- Loss of leadership in research and development of key technologies

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)

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)
3. Global strategic stability

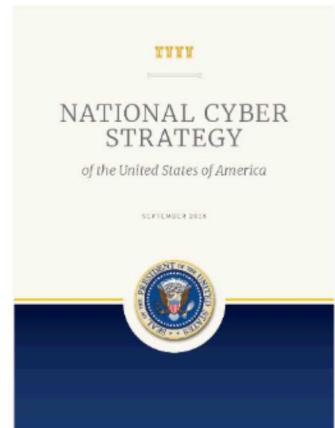
National Security Council's Recommendations to the President on Deterring Cyber Adversaries (2018)



Deterrence of cyber adversaries is U.S. policy

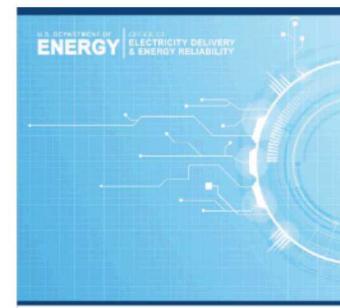
National Security Strategy (2017)

Priority actions include “deter and disrupt malicious cyber actors.”



National Cyber Strategy (2018)

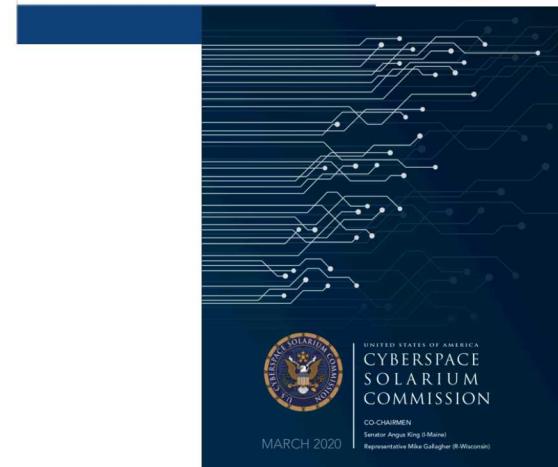
Strengthen U.S.’s ability “to deter and if necessary punish those who use cyber tools for malicious purposes.”



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)

Discussion

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

Why Sandia?

PROBLEM

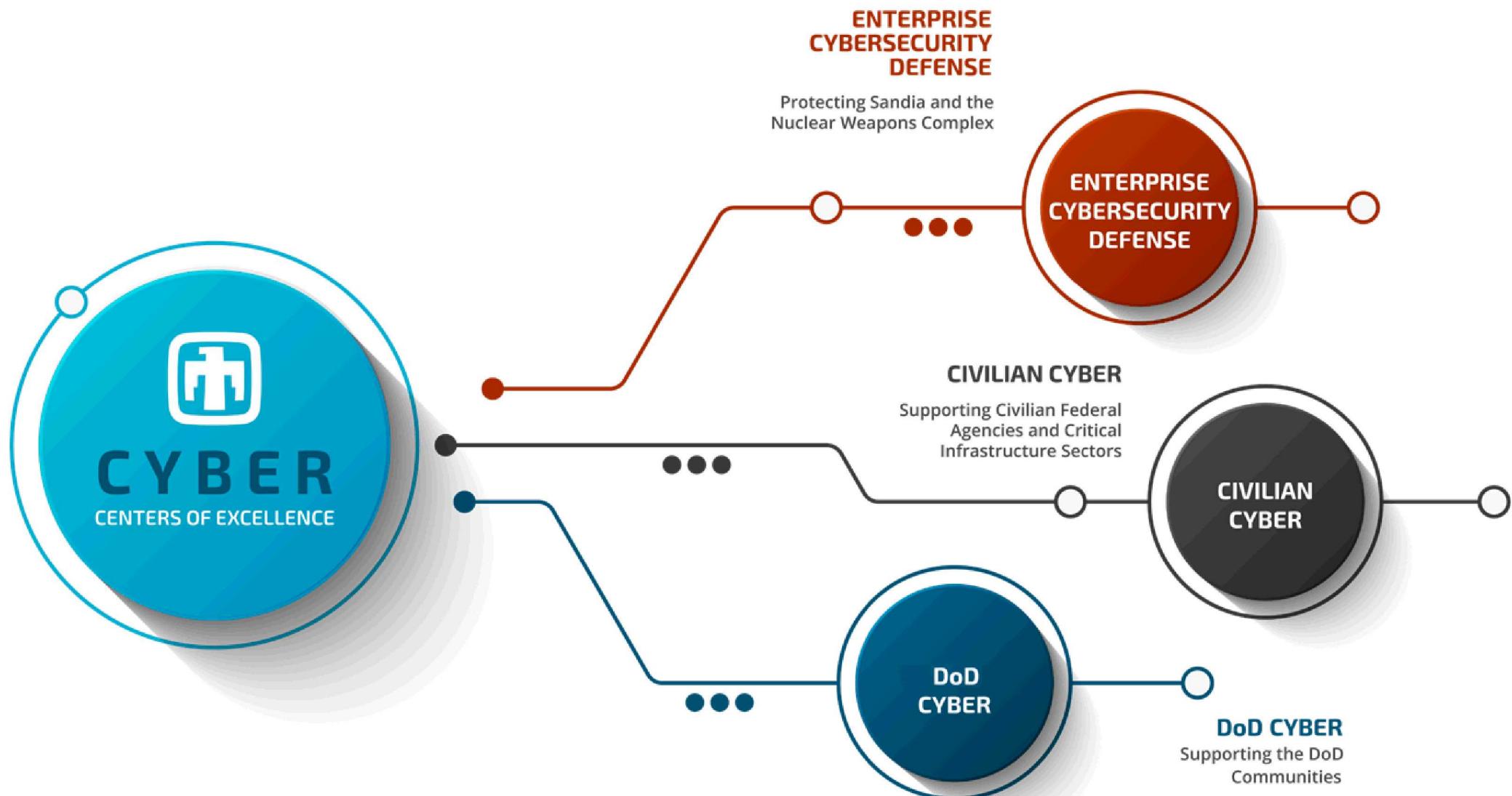
The need and policy for cyber deterrence is evident, but there is lacking a clear set of frameworks, tools, and metrics to enable the community to operationalize cyber deterrence.



SOLUTION

Sandia is 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.

Our cyber deterrence work complements Sandia's existing cyber programs



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



Hypothesis: An adversary is dissuaded from action when:

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

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

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

- B_{action} = benefits of action
- $B_{inaction}$ = benefits of inaction

Discussion

- What are elements of cyber that make deterrence of cyber adversaries unique and/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)

Attribution of attacks and intrusions is difficult

3 Detection of attacks and intrusions is often delayed

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

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)

Thresholds



The current approach to thresholds in cyber scenarios lacks nuance...

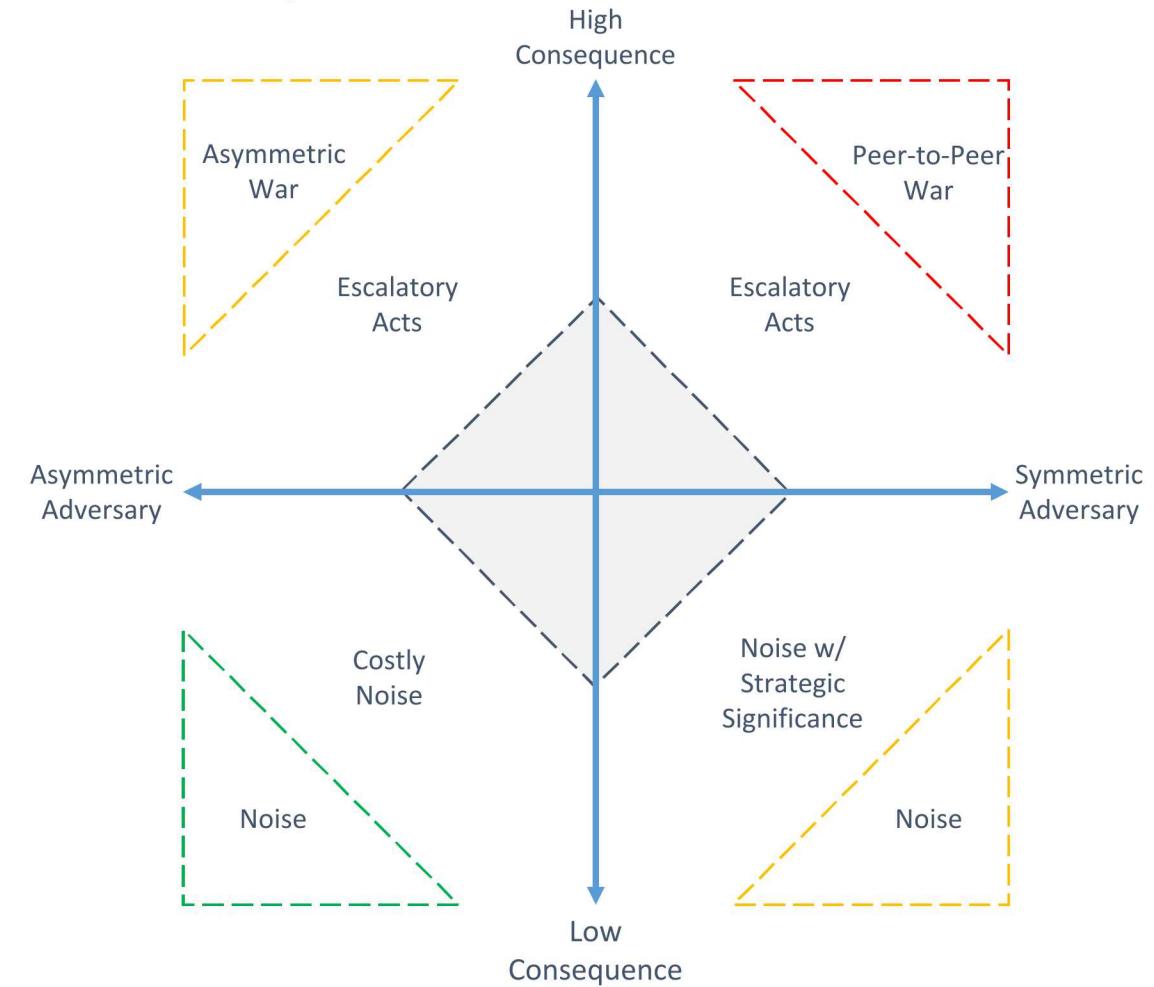
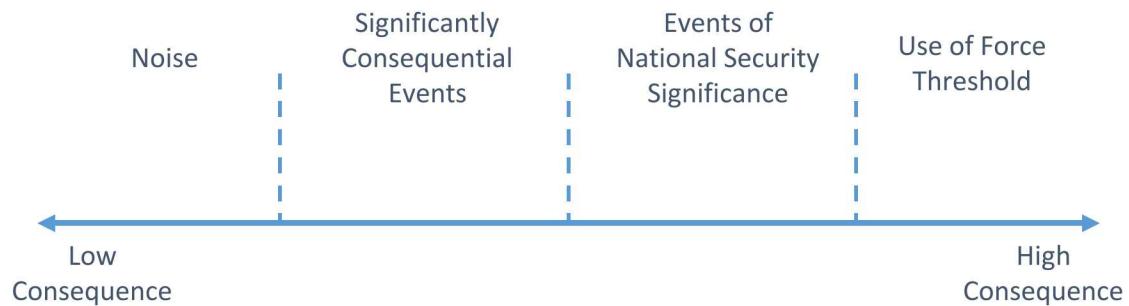


U.S. CYBERCOM Command Vision (2018)

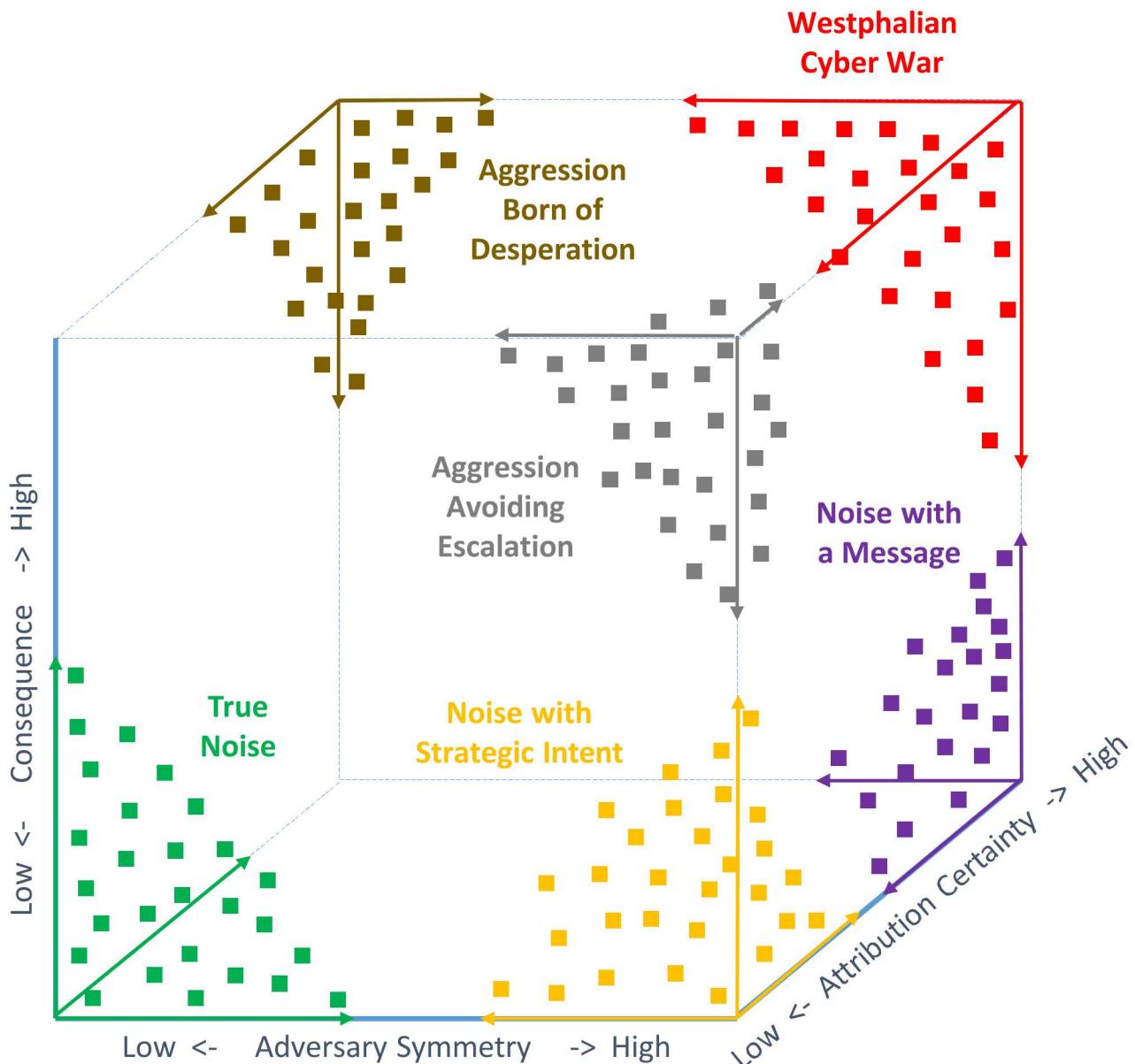
“Adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages.”

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.

How can we analyze this space systematically?



Example Deterrence Mechanisms



DENIAL

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



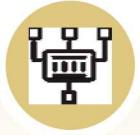
ENTANGLEMENT

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.

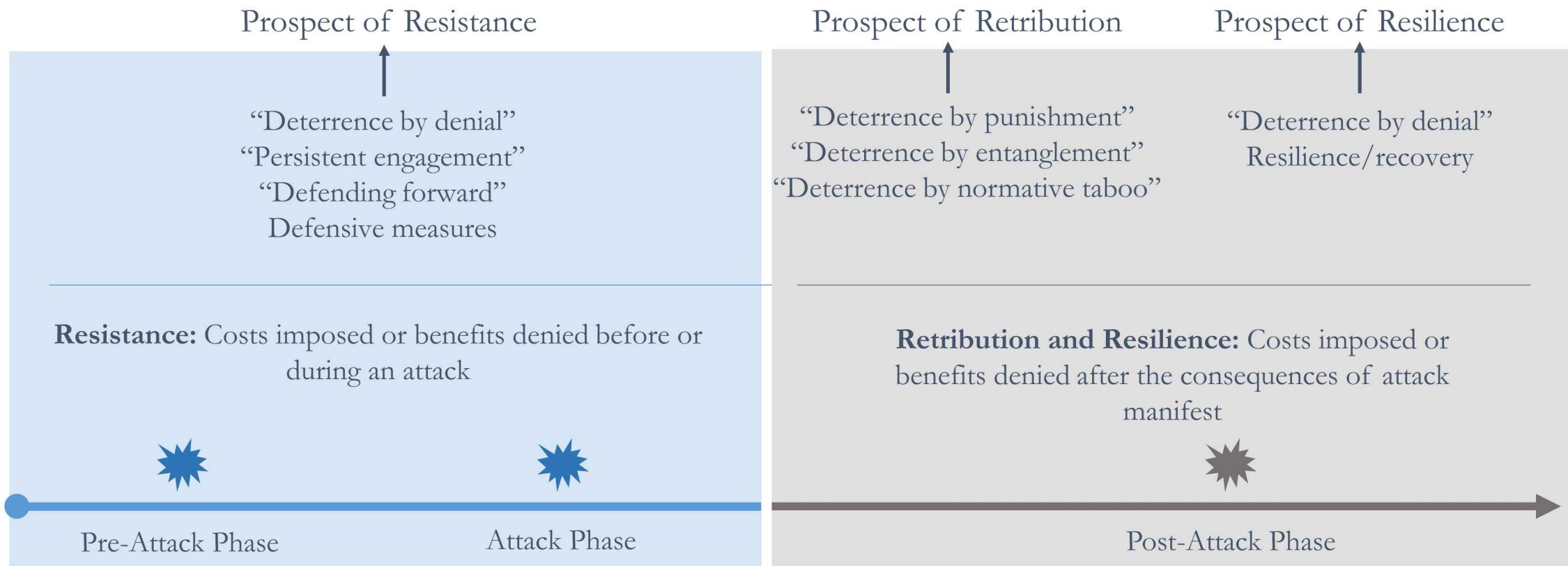
Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies*, 40, 1-2 (2015) 92-117.

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



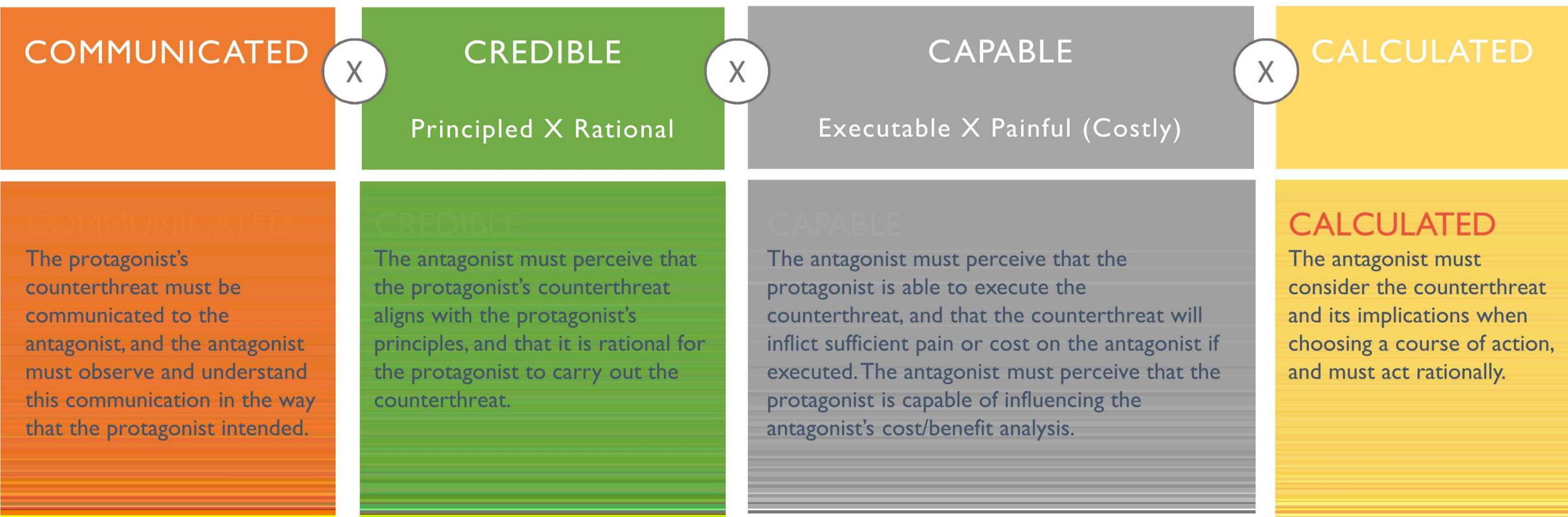
For all deterrence options, capabilities can (and in many cases should) be developed, demonstrated, and communicated well before an attack takes place.

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 following components:



The cyber deterrence framework and example scenario





Red vs. Blue

(upset status quo)

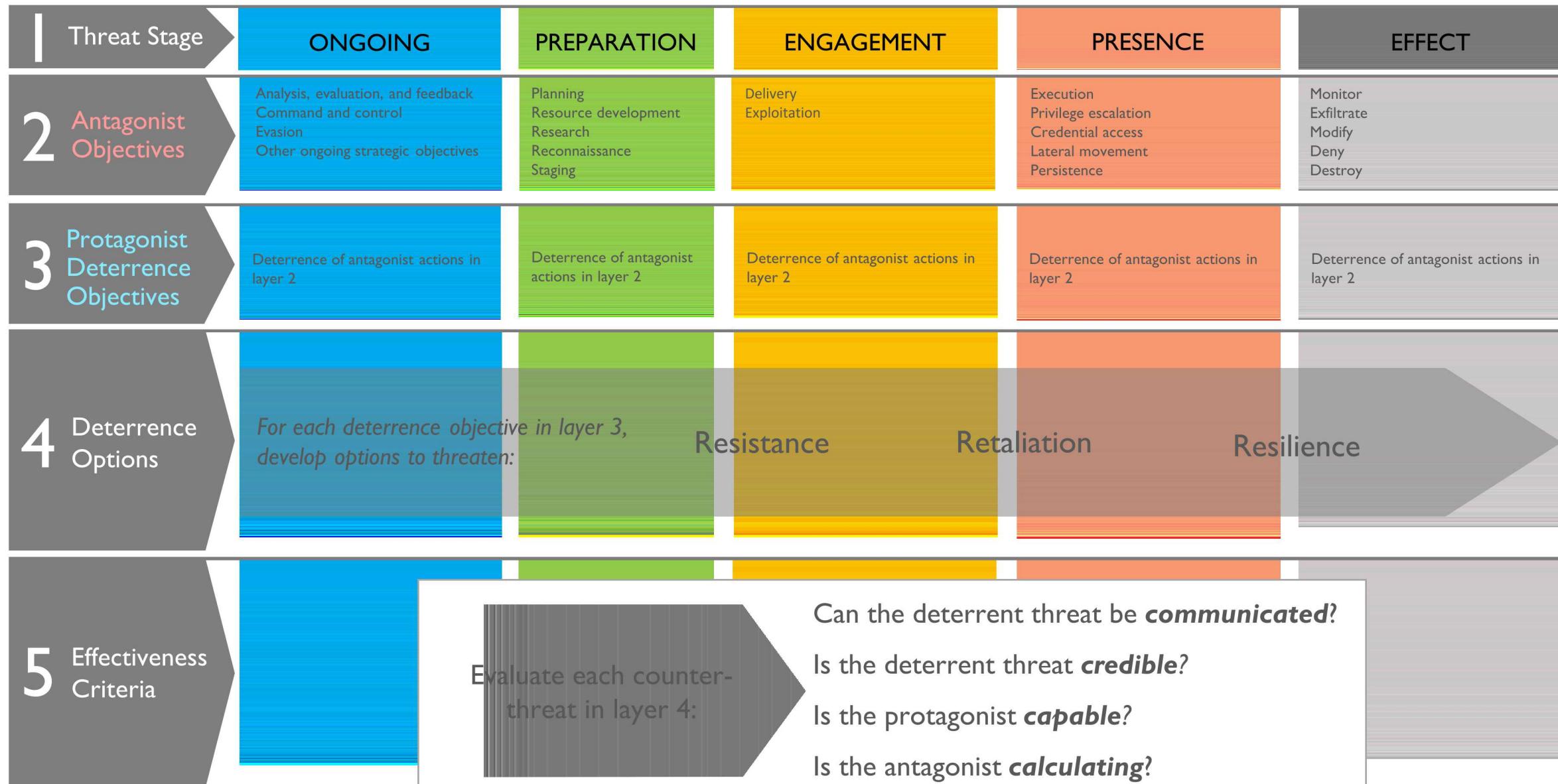
(maintain status quo)

The cyber deterrence framework helps us understand:

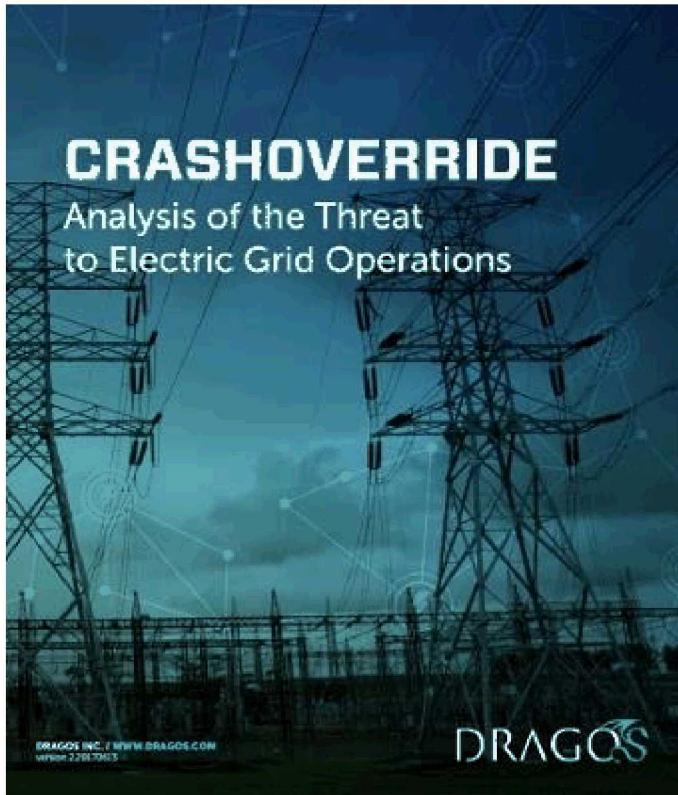
1. Which strategies can **Blue** employ to deter or dissuade **Red** from attacking in the first place?
2. Which deterrence actions are feasible for **Blue** to implement?
3. Which deterrence actions can influence **Red** cost/benefit analysis?

CYBER DETERRENCE FRAMEWORK

MITRE ATT&CK™



We used open source resources for our trial scenario



ICS Defense Use Case No. 6: Modular ICS Malware

August 2, 2017



Official website of the Department of Homeland Security

CISA
cybersecurity.dhs.gov

HOME ABOUT ICS-WG INFORMATION PRODUCTS TRAINING FAQ

Control Systems

Alert (IR-ALERT-H-16-056-01)
Cyber-Attack Against Ukrainian Critical Infrastructure
Original release date: February 25, 2016 | Last revised: August 23, 2016

More Alerts

Print [Twitter](#) [Send](#) [Report](#)

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp>.

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the companies' computer networks, however it is important to note that the role of BE in this event remains unknown pending further technical analysis.

An interagency team comprised of representatives from the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation traveled to Ukraine to collaborate and gain more insight. The Ukrainian government worked closely and openly with the U.S. team and shared information to help prevent future cyber-attacks.

This report provides an account of the events that took place based on interviews with company personnel. This report is being shared for situational awareness and network defense purposes. ICS-CERT strongly encourages organizations across all sectors to review and apply the mitigation strategies listed below.

Additional information on this incident including technical indicators can be found in the TLP GREEN alert (IR-ALERT-H-16-043-01P and subsequent updates) that was released to the US-CERT secure portal. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov.

CYBER DETERRENCE FRAMEWORK

MITRE ATT&CK™



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					

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

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

