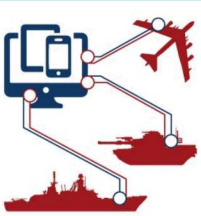
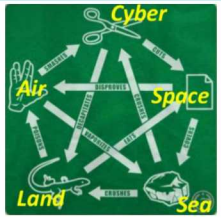
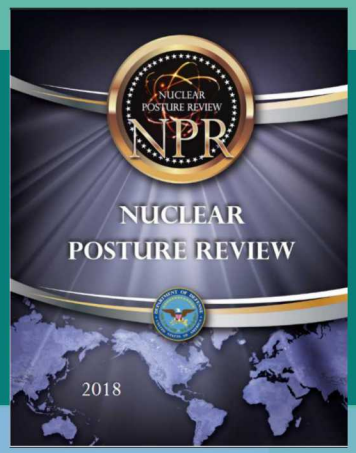
SAND2019-4413PE

Cross-Domain Deterrence







PRESENTED BY

Celeste A. Drewien, Ph.D.

Presentation to US Air Force Academy
April 26, 2019

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.

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.

What is Cross-Domain Deterrence?

- What is deterrence?
- What are domains?
- Definition of cross-domain deterrence

The Morass of Terms

Coercion Use of threat to influence another's behavior

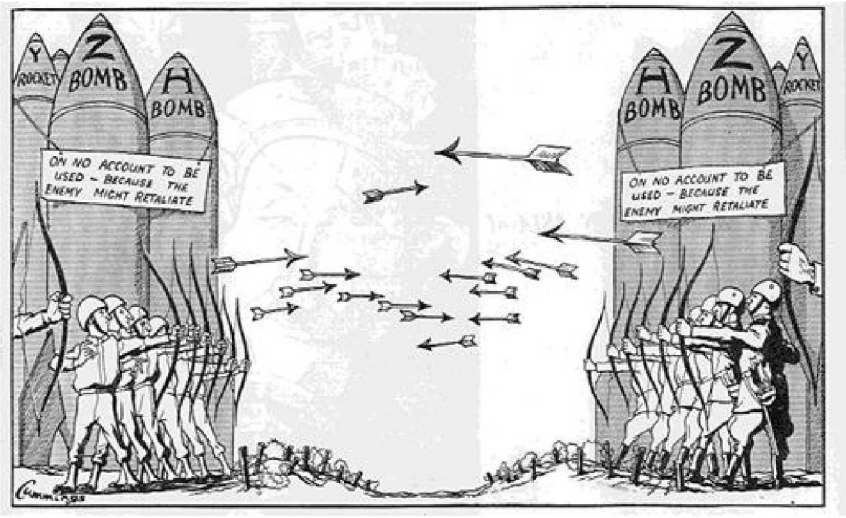
= Deterrence & Compellence

Deterrence Threat made to cause opponent not to take a certain action

Threats can be implicit or explicit

Compellence Threat made to cause opponent to take an action—to comply

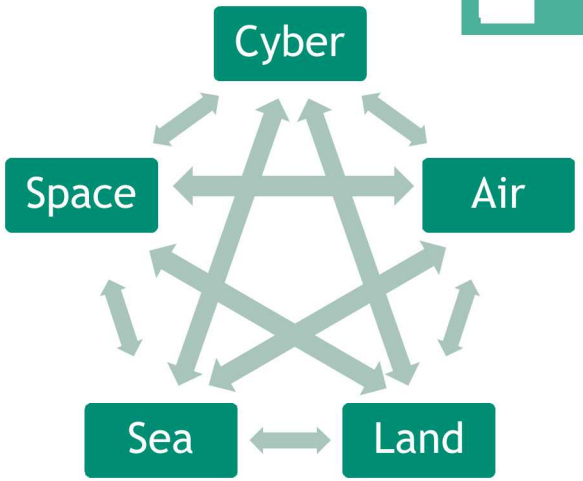
Cold War and Nuclear Deterrence



Mutual Assured Destruction (MAD)—defense strategy based on concept that neither the US nor adversaries would ever start a nuclear war because the other side could massively retaliate. This drove weapon system and force structure design to ensure a second strike capability.

Flexible response—a range of options are needed to credibly deter a spectrum of adversary attack possibilities—to deter limited wars as well as to deter general wars

Cross-Domains—Platform or Means Perspective



- US doctrine identifies land, air, and sea as domains
- Recent doctrines recognize space and cyber as well
- Assume all five are strategic domains

		US Deterrent Counter-Threat Domain				
		Air	**Land**	**Sea**	**Space**	**Cyber**
Adversary Threat Domain (Attack domain)	**Air**	Air-Air	Air-Land	Air-Sea	Air-Space	Air-Cyber
	Land	Land-Air	Land-Land	Land-Sea	Land-Space	Land-Cyber
	Sea	Sea-Air	Sea-Land	Sea-Sea	Sea-Space	Sea-Cyber
	Space	Space-Air	Space-Land	Space-Sea	Space-Space	Space-Cyber
	Cyber	Cyber-Air	Cyber-Land	Cyber-Sea	Cyber-Space	Cyber-Cyber

Lack of geographical boundaries for space and cyber expand need to deter potential aggression within and across all domains.

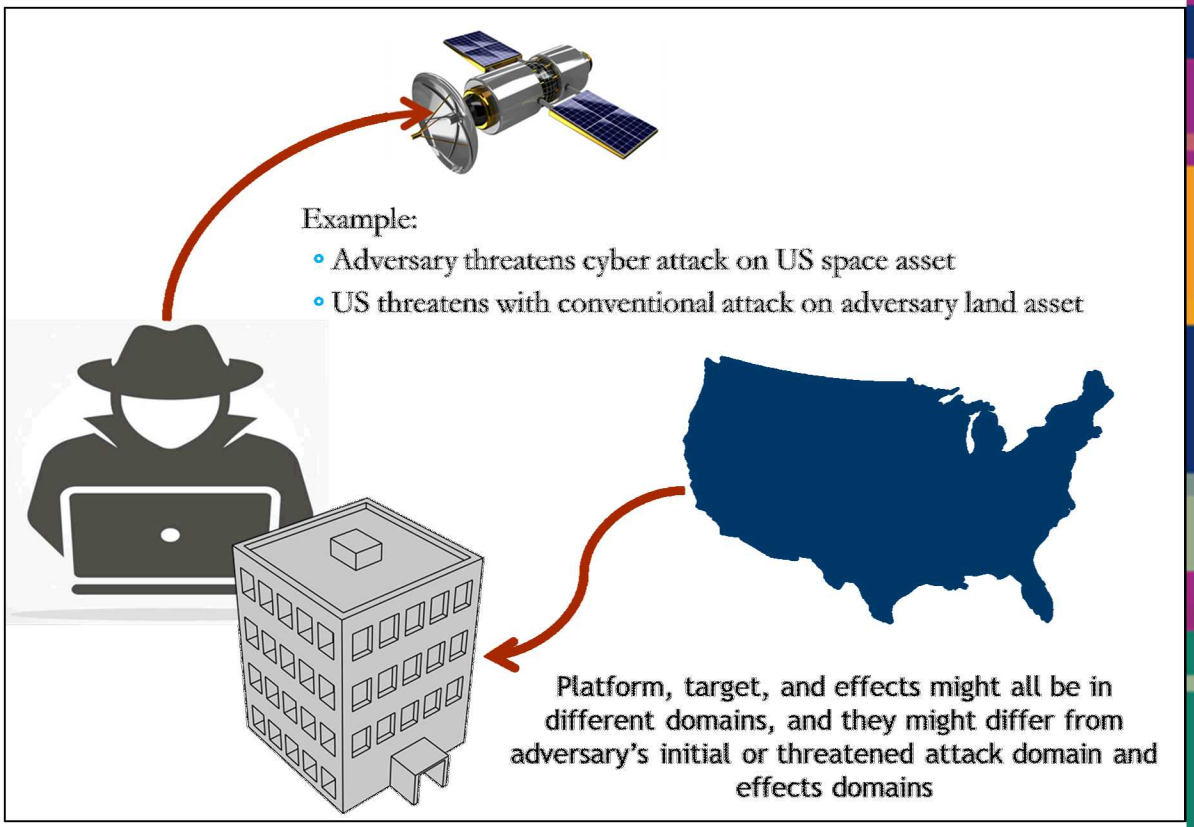
Attack (Platform) Domains versus Effect (Target) Domains

- Domain could be based on
  - Platform (that would be) used to launch attack
  - Where effects of (would-be) attack are manifested

Cross-domain operations occur

Means of attack (platform) may be:
- Conventional munitions
- Non-conventional
- Nuclear
- Chemical
- Biological
- Cyber

Targets can be:
- US or ally
- Civilian or military
- Physical or cyber
- Geo-located or space-based
- People or infrastructure
- Financial/Economic and/or status



Cross-Domain Deterrence

Definition: Cross-domain deterrence is threat of taking action in one domain to deter an adversary from taking action in another domain.

Classical deterrence by:

- Punishment—deter adversary from acting based on fear of punishment
- Denial—deter adversary from acting because their goals will not be achieved

Old Domains and New Domains

- Conventional
- Nuclear

} Air, Land, and Sea Domains

- Cyber Domain
- Space Domain

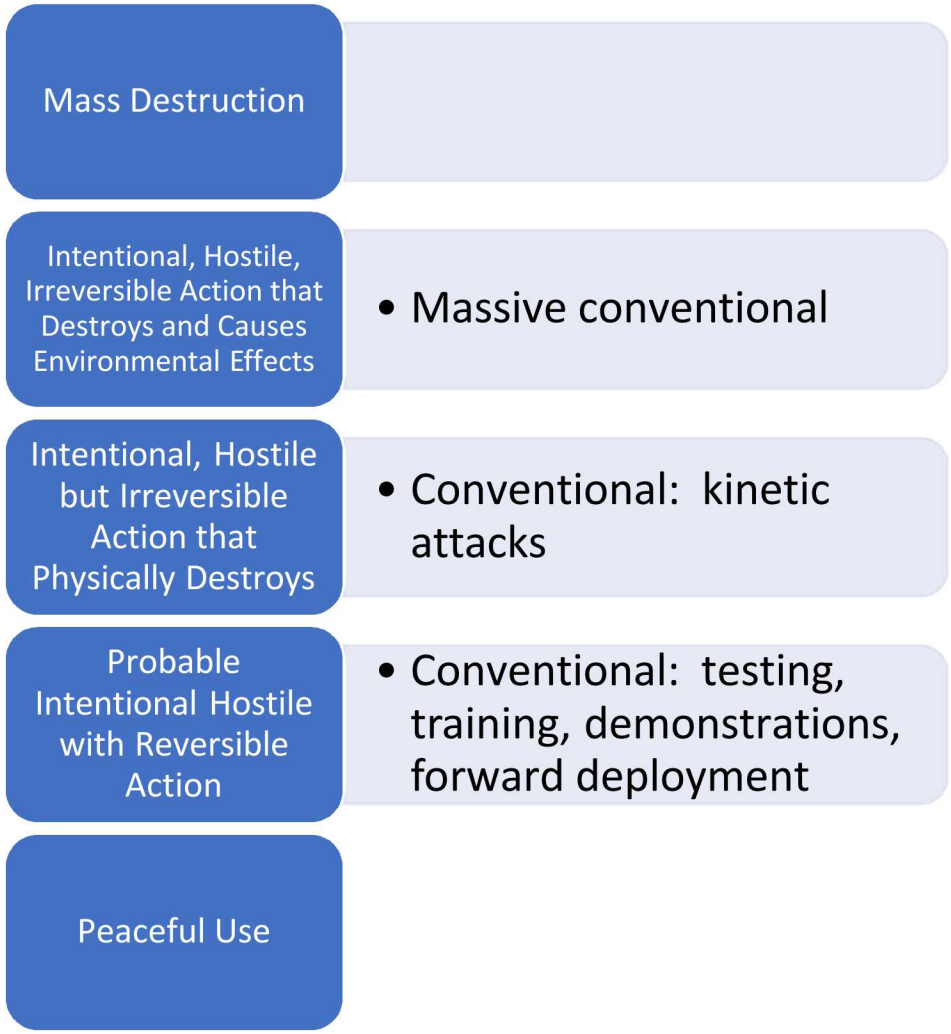
<u>Question</u>

Can domain deterrence by itself be considered or only in conjunction with the overall concept of state or general deterrence?

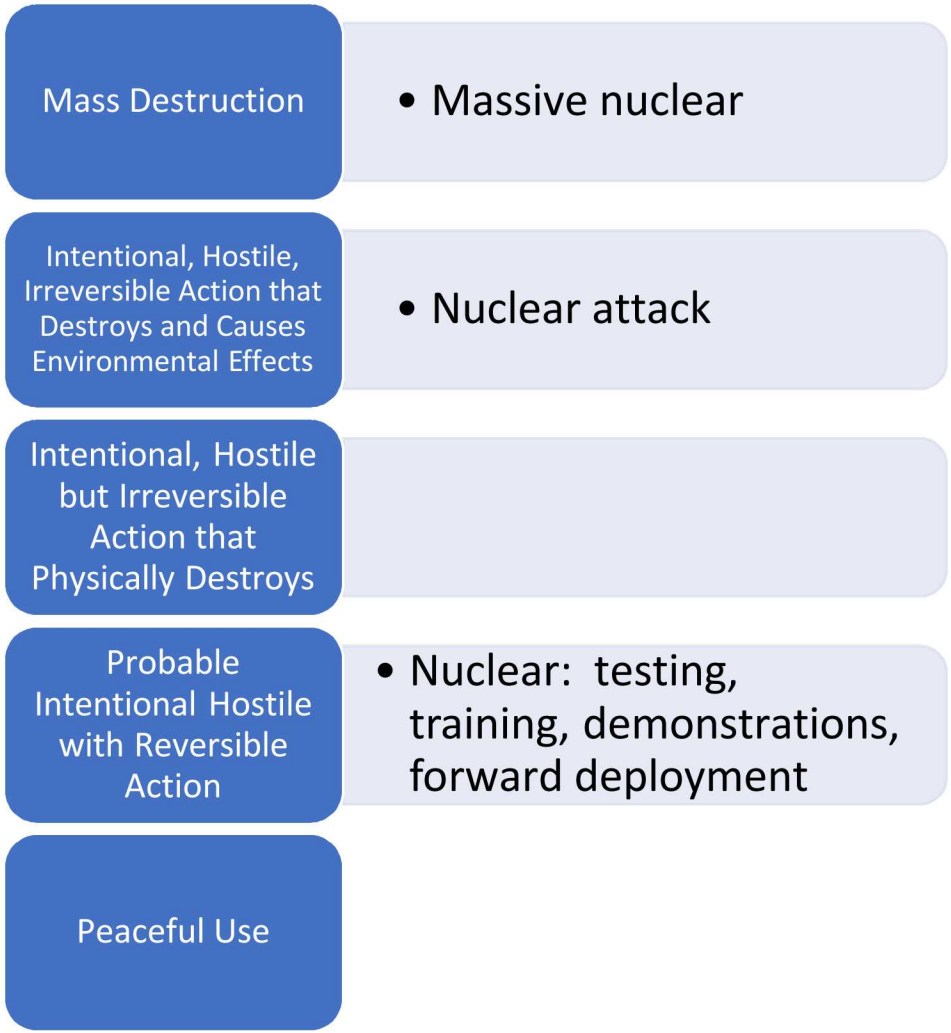
Conventional Domains and Deterrence

- States go to war for specific political goals
  - Intensity of political forces can push state to consider war
- States pay attention to military considerations also, wanting to weigh if they are likely to achieve their goal through conflict.

They may assess that military success is low but still go to war because political calculations dictate the risk is worth taking.



Nuclear Domain and Deterrence



Deterrence by punishment and denial

Cyber Domain Deterrence

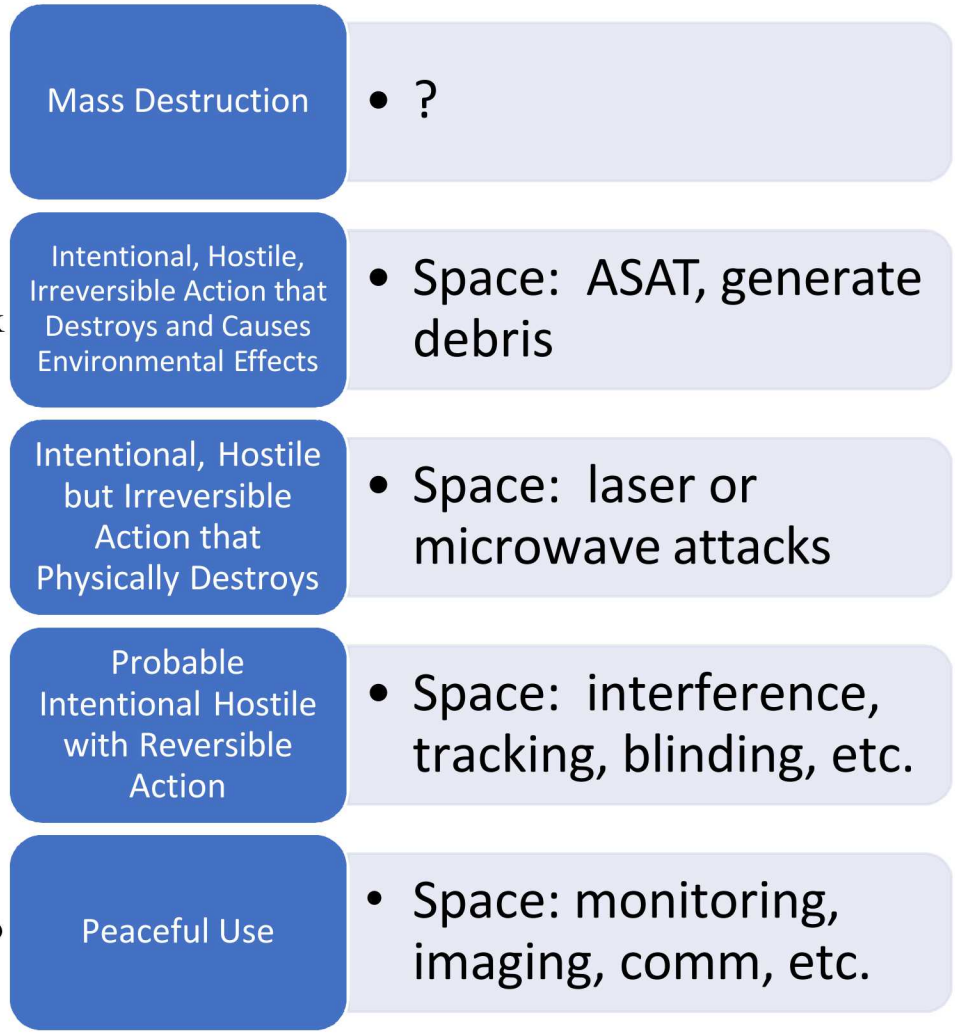
- Deterrence by punishment—difficult, must attribute
  - May hack-back but might be caught and subject to laws
  - Need national law enforcement cooperation to effect deterrence by punishment
- Deterrence by denial possible via artificial intelligence
  - Detect malicious actors and ban them
- Deterrence by association—out the hacker publicly or to call out poor behavior publicly
- Deterrence by norms and taboos—establish agreement to refrain from state-sponsored industrial espionage or intellectual property theft
  - Breaking norm therefore has a social and political cost—lead to sanctions, etc.
- Deterrence by entanglement—cooperate due to reliance on internet, nodes, etc. for economic, diplomatic, and strategic relationships
  - Disincentive for conflict

Mass Destruction	• ?
Intentional, Hostile, Irreversible Action that Destroys and Causes Environmental Effects	• Cyber: damages physical systems that cause effects
Intentional, Hostile but Irreversible Action that Physically Destroys	• Cyber: damages systems, including infrastructure
Probable Intentional Hostile with Reversible Action	• Cyber: data theft, monitoring
Peaceful Use	• Cyber: signals, data, information, etc.

Space Domain Deterrence

- Encompasses more than assets in space—entire system from ground stations to space and back
- Difficult to distinguish intentional, unintentional, and natural events in space
- Actions against ground station and comm link segments can be treated differently from satellites
  - Space attacks that generate debris impact more than just adversary
- Much technology is dual use—so question of intent

- Provides information services for use by all other domains
- Greater importance as critical economic domain than military domain
- Commercial capabilities (can) add resilience to military capabilities



Deterrence by entanglement and norms and taboos?

Challenges of Cross-Domain Deterrence

- Effectively communicating cross-domain threats
- Potential to misconstrue—exploitation vs attack
- Concern for violating laws of war
- Balance of power and stability upset
- Escalation and de-escalation miscalculations

Cross-Domain Deterrence has Credibility and Communication Challenges

Deterrence = Capability + Credibility + Communication

- Capability—US has demonstrated capabilities
- Credibility
  - Is a cyber threat against a nuclear threat credible?
  - Is a nuclear threat against a cyber threat credible?
- Communication
  - Threats in the conventional and nuclear domains exist via signaling and forward deployment
  - How are threats in cyber and space domains communicated?
  - How are threats interpreted?

Potential to Misconstrue Cyber Exploitation for an Attack

- Exploitation → does this cause harm?
  - Monitors and spies on a computer and network systems
  - Copies or steals data or code on these systems
- Attack causes harm
  - Disrupts, denies, degrades, or destroys information, data, code, system or network

- Can exploitation be used for signaling?
- Could exploitation be misconstrued as an attack and cause escalation?

Laws of War: Proportionality and Discrimination Must be Considered

<table>
<tr><th></th><th>Necessity</th><th>Discrimination</th><th>Humanity</th><th>Proportionality</th></tr>
<tr><td>Conventional</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Non-conventional</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Nuclear</td><td rowspan="3">Is there an alternate means?</td><td>Can collateral damage be limited?</td><td></td><td>Could this be excessive?</td></tr>
<tr><td>Chemical</td><td></td><td rowspan="2">US abides by weapons chemical and biological weapons conventions</td><td></td></tr>
<tr><td>Biological</td><td rowspan="2">Can effects be contained?</td><td></td></tr>
<tr><td>Cyber</td><td></td><td></td><td>How is impact measured?</td></tr>
</table>

Cross-Domain Upsets Balance of Power and Stability

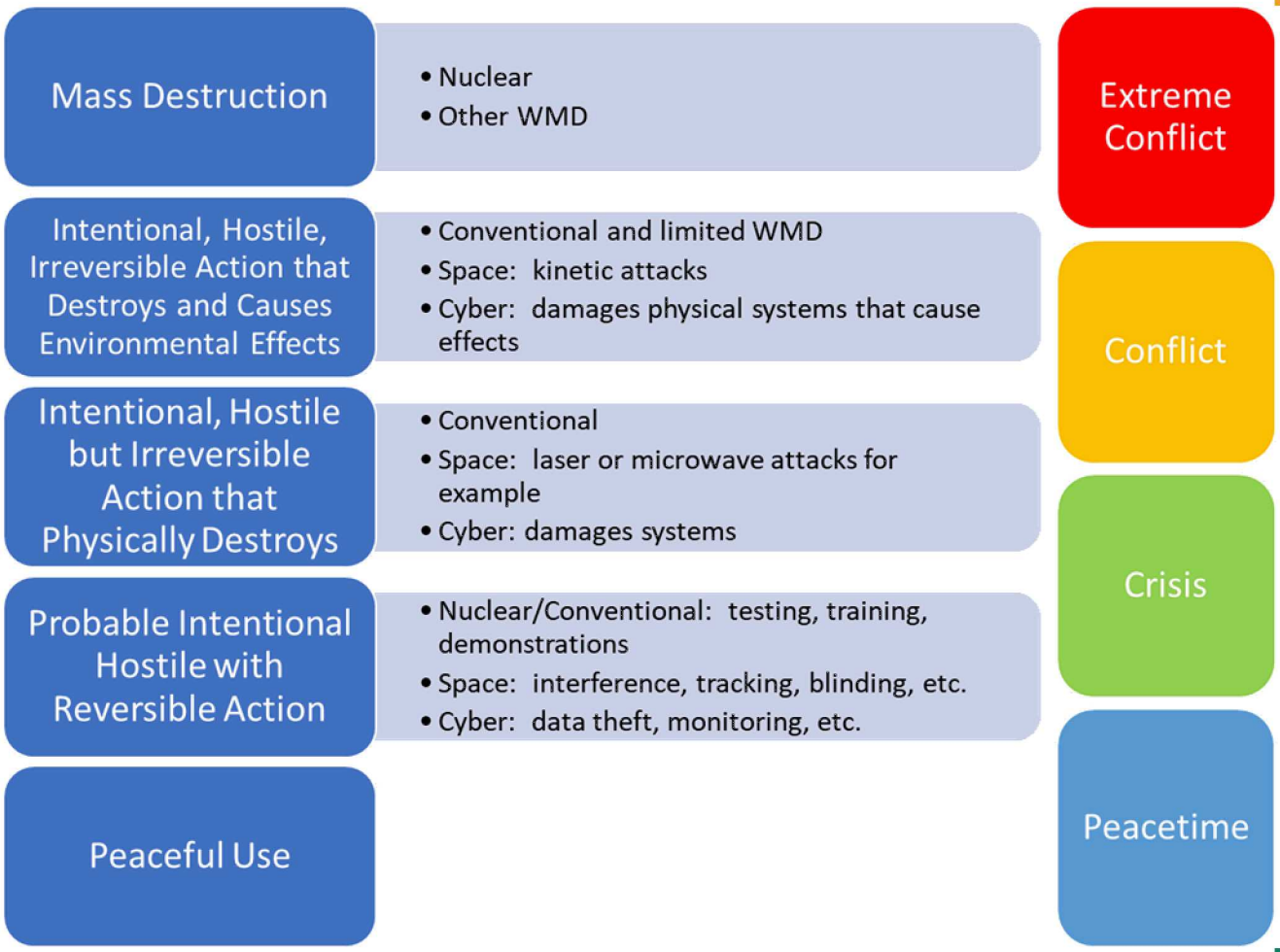
- Balance of power is gauged by numbers and capabilities and ability to defend—equal numbers and capabilities → stability
  - How are numbers and capabilities measured for cyber?
  - Are (sufficient) defensive means available in space?

- Ability to hold assets at risk leads to stability.
  - Must know presence or location of asset.
  - Not all cyber assets are viable targets.
  - General deterrence is therefore hard to affect.

- Asymmetric warfare is possible given new domains.
  - Not all countries possess space assets, so no means to deter or retaliate in the space domain.
  - Space and cyber attacks can be difficult to attribute, so how to deter? How to retaliate?

Escalation and De-escalation Threats Possible in Cross-Domains

- Escalation of threat or action may be needed
  - Ability to deploy more
  - Ability to affect more targets
  - Ability to have greater damage on a target
- Reversible measures may function as form of de-escalation
  - Ability to recall troops or systems
  - Ability to reverse an action taken in cyberspace
  - Ability to restore denied space asset functionality, or temporary impact



How does adversary interpret threat or action?

Summary

- Cross-domain deterrence involves implicit or explicit threat of taking action in one domain to deter an adversary from taking action in another domain.
  - Many weapon systems and most military operations access multiple domains.
- Cross-domain deterrence presents many challenges.
  - Communications, escalation, laws of war
  - Containment of and understanding effects
- Classical deterrence
  - Deterrence by punishment
  - Deterrence by denial
- Modern deterrence additions to the suite of deterrence strategies available in purely military domains
  - Deterrence by norms and taboos
  - Deterrence by entanglement

Recommended Reading

- "WHEN IS COERCION SUCCESSFUL? And Why Can't We Agree on It?" Patrick C. Bratton, Naval War College Review, Summer 2005, Vol. 58, No. 3; https://apps.dtic.mil/dtic/tr/fulltext/u2/a521130.pdf
- Flexible Response: General Maxwell Taylor's book, The Uncertain Trumpet, 1959; https://apps.dtic.mil/dtic/tr/fulltext/u2/a511036.pdf
- "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?" By Manzo, Vincent, Strategic Forum; https://www.questia.com/library/journal/1G1-291503426/deterrence-and-escalation-in-cross-domain-operations
- "New Challenges in Cross-Domain Deterrence", Mallory King, RAND Corporation, Perspective, (Santa Monica: CA, RAND Corporation, 2018); https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE259/RAND_PE259.pdf
- Conventional Deterrence: An Interview with John J Mearsheimer, conducted 15 July 2018; https://www.jstor.org/stable/26533611?seq=1#metadata_info_tab_contents
- Nuclear Deterrence: "Defending the Record on US Nuclear Deterrence", Kevin P. Chilton, Strategic Studies Quarterly (Spring 2018), p. 12; https://go.galegroup.com/ps/i.do?v=2.1&it=r&sw=w&id=GALE%7CA532528725&prodId=AONE&sid=googleScholarFullText&userGroupName=cobleskill
- "Five Kinds of cybersecurity", N. J. Ryan, Philosophy and Technology, September 2018, vol. 31, Issue 3, pp. 331-338; https://link.springer.com/article/10.1007/s13347-016-0251-1
- "Contested Space Operations, Space Defense, Deterrence, and Warfighting: Summary Findings and Integration Report", Dr. Allison Astorino-Courois et al., NSI, July 2018; https://apps.dtic.mil/dtic/tr/fulltext/u2/1066708.pdf