Cyber Persistence:

Re-thinking Security and Seizing the Strategic Cyber Initiative

Professor Richard J. Harknett

University of Cincinnati, Dept. of Political Science,

US-UK Fulbright Professor in Cyber Security, Oxford University, UK (2017)

contact info: richard.harknett@uc.edu

National Academies of Sciences, Engineering, Medicine, Decadal Survey of Social & Behavioral Sciences for Applications to National Security, October 11, 2017

For more see, M. Fischerkeller and R. Harknett, “Deterrence is Not a Credible Strategy for Cyberspace,” *Orbis* 61 3 (Summer 2017): 381-393

Central Thesis (BLUF)

- We live in a world of growing cyber persistence. Our adversaries seem to have recognized this condition, while our current strategy and much of our academic research has not. We have remained locked incorrectly in a deterrence paradigm.

- This strategic environment represents a **new seam** of international competition that may allow a significant shift in the distribution of power, if the U.S. does not align its strategic approach correctly to the structural realities of cyberspace.

- As nuclear weapons <u>precluded defense</u> and necessitated a shift to a strategy of nuclear deterrence to secure the nation, cyberspace <u>precludes deterrence</u> and necessitates a new strategy of cyber persistence.

Strategic Misalignment

- The 2011 *International Strategy for Cyberspace* and *2015 DoD Cyber Strategy*, which commit the United States to a “doctrine of restraint,” cannot succeed in making our nation more secure because they do not map to the structural realities of cyberspace.

- This doctrine of restraint and strategy of cyber deterrence distort our capabilities development, our decision-making models, and our operational impact. As they inhibit us from playing to our strengths, our adversaries have seized the initiative.

Strategy v. Effect—we are conflating the two

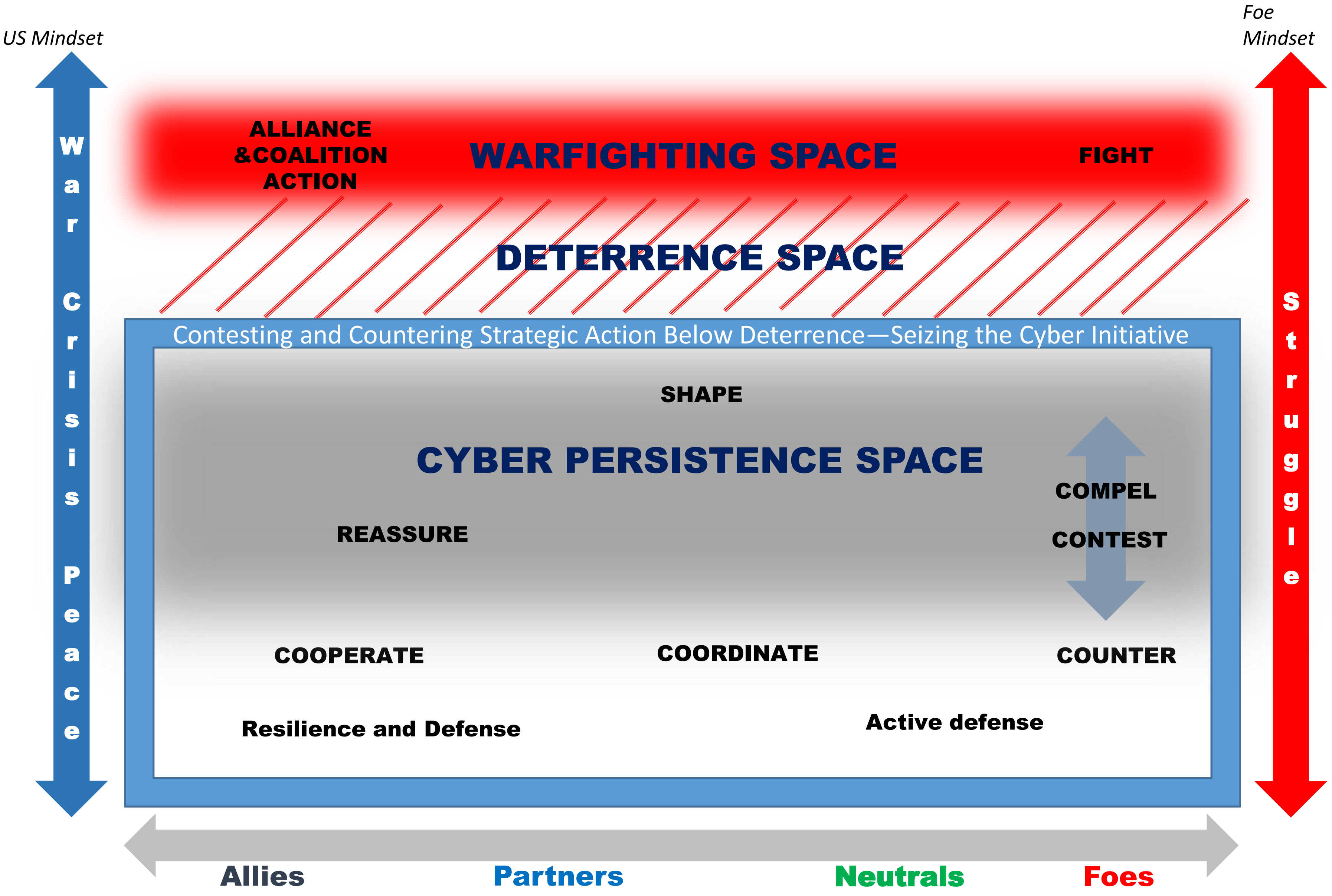
- Strategy of deterrence
  - Communication of a promise to react to a designated unacceptable action by an adversary in such a way as to convince the adversary that not taking the action will advance their interests more than taking the action.

- Deterrence effect
  - an actor is actually persuaded *not to execute* a course of action

- Deterrence effects can be generated directly, indirectly, or residually
  - <u>directly</u> through an adversary-specific strategy of deterrence;
  - <u>indirectly</u> through strategies of shaping, reassurance, deterrence of others and compellence;
  - <u>residually</u> through effective operations, including defense, active defense, countering, and contesting.

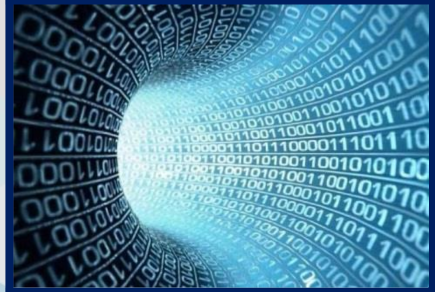
Strategists must take care not to couple a deterrence effect with <u>only</u> a strategy of deterrence

Seizing Cyber Initiative – Strategic Interactions Below Deterrence



Three distinct strategic environments

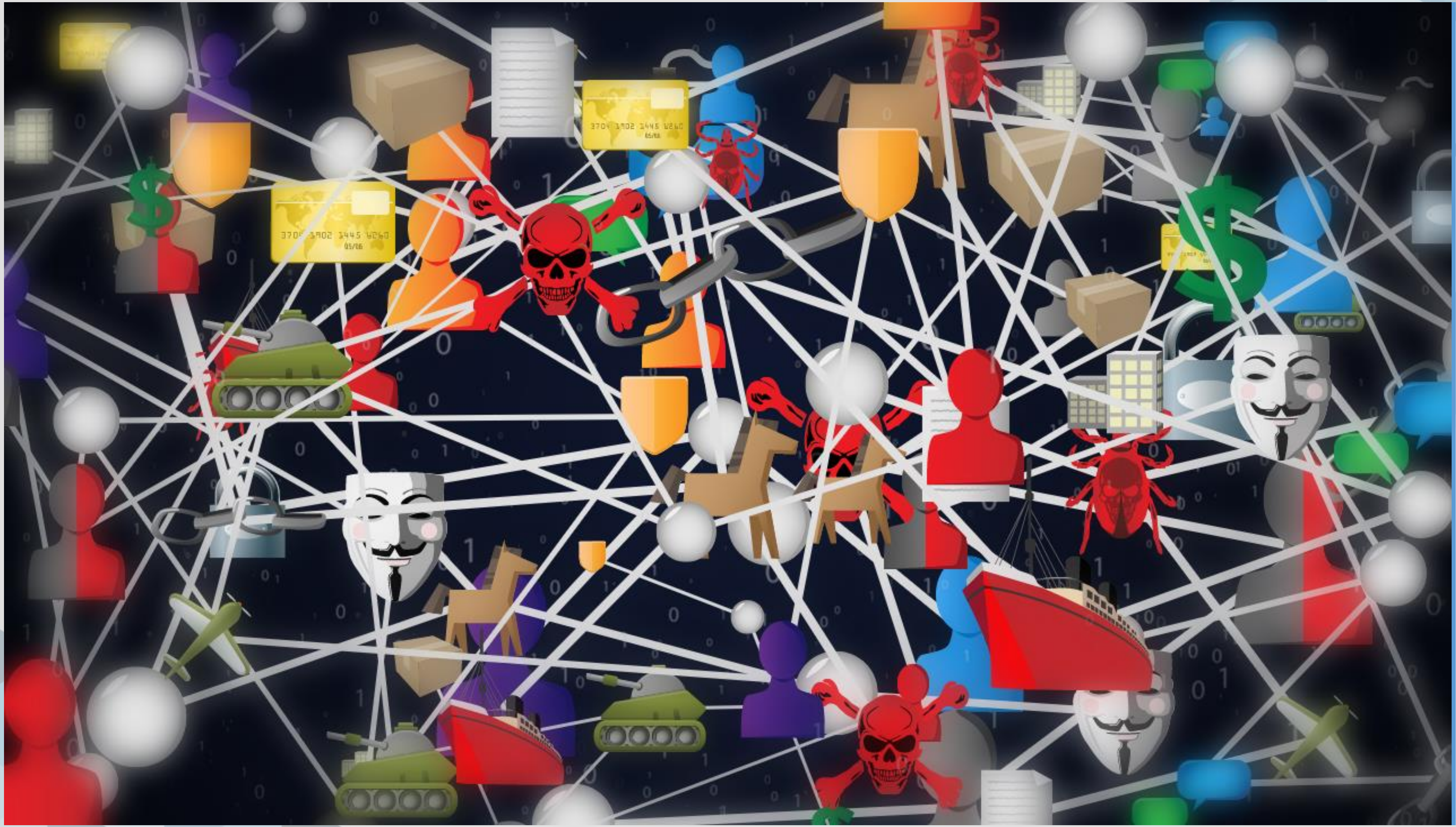
Strategic environments are structures that shape fundamental dynamics and the strategies that produce security.

	NUCLEAR	The ultimate offense-dominant strategic environment.
	CONVENTIONAL	Range from offense-advantaged (blitzkrieg) to defense-advantaged (trench warfare).
	**CYBER**	An offense-persistent strategic environment. You can defend, but you cannot attrite. The offense will persist.

Persistence as a systemic dynamic in cyberspace

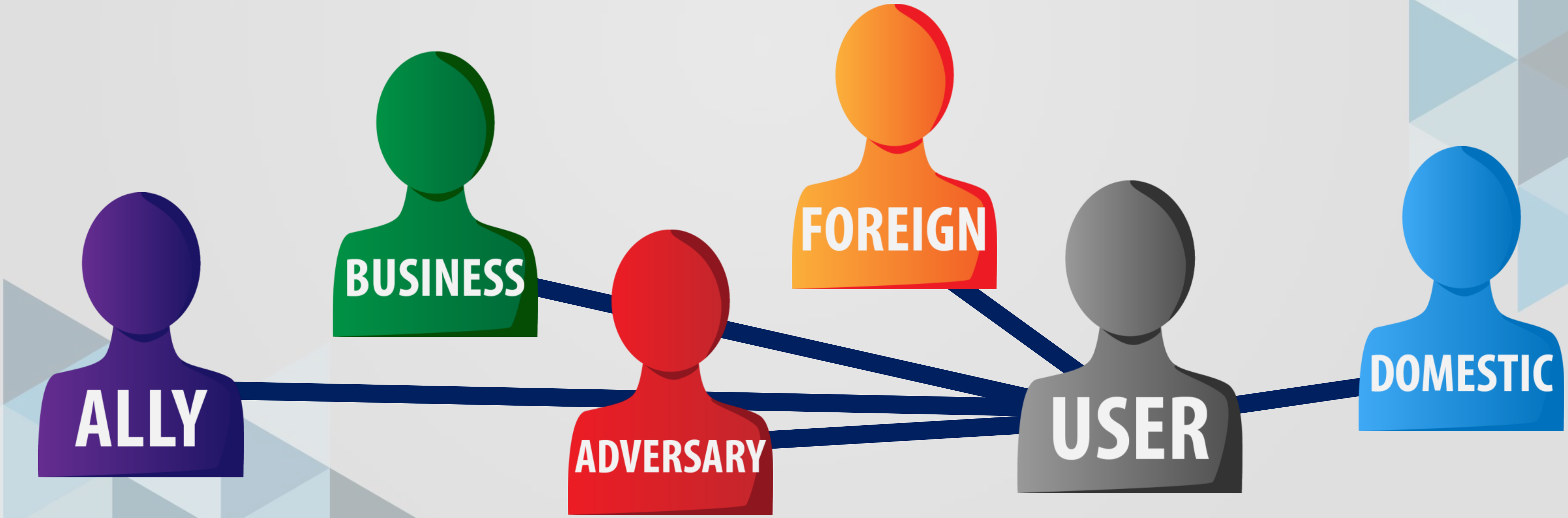
An offense-persistent environment is one in which you can defend, but you defend only in the moment, and the cumulative effect of this defense has little impact on the overall scale and scope of adversarial capacity to act. You can't attrite for security; thus, you must persist operationally.

It is structurally INTERCONNECTED, so we need strategies and organizations of interconnectedness

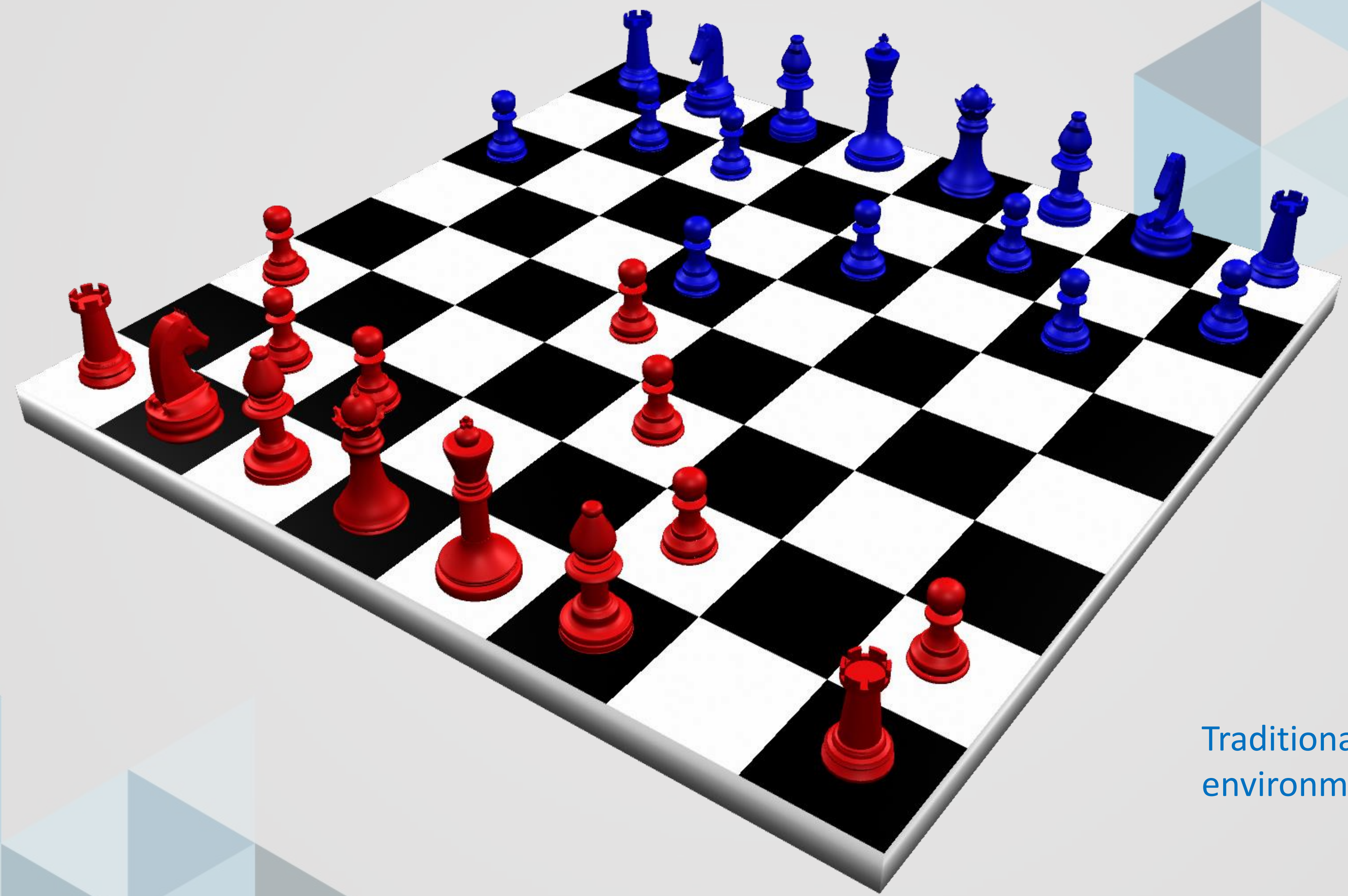


Interconnectedness creates a Condition of Constant Contact

Changes the question: How do I secure when I am in constant contact with the adversary, the ally, the business sector, the foreign and domestic civilian? To operate <u>in</u> this space, segmentation is not the answer.

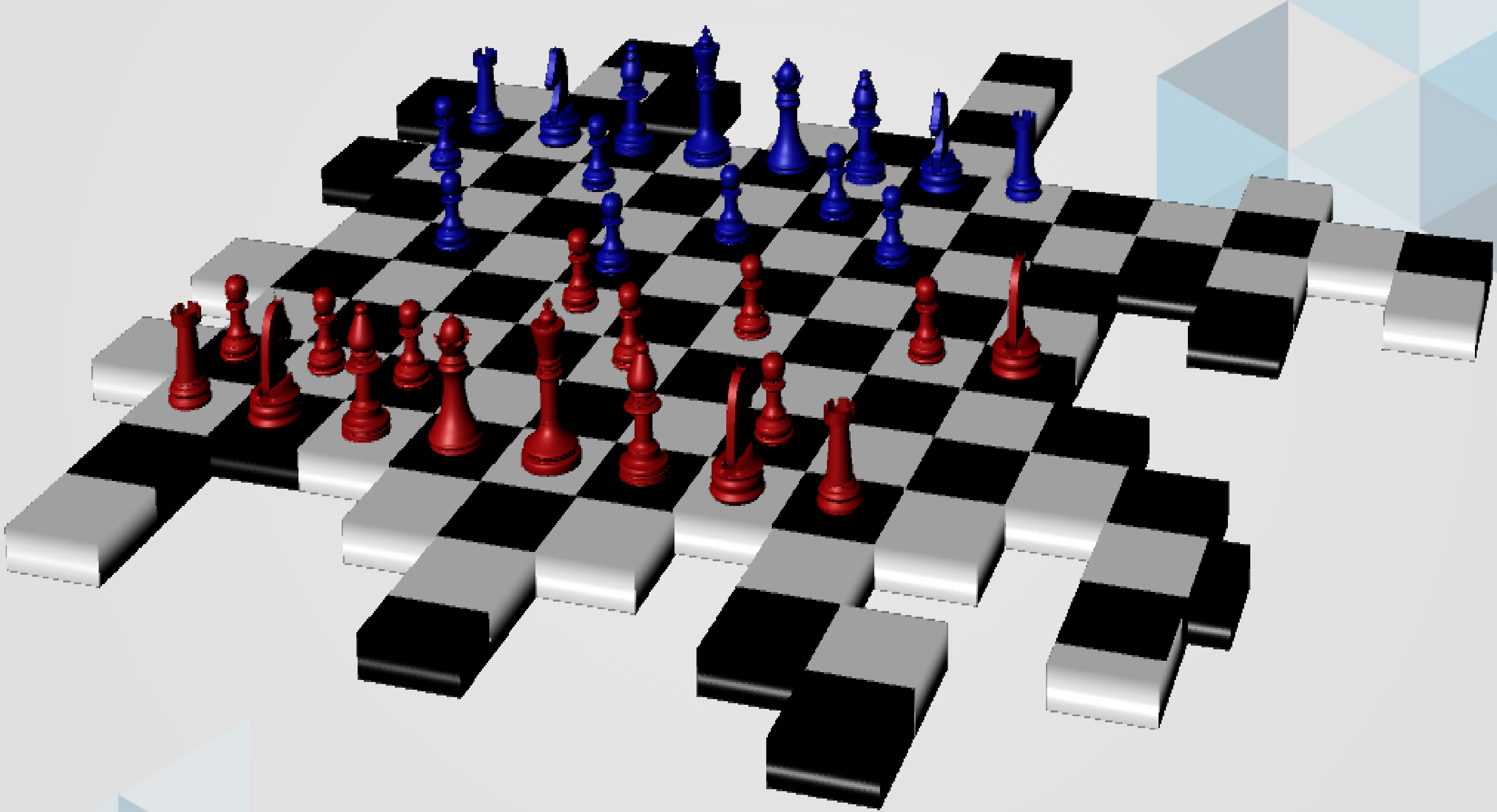


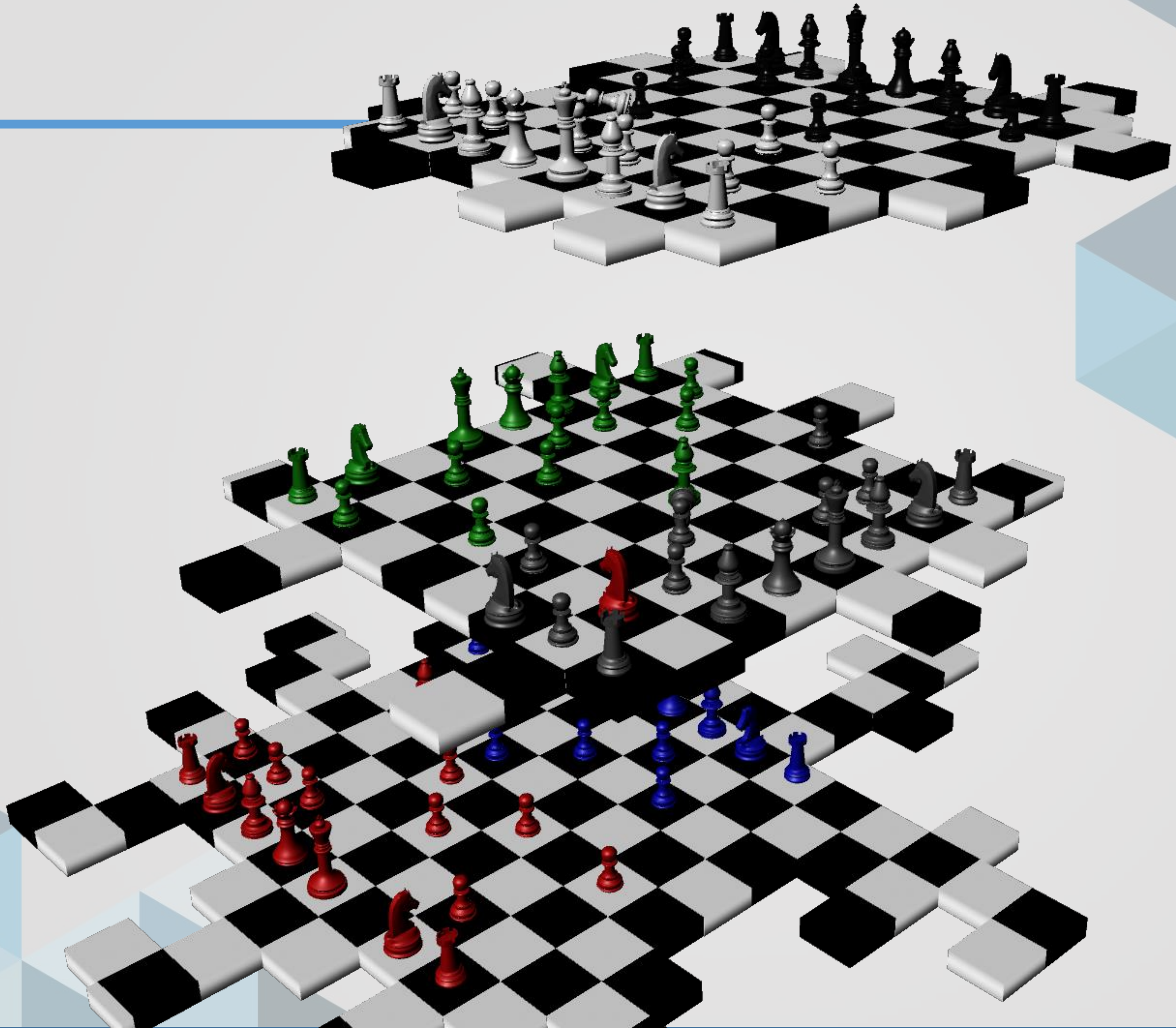
Differently motivated players on a continuously iterating terrain of space and means



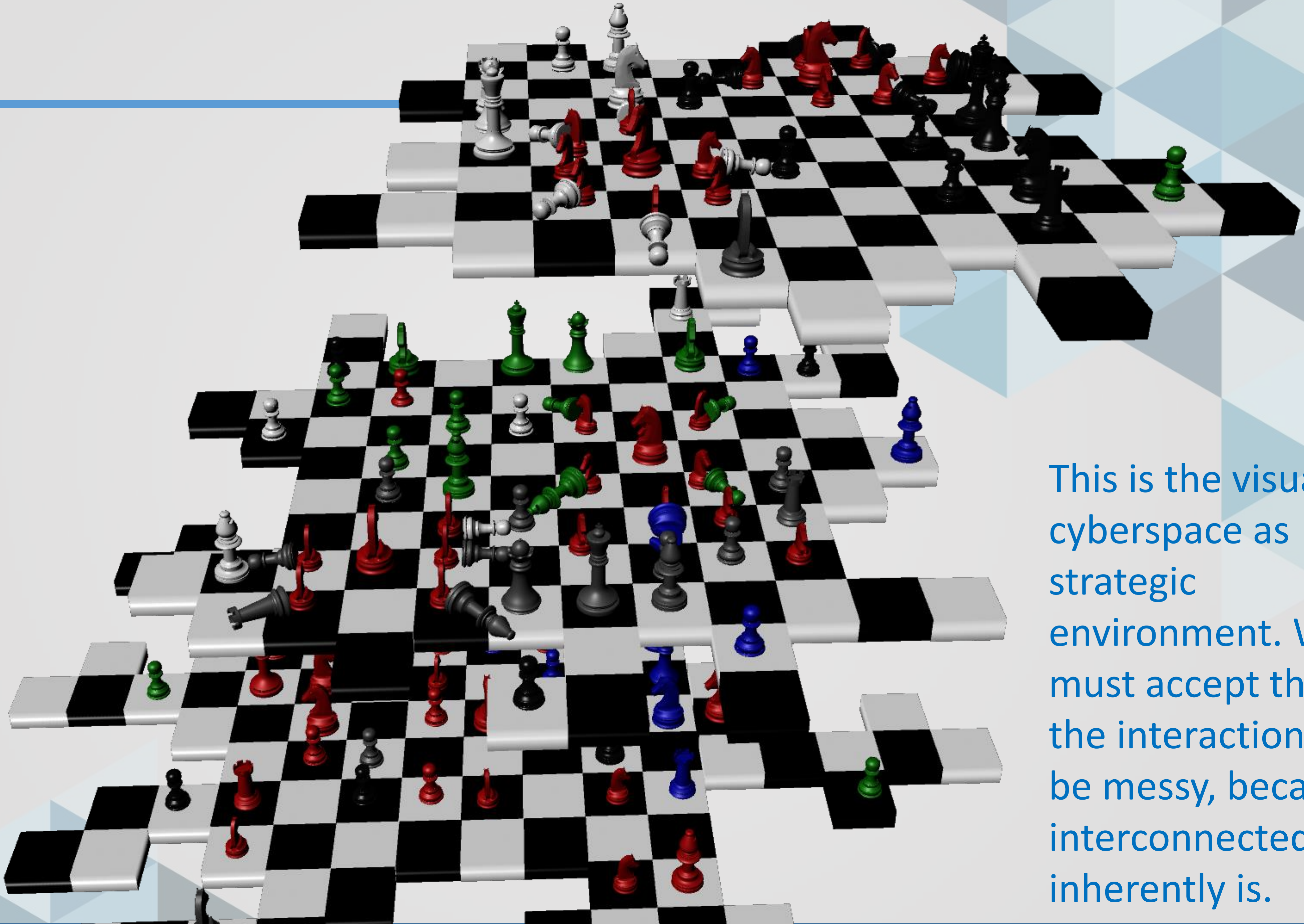
Traditional visual of a strategic environment.

Every new version, hardware or process update changes the terrain in which we must achieve security





The national security-focused state is not primarily driving the creation of this terrain, but market forces and individuals are. Their motivations and interests are different, but they are creating seams we must anticipate.



This is the visual of cyberspace as strategic environment. We must accept that the interaction will be messy, because interconnectedness inherently is.

An Offense-Persistent Strategic Environment

Cyberspace is an interconnected domain of constant contact and continuously constructing terrain of space and means that creates a continuous willingness and capacity to seek the initiative. → offense persistent environment

Rethink Security as denying, disrupting, seizing and retaining the **cyber initiative**.

This is an operational space in which security will be found through cumulative action, not through the threat of prospective action.

→Cyberspace is not a deterrence space

A New Security Strategy For New Dynamics

- A strategy of cyber persistence seeks to deny to competitors and retain for oneself the cyber initiative→ You attain it when:
  - Simultaneously anticipating the exploitation of your vulnerability, while leveraging the vulnerability of others.
  - It runs the full spectrum of security practices from resiliency, defense, active defense, counter-capability, and counter-campaign.

In an environment of constant action and universal vulnerability, security is obtained through action and anticipating action.

Note: the measure of success for deterrence is the absence of action, which is not possible in an environment of constant action

Strategic Cyber Persistence

National security planning must assume that actors will seek to disrupt the distribution of power through strategic action in cyberspace—they will seek to level power, rather than balance it.

- Cyber-enabled operations to undermine sources of relative power
- Cyber geo-economic activity to enhance economic wealth
- Cyber grand strategy →

Two competing models:

Open & Inoperable based on information dissemination

V.

National & Segmented based on information control

We know who is strategically interested in the latter, the US must be willing to defend the former, which cannot be taken for granted, but must be strategically pursued.

Back-up slides

Cyber Persistence and Deterrence

Deterrence as Paradigm Shift

The technological revolutionary shift of the atomic bomb, required us to think differently about security.

Question: How do I secure myself when I can’t defend?

Answer: convince the other side not to attack in the first place.

Nuclear Paradigm Shift

Radical departure from thousands of years of national security organizing that had proceeded 1945.

Our security would not rest
primarily in our hands,
but in the heads of our enemy.

A Distinctive Strategic Environment

A simple metaphor that was right: press a button and you get assured destruction. In fact strategic effect in the nuclear environment comes from mere possession, not use.

There is No Cyber Button

Despite Policymakers acting as if there is a cyber button, we have to understand cyberspace as creating a very different flow between strategy, action, and effect.

This is an operational space in which security will be found through cumulative action, not through the threat of prospective action.

→Cyberspace is not a deterrence space

Five Operating Domains:
One of These Things is Not Like the Other

Land, Air, Sea and Space

- Sovereignty
  - Int'l-agreement on jurisdictions over well-defined, fixed boundaries and activities. Boundaries serve as unambiguous thresholds.
- Operational restraint is the domain norm
- Set of actors who can have significant impact is well-known
- Actors' intentions are relatively easy to discern
- Acts are relatively easy to attribute
- Proportional responses/effects are relatively easy to calculate
- Some capabilities in one domain (and national instruments of power) are enabled by or dependent upon other domains

Cyberspace

- Sovereignty
  - No int'l (sub-nat'l) agreement on well-defined, fixed boundaries and/or activities, consequently, ambiguous jurisdiction. No unambiguous thresholds.
- Operational persistence/contact is the domain norm
- Set of actors who can have significant impact is not well-known
- Actors' intentions are relatively difficult to discern
- Acts are relatively difficult to attribute
- Proportional responses/effects are relatively difficult to calculate
- Most capabilities in all other domains (and national instruments of power) are enabled by or dependent upon cyberspace

A strategy of deterrence *does not align* with the operational/operating characteristics of cyberspace that flow from its structure

The Wild Card: we are just getting started

- The most innovative and powerful advances in Machine Learning and Artificial Intelligence will either come from large corporations or China based on current trends and capacity.

- Who controls the most powerful algorithms is a political question, not a market question and control will be contested because of the potential power of algorithmic decision-making.

- AI itself, however, will also be contested space. It will be an asset to possess, but also a space in which to operate. It amplifies the need for constant contact and thus reinforces the space for persistence.