How Strategy Must Align to Strategic Environments: Deterrence and Initiative Persistence

*

Prof. Richard Harknett, PhD
Center for Cyber Strategy and Policy
School of Public and International Affairs
University of Cincinnati

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Bottom Line Upfront– Cyber Persistence Theory

- The reality of State behavior and interaction in cyberspace has been quite different from the model of war and coercion upon which many countries had based their cyber strategies.
- This unexpected reality has developed because security in and through cyberspace rests on a distinct set of features that differ from the dominant security paradigms associated with nuclear and conventional weapons environments.
- Cyber persistence theory posits the existence of a distinct strategic environment supporting the logic of exploitation rather than coercion.
- This represents a Paradigm change—a new set of assumptions, key concepts and methods.
- To achieve security in this cyber strategic environment, States must engage in initiative persistence, continuously setting and maintaining the conditions of security in their favor.
- Alignment to the structural features and strategic opportunities of the cyber strategic environment that emerged from the creation of global networked computing will, in large measure, determine how well States and non-State actors leverage cyberspace to advance their interests and values.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

CONTEXT: Financial Times (London) Report March 9, 2022

- A Public-Private whole of nation-plus operation through Persistent Engagement Hunt Forward activity under Defend Forward Strategy created:

IN COMPETITION, *seized the cyber initiative and thus achieved enhanced security*

- Improved Defense of a foreign friendly network without adversary knowledge
- Improved understanding of adversary TTPs, which remained active
- Anticipatory Resilience of domestic networks through private sector coordination

IN WAR, possibly the first cyber defensive operation that directly saved lives with possible strategic implications for the war-fight depending on Russian planning.

In a deterrence orientation, this operation and effects do not happen

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Aligning Proper Strategy to the Strategic Environment

	**NUCLEAR**	The ultimate offense-dominant strategic environment.
	**CONVENTIONAL**	Ranges from offense-advantaged (blitzkrieg) to defense-advantaged (trench warfare).
	**CYBER**	Initiative Persistent. You can defend, but only in the moment. You cannot attrite.

You cannot impose a strategy on a strategic environment and succeed; you must derive strategy from it.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

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.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

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. It is PROSPECTIVE THREAT that is causal.

Incontestable Costs

It is not the scale of nuclear destruction that makes it an effective deterrent, but that **its scale is incontestable**.

It creates a crystal ball effect for decision-makers.

Contestable Costs

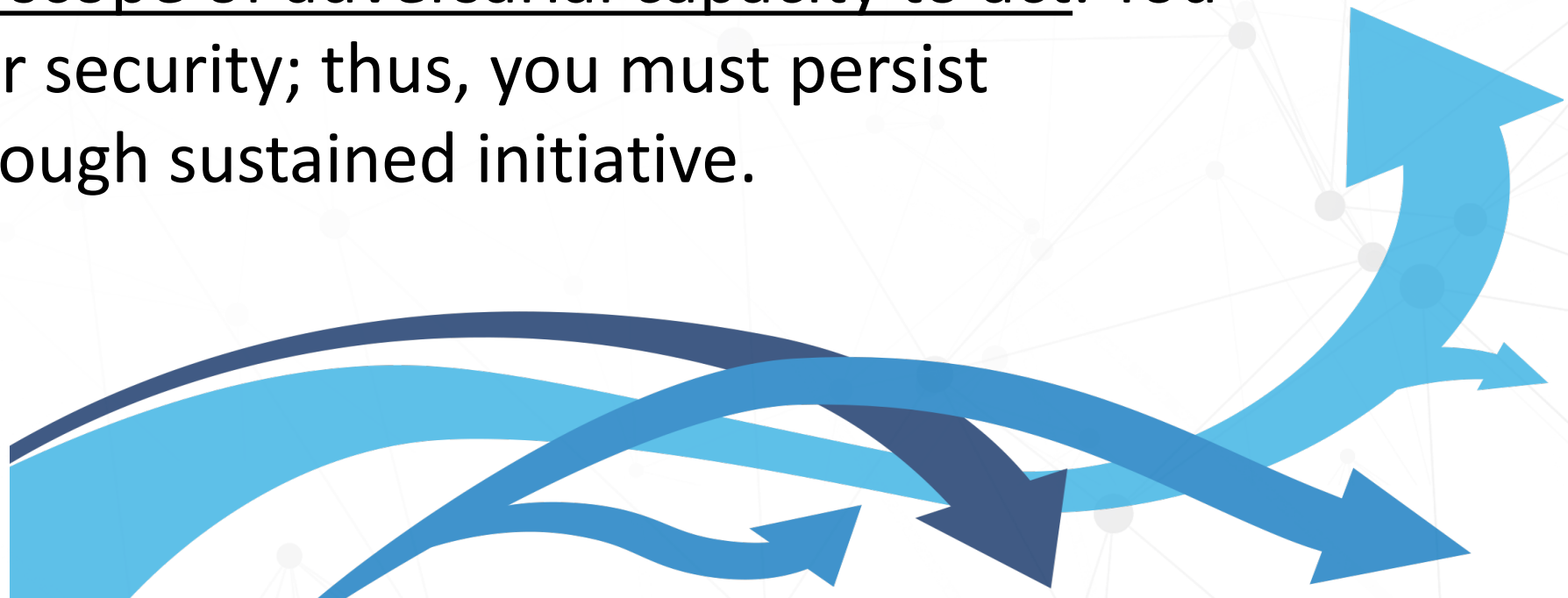
There was no crystal ball at Verdun and despite its scale, there was no way to contemplate such a vision of the future that would dissuade going on the offense again the next day.

(because it was a defense-advantaged strategic environment, attrition ultimately brought the offensives to an end)

A Distinctive Strategic Environment

Initiative Persistence as redefinition of national security

An initiative-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 not attrite for security; thus, you must persist operationally through sustained initiative.



Cyber Persistence Theory: Structuralist perspective

- Structuralist approach meant to clarify core causal dynamics through a parsimonious focus on the systemic structuring of behavior. Behavior is driven by the operational and strategic environments in which the actors find themselves.

- The core elements of the structure of the cyber strategic environment are interconnectedness, constant contact, and a base technology that fluidly reconfigures, is ubiquitously accessible, and inherently vulnerable to unauthorized and unexpected use by others.

- These elements, taken together, structure a space that rewards those who can anticipate the exploitation of vulnerabilities and thus, in structuralist terms, creates an imperative to persist in seeking the initiative (if you have anticipatory capacity, and you use it, you can define the conditions of your own security)

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Cyber Persistence Theory: Core analytical concepts

- There exists an inherent opportunity for exploitation defined as using code to take advantage of others' cyber vulnerabilities for the purpose of gaining strategic advantage. It is the dominant behavior in cyberspace.

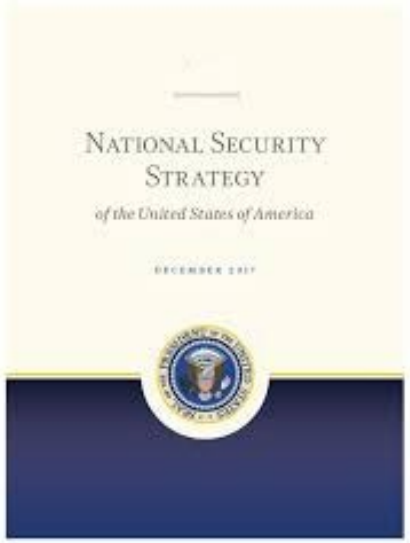
- To date, states are setting and resetting the conditions of security and insecurity *directly through* cyber *fait accompli defined as* a limited unilateral gain at a target's expense where that gain is retained when the target is unaware of the loss or is unable or unwilling to respond.

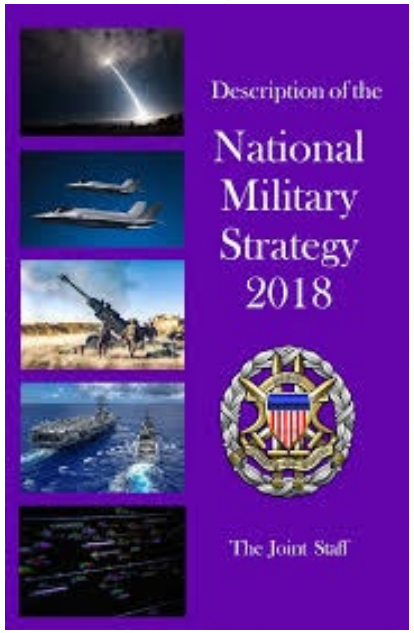
- Under certain conditions, including high value of the network (either in its connectivity and or its data), direct cyber engagement occurs, but much less currently than most assume→ because the opportunity for CFA is too prevalent.

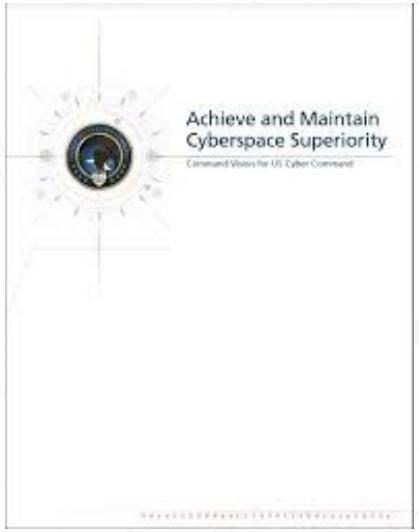
- **Unilateral action** is what is most prevalent and what must be studied, not shaping the calculus of others. The large majority of cyber campaigns are not coercive in intent nor execution.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

2018 Cyber Strategic and Operational Pivot







National Security Presidential Memorandum (NSPM) 13
United States Cyber Operations Policy

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Doctrine of Persistent Engagement

- General Nakasone (Feb 10, 2022) "…defend forward and persistent engagement have become **cornerstones** to our strategy."

- US Persistent engagement seeks "to thwart adversary cyberspace campaigns by continuously anticipating and exploiting their vulnerabilities, while denying their ability to exploit ours. It comprises continuous cyber operations that support resiliency, defend forward, and contesting to sustain strategic advantage." (2018 US Cyber Command Public Affairs Office)

- "In March 2021 the UK published its Integrated Review (IR) of Security, Defense, Development, and Foreign Policy, representing a significant shift in our posture towards persistent global engagement and constant campaigning. The UK will be more proactive, adaptable, and integrated with its partners to compete with adversaries, strengthen deterrence, and improve the ability to intervene and fight decisively." (UK IR 2021)

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Defend Forward
(Active is not Aggressive) (Action is not Offense)

- *We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."* 2018 DoD Cyber Strategy
- Defend Forward is both a geographical and temporal concept.
- It focuses on an aggressor's confidence and capabilities by keeping them on-guard and off-balance.

- 3 LOEs: Warning, Influence, Positioning
- **Warning:** of adversaries' actions and intentions and capabilities allows for better defense and anticipatory resilience. We can change the terrain before they maneuver (cooperate with industry);
- **Influence**: shifts the balance of initiative by the dialing up of organizational friction in the TTPs of the attacker.
- **Positioning**: Defend Forward supports a cyber posture that can be leveraged to persistently degrade the effectiveness of adversary capabilities and blunt their operations before they reach US networks.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

2022 US National Defense Strategy

- NDS calls for campaigning in competition below armed conflict focused on “limiting, frustrating, disrupting competitor activities that seriously affect US interests.” (NDS 2022)

- Cyber “campaigning enables US Cyber Command to generate insights, opportunities, and options that constrain adversary freedom of maneuver and deny them leverage in crisis and conflict. When cyber forces hunt forward on partner networks, tip industry, publicize malign activity, expose malware, they preclude options, reduce attack vectors and deny terrain to malicious actors.” Goldman, Warner, Clark, “US Cyber Command and Integrated Deterrence,” unpublished white paper, (fall 2022) quoted by permission.

- Cyber campaigning to compete **and** structure contingency.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Paradigm Change –the shift is taking root.

Defend and Disrupt, instead of deter

Sustained disruption campaigns

In a strategic competition with China over the fundamentals of the digital space

Focus on the most capable capabilities for collaboration to produce defense, resilience and disruption

Rebalance responsibility and incentives for better practices.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY