# Understanding the Security Challenge of Cyberspace

## The Structure of Cyber Persistence

**Southeast Association of Rail Shippers Annual Meeting**
**October 27, 2021**

Prof. Dr. Richard Harknett
Center for Cyber Strategy and Policy
University of Cincinnati

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

# Morning of a Holiday

Someone with privileged access

Over 30,000 computers data wiped out

...anonymously...

# USB Drive --INSERTED

## Control-room monitoring NORMAL

## Over 900 centrifuges destroyed

## ...anonymously...

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

10 Hours

36,000 ATM transactions

24 Countries

$40 million stolen

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Cincinnati, Ohio

Mom wakes up hearing someone yelling at her baby in the other room.

Dad runs in and the baby monitor camera turns at him and starts yelling.

Someone was watching them.

# Key Points

1. You cannot segment physical/operational security planning from its cyber context. Thus, understanding the dynamics of security in cyberspace is essential;

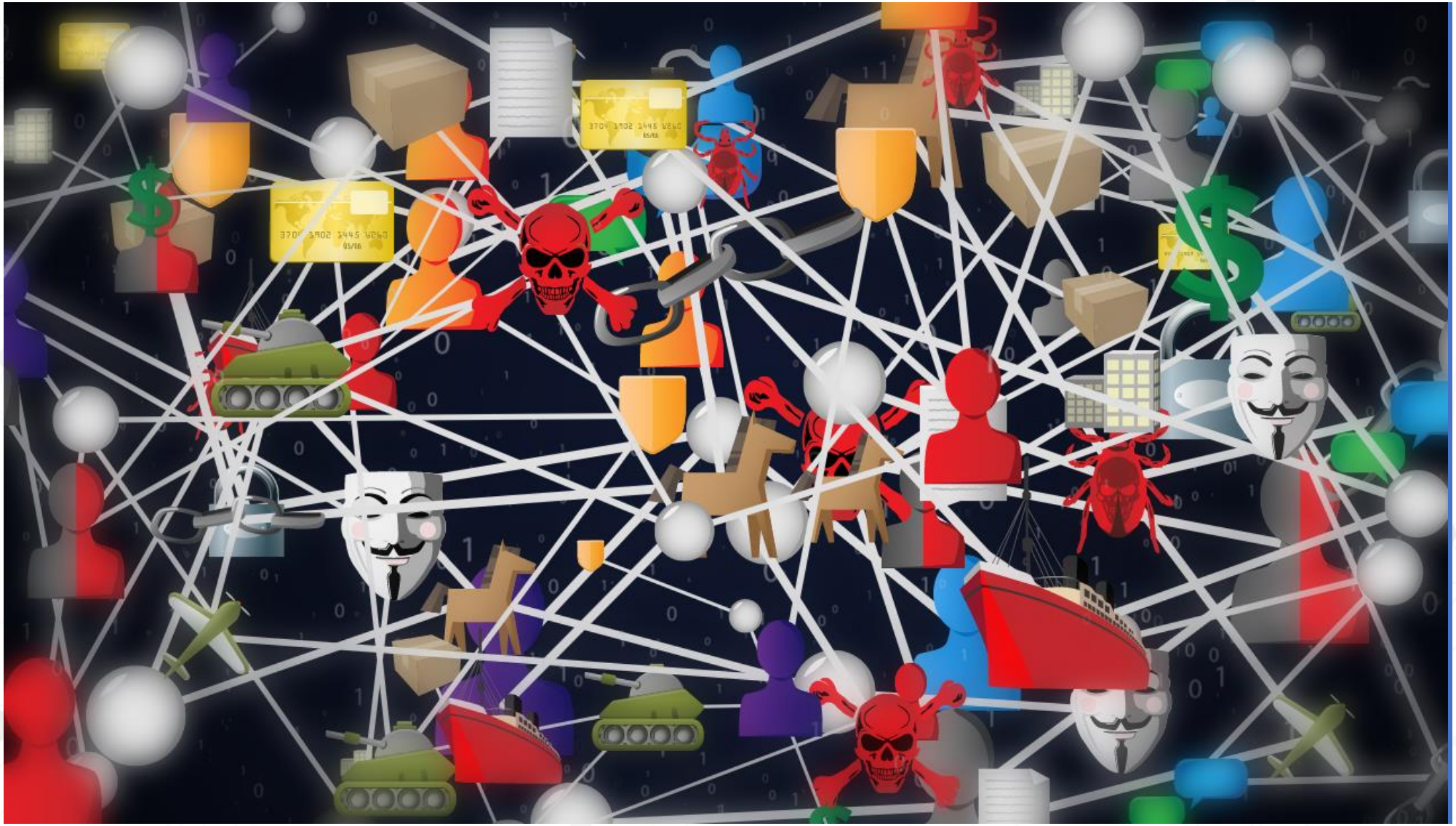
2. Cyberspace is a distinct “initiative persistent” strategic environment that is ripe with opportunity to exploit inherent vulnerability;

3. It means that all the efficiencies you leverage through digital platforms actually also support the opportunity to disrupt those efficiencies.

4. While Government protection will improve, defense of your operations lies with you.

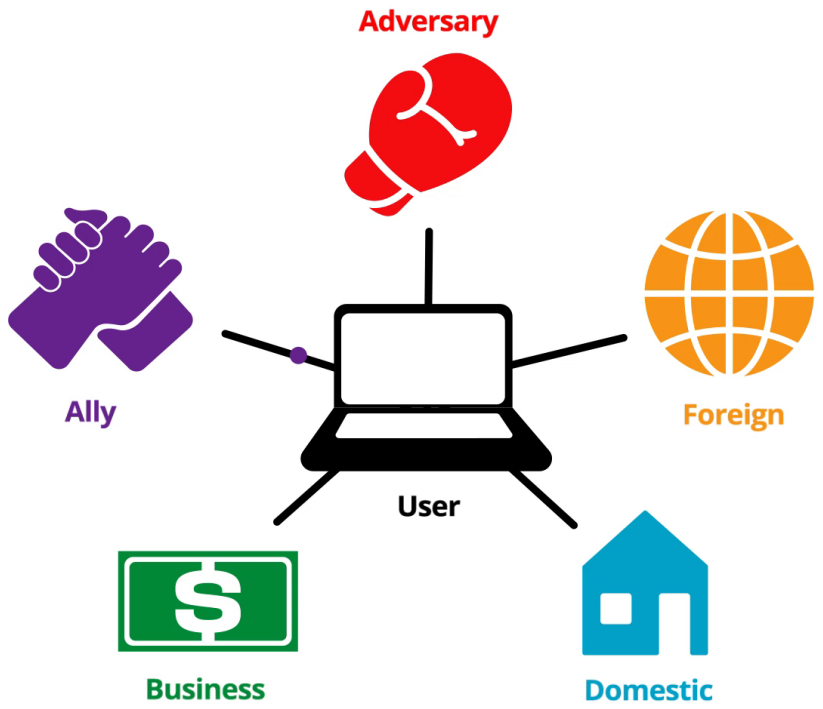
University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

# An Organizing Principle 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 in this space, segmentation is not the answer.

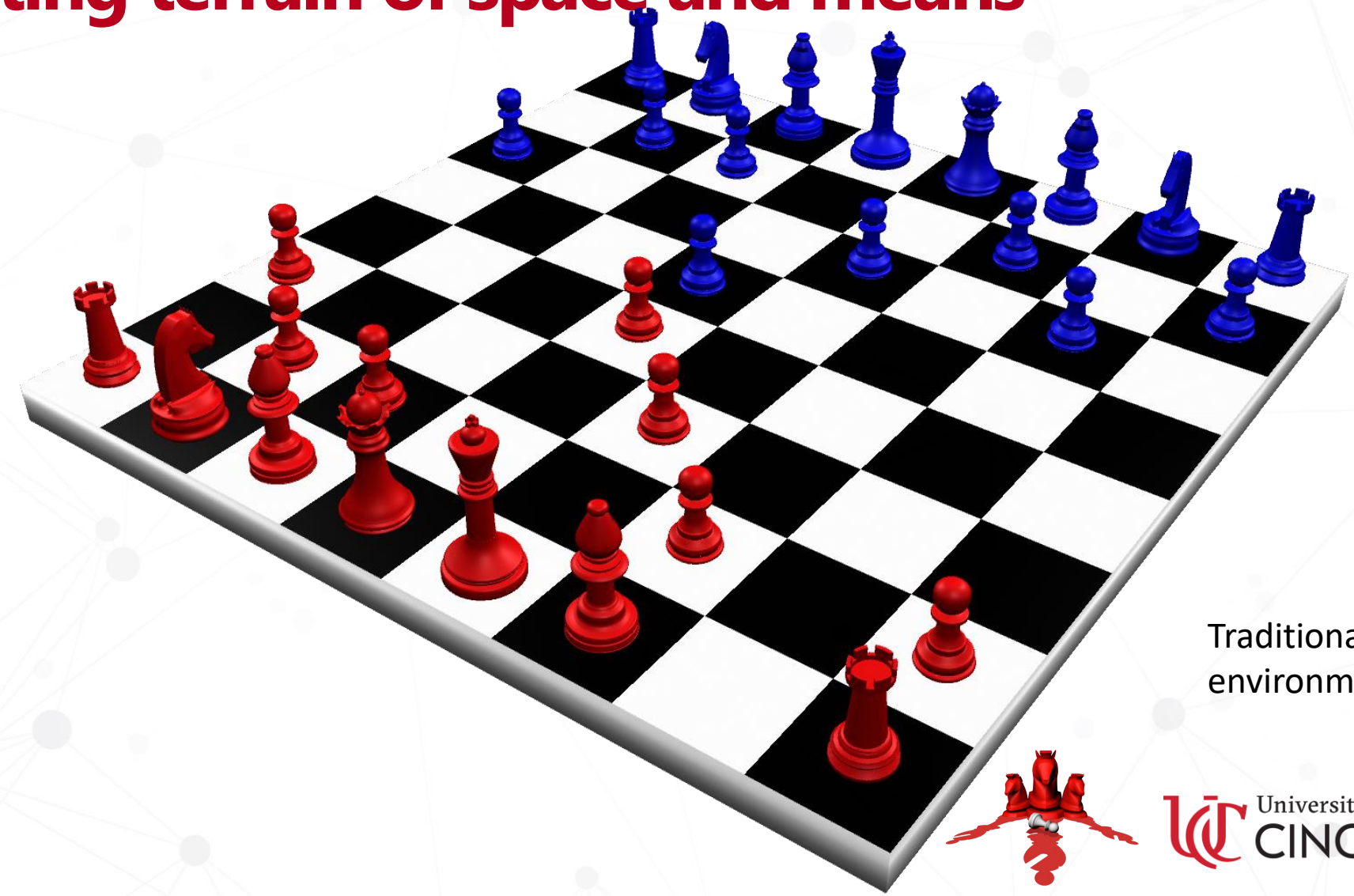


# Interconnectedness in the Rail environment

- Communication systems for rail maintenance, rail performance, and control;
- Communication systems for passengers or employees' data surveillance;
- Embedded cyber-physical systems for maintenance, performance and control; (the update v. replacement cycle issue)
- Company administrative operations and finances.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

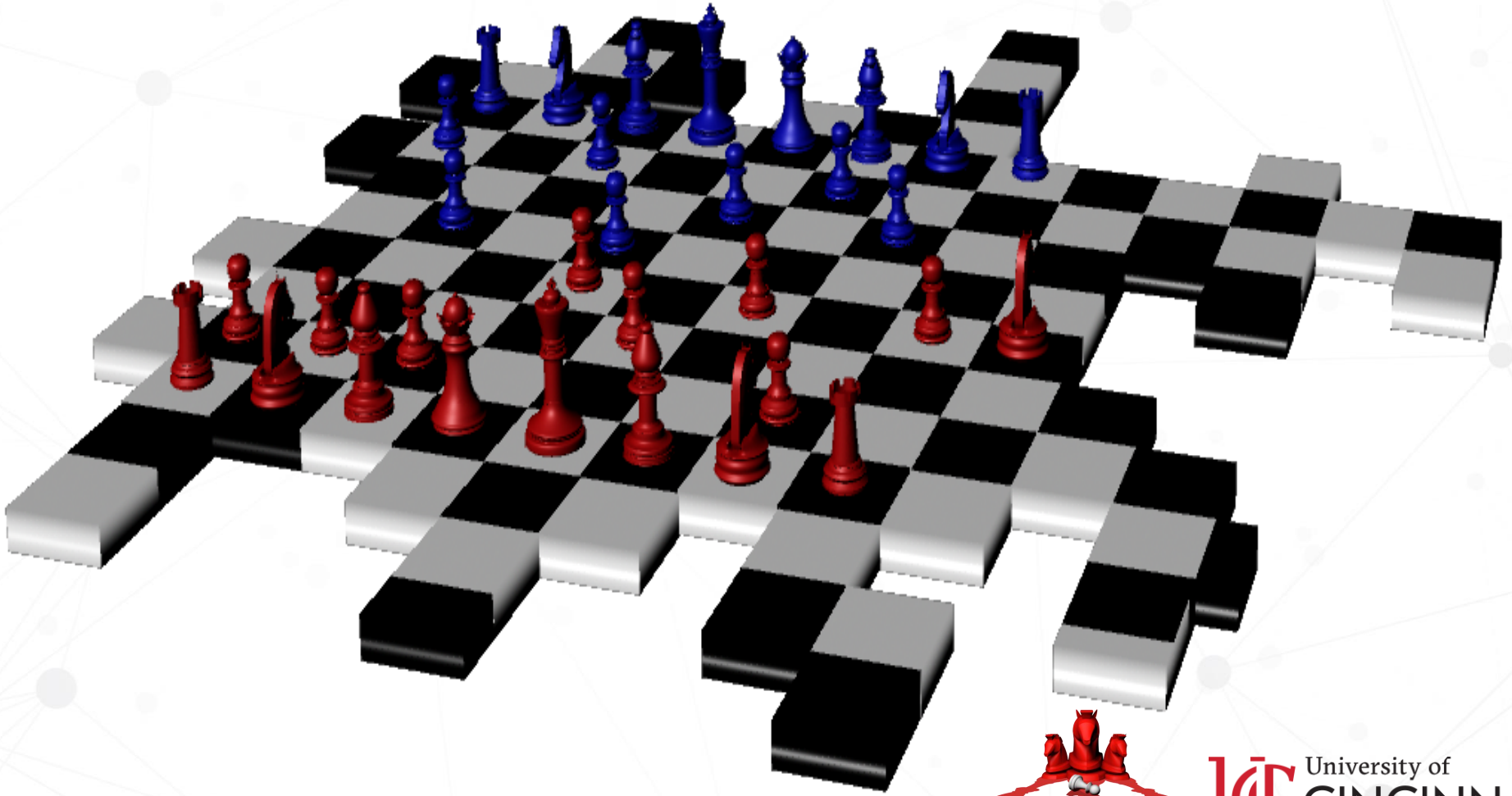
# Differently motivated players on a continuously iterating terrain of space and means



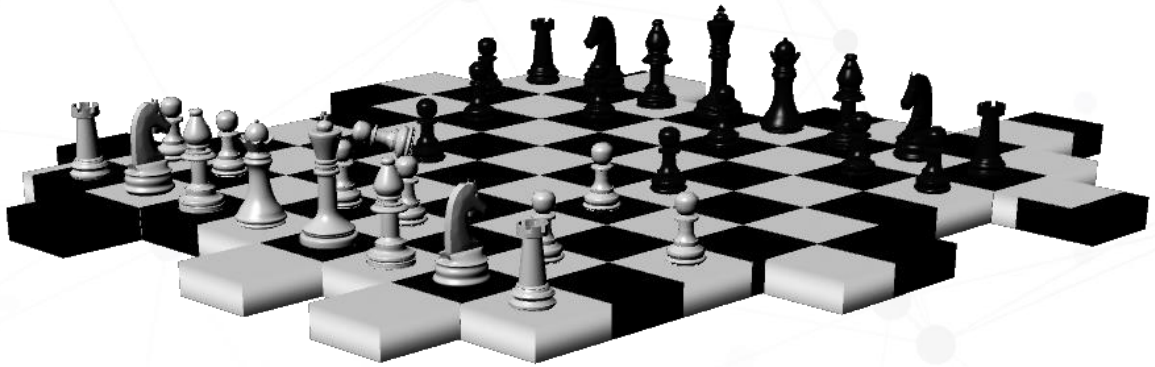
Traditional visual of a strategic environment.

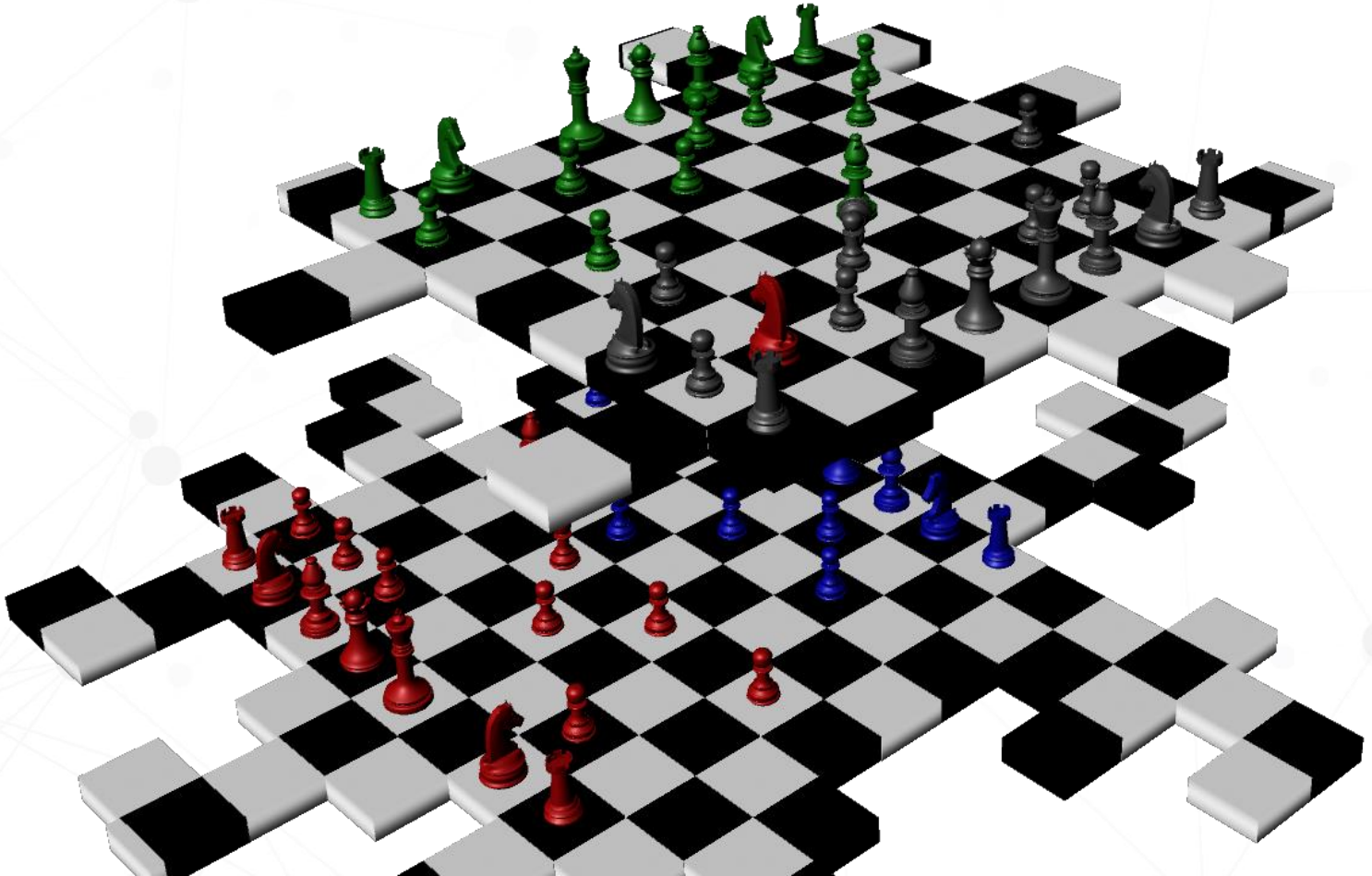
University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

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



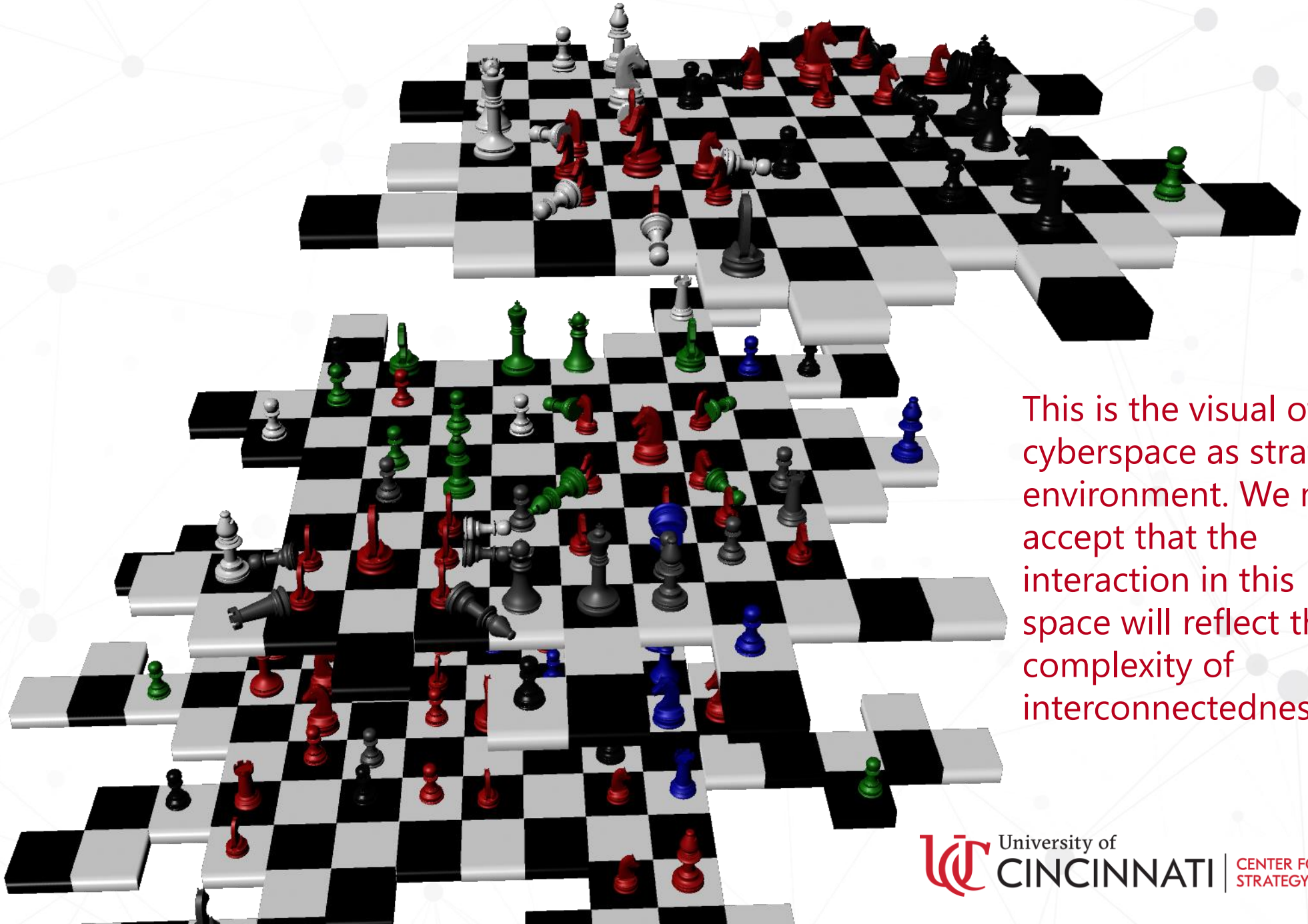
University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY





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. (Strava)

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY



This is the visual of cyberspace as strategic environment. We must accept that the interaction in this space will reflect the complexity of interconnectedness.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

# An Initiative-Persistent Strategic Environment

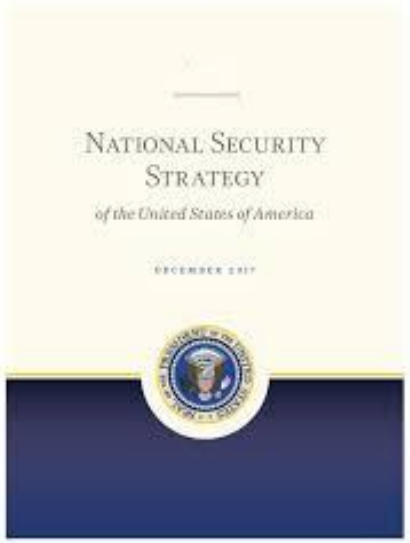
*Cyberspace is an interconnected domain of constant contact and continuously constructing terrain of space and means that creates a continuous willingness and capacity to seek the initiative.*

→ *initiative persistent environment*

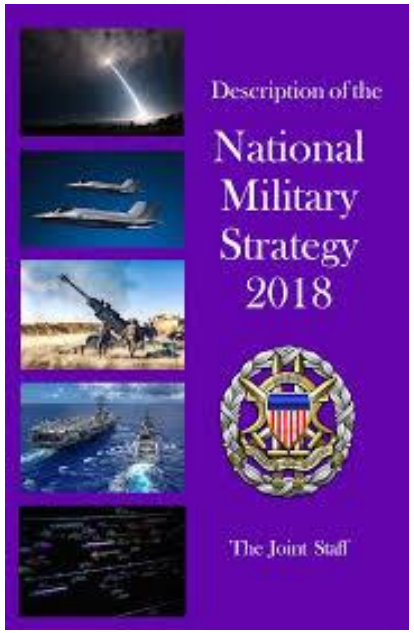
Rethink security as denying, disrupting, seizing and retaining the **cyber initiative** over who is changing the conditions of security.

This is an operational space in which security will be found through cumulative action.

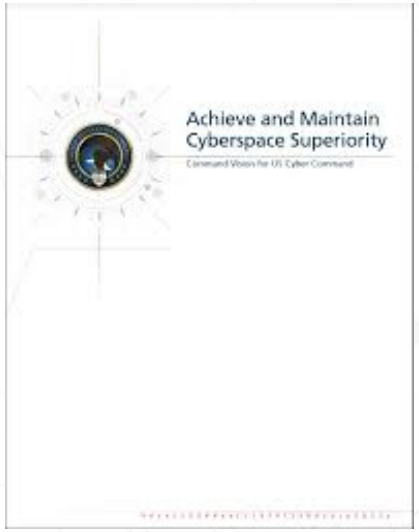
# 2018 DOD Strategy Pivot

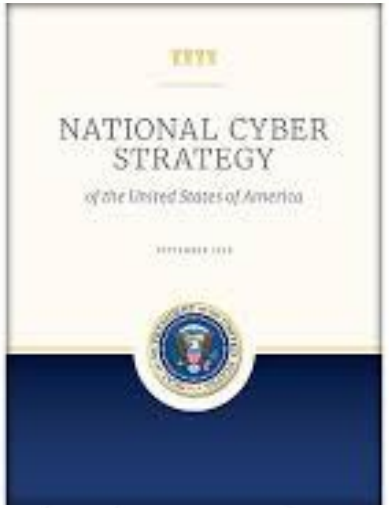












National Security Presidential Memorandum (NSPM) 13
United States Cyber Operations Policy

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

# Shifts in Strategy (2018-2019)

- The *central challenge* to U.S. national interests is the re-emergence of a long-term, strategic competition with revisionist and rogue regimes and actors that have become skilled at operating below the threshold of armed conflict (2017 National Security Strategy of the United States of America,)

- "Global Operating Model - Foundational capabilities include … cyber; It comprises four layers: contact, blunt, surge, and homeland. These are, respectively, designed to help us compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland." (2018 National Defense Strategy)

- "Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure. We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long term strategic risk to the Nation as well as to our allies and partners. (2018 DoD Cyber Strategy)

- "Adversaries are *continuously* operating against the United States below the threshold of armed conflict– demonstrating resolve, technical capability, and *persistence* to undertake strategic cyberspace *campaigns* to gain advantage over the United States." (2018 Command Vision for U.S. Cyber Command: Achieve and Maintain Cyberspace Superiority)

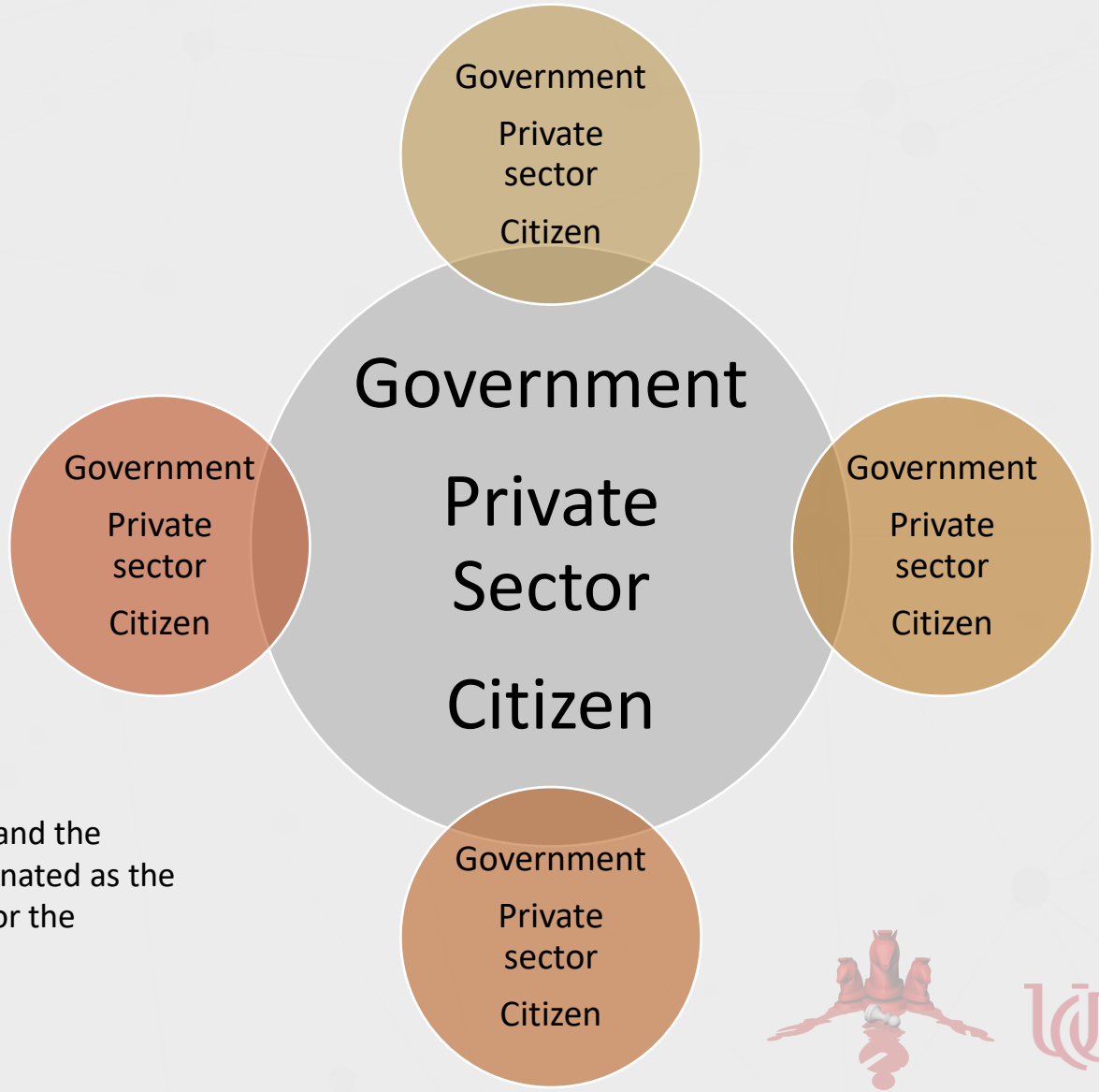
University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

# Doctrine of Persistent Engagement

- US Persistent engagement is "a strategy 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)

- "…persistent engagement, which includes partnering with other USG elements to build resilience into US networks and systems, defending against malicious cyberspace activities as far forward as possible, and contesting adversary attempts to disrupt our nation's key government and military functions." (Gen P. Nakasone, Senate Armed Service Feb 14, 2019)

# Whole of Nation Plus (WON+)




The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector.

# What does Cyber Persistence mean for your Company?

- Globally→Grand strategic competition between 2 models: information dissemination versus information control
  - Chinese advanced rail infrastructure and communication technologies as part of this competition. Questions of collection and control capability versus lower price point. Your Intellectual Property and Business proposition will be caught up in this; We will see increased regulation of software and hardware.

- Domestically→ USG will seek improved alignment through a mix of incentives and disincentives, but defense will remain primarily your responsibility. TSA Security Directive (unfortunate confusion).

- Interconnectedness→ means you will also be increasingly surveilled by individuals, criminals, and competitors

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

# Beyond Resiliency

- **Cyber resiliency** is necessary but not sufficient to handle cyber threats; Recovery has to be part of your planning but reducing the need to recover must be an additional focus.
- Security flows from **anticipating** the Exploitation of Digital Vulnerability, not from responding to it. You need to seize and sustain the cyber initiative in your operations.
- Reducing your vulnerability landscape includes the **training** of your people on good cyber hygiene (counter social engineering attacks; be suspicious)
- **Work as an association** to share best practices; information about incidents and coordinate with government.

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY