CYBERSECURITY POLICY AND POLITICS

CHAPTER THREE: A REALIST VIEW OF CYBERSPACE

AT THE END OF THIS CHAPTER, STUDENTS WILL BE ABLE TO:

- Describe significant concepts associated with Realism
- Apply the realist lens to describing issues of cybersecurity and cyber power
- Define cyber capabilities and their relation to both hard and soft power

THE FOUNDATIONS OF THE INTERSTATE SYSTEM: A QUICK REVIEW

State

- a defined territory held together by **institutions of governance**
- including some form of **executive** or ruler
- and **a system of courts and other institutions.**

Sovereignty

- each state has the **exclusive authority** to determine what happens within the **territorial borders** of their state, **free from outside interference** by other states or actors.
- Other states are prohibited from interfering and from usurping that state's inherently governmental powers.

SOVEREIGNTY: A QUICK HISTORY

The Peace of Westphalia

- ended the Thirty Years' War in 1648
- established the principle of state sovereignty, a crucial building block of our international system today.
- Signatories agreed to respect one another's borders and to allow each state and its rules to determine what laws and rules applied within its territory.

Customary international law

- legal basis for the resolution of many disputes among states in the international system
- evolved over hundreds of years.

REALISM: A SHORT REVIEW

State of nature

- Human beings are not inherently peaceful, and that without structures of authority (like government) life would be "solitary, poor, nasty, brutish and short."
- People needed a sovereign to keep order so that people would not fight and kill each other over resources.

international system

- self-help system in which each states' greatest obligation is to protect and defend its territory so that their state would continue to survive
- conflict is inevitable since state's interests are configured by the international system itself.
- State preferences (for survival, through conflict if necessary) will not alter over time, nor will they learn to cooperate or figure out how to build structures of peace.

SECURITY DILEMMA

- States will likely interpret all activities along their borders by their neighbors as offensive in nature,
- Escalation of conflict along **with arms races** are a feature of the system

CYBER REALISM

- Cyberspace is an electronic extension of physical, real-world territory.
- US military could acquire 'command of the commons' of cyberspace.

- States are compelled (by the international system) to compete for control of cyberspace
- Traditional rivalries (such as that between the US and China or the US and Russia) will be reproduced in cyberspace.
- Questifor cybersecurity is 'zero-sum'. One side acquires it at the other's expense.

DEFENSE OF PHYSICAL INFRASTRUCTURE CONNECTS REAL WORLD AND CYBER WORLD

- Land and undersea cables that produce connections amongst people, organizations, and states
- Communication satellites which orbit the earth, passing through and above the physical space of specific states
- Server farms, routers and other essential hardware and
- Physical facilities belonging to groups which administer cyberspace, such as the national Computer Emergency Response Teams

REALISTS

- reject the idea that there is an information commons, or that the internet is predominantly a good which states should share and administer together.
- Instead, states should construe their role as that of guarding 'their cyberspace' and 'their cyber infrastructure

WHAT IS CYBER POWER?

- Capital strength: a state's physical cyber resources.
- Cyber workforce technical skills
- Intelligence
- Strategy

OTHER WAYS OF CONCEPTUALIZING, MEASURING CYBER POWER

- DIME model: diplomatic power, informational power, military power, and economic power.

- Resilience: 'the ability of a system to resist, absorb, recover from or successfully adapt to a change in environment or conditions."

LET'S DISCUSS:

- We often assume that democracy is a key component of state power. Democracies are able to implement policies with strong citizen support since democratic citizens regard their government as legitimate and believe that their values are worth fighting for. However, many analysts today argue that democratic states do not have an advantage in terms of creating cyber capabilities.

- What do you think?
- Is democracy a weakness or a strength for states in the cyber arena?

WHAT STATES ARE MOST CYBER POWERFUL?

- Originally, US was HEGEMON in cyberspace.
- Today, "seven sisters" of cyber conflict – United States, Russia, China, Britain, Iran, Israel, and North Korea.

POWER GAP

- Refers to the differences between states which are Major Cyber Powers and those which are not.
- This gap is narrowing quickly, and just as significantly, the Power Gap between states and other types of actors (like terrorist organizations and other types of nonstate actors) is narrowing.

ALLIANCES IN CYBERSPACE

- **A formal agreement between two or more nations to collaborate on national security issues."**
- **There must be a formal treaty,**
- **directly concerned with national security issues,**
- **between partners who are nation-states.**

- NATO
- Shanghai Cooperation Initiative
- ALLIANCES vs. Structures for Cooperation

CYBER PESSIMISTS VERSUS CYBER OPTIMISTS

- **CYBER OPTIMISTS**:
- Cyber power is of LIMITED UTILITY
- cyber weapons will serve mainly as a new type of deterrent;
- states will be unlikely to unleash significant cyber attacks,

- ***CYBER PESSIMISTS***:
- *advent of cyber weapons and cyber power can destabilize the international order and make conflict more likely.*

LET'S DISCUSS

ARE YOU A CYBER OPTIMIST OR A CYBER PESSIMIST/

WHY?