



CYBER POLITICS AND POLICIES

CHAPTER SIX: GOVERNANCE

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

Define governance and relate it to ideas of power, sovereignty, and rule-making

Name major agreements and events in the evolution of multistakeholder governance

Describe the players who participate in multistakeholder governance in the internet area, and how this differs from other types of international governance

CURRENTLY, LACK OF CONSENSUS REGARDING INTERNET GOVERNANCE

- 1. Should states be the primary organizing unit for cyberspace, as they are in the global order?**
- 2. Should the internet be viewed as territory? Should it be subdivided along state lines or viewed as a global commons?**
- 3. Are there norms and values which states should be compelled to observe in cyberspace?**

- 4. Where should norms regarding internet governance come from? The internet itself, or a consensus arrived at by key players?**

KEY QUESTION

If structures of governance and organization for cyberspace have not yet emerged organically, can they (and should they) be created and imposed from the top down?

Can the major players in cyberspace – from states to international organizations to corporations – agree on what sorts of regulatory frameworks should exist in cyberspace?

HOW DO STATES FORM STRUCTURES OF GOVERNANCE?

VIEW ONE

States get together to form international organizations like the UN when a consensus **ALREADY exists. Institution is thus a reflection of an existing consensus.**

VIEW TWO

Strong states often impose norms and structures on developing countries. Norms are presented as universal but are really Western.

GLOBAL GOVERNANCE: OPTION ONE: OPEN INFORMATION VIEWPOINT:

- **Major actors would not be states**
- **Internet would be regulated by loose confederations of volunteers, many with technical expertise,**
- **Non-state actors like the Internet would keep the internet running on a technical level.**

- **Norms: transparency, openness, and freedom of information.**
- **Cyberspace should not be carved up into territorial domains**
- **Technology specialists, corporations, nongovernmental organizations, and states – could cooperate to create a secure cyberspace**

OPEN INFORMATION VIEW

- **Evolution** of multistakeholder global governance is a logical outgrowth of the internet's unique history and organization.
- An inevitable, organic, natural process – or an evolution of the environment
- We cannot **STEER** the evolution of internet governance through actions by leaders.

GLOBAL GOVERNANCE: OPTION TWO: CYBER SOVEREIGNTY

- The United States Department of Defense played a key role in creating the cyber sovereignty paradigm.
- States can form cyber commands.
- States can file petitions with international bodies (i.e. UN) if their “cyber sovereignty” has been violated.

REALIST PERSPECTIVE

- States can claim TERRITORY in cyberspace,
- States are the final authority regarding actions and activities occurring in “their” cyberspace
- Cyberspace is not international, but can be broken into Russian cyberspace, American cyberspace and Chinese cyberspace.

CYBERSOVEREIGNTY: STATES DETERMINE WHAT HAPPENS IN THEIR 'TERRITORY'

- **Internet Kill Switch**
- **States act to DEFEND “their” cyberspace and their critical infrastructure (i.e. Active cyber defense)**
- **2015: China Cybersecurity Law – comprehensive control of its domestic cyberspace**

CYBERSOVEREIGNTY IN MILITARY DOCTRINE

- The US Department of Defense defines the cyber domain as:
- A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

- **In 2016, the North Atlantic Treaty Organization (NATO) recognized cyberspace as a military domain,**
- **Tallinn Manual puts forth the understanding that international law applies to cyberspace.**

CHINA'S OWN INTERNET: FULL CYBER SOVEREIGNTY

- No right to privacy, anonymity online.
- Digital identification system: state can track all of a citizens' online activity



- **State OWNS** its citizens' data and communications.
- States have the right to store data within the geographic confines of their state or to access the data of others stored within their country

ARE THERE GLOBAL CYBERNORMS? A



United States

- ‘Universal’ values like the right to assemble and the right to freedom of speech exist in cyberspace, regardless of who claims to own that cyberspace.
- States have **limited sovereignty** in relation to what takes place in ‘their cyberspace.’

China and Russia

State should protect its citizens from immoral and corrupt foreign influences, even if that means imposing what outside observers might label as surveillance or censorship.

Internet users are not ‘global citizens.’

People have IP addresses which are attached to a physical location, as well as an e-mail address which may contain a geographic prefix.

REALISM AND CYBER WESTPHALIA

- **Full state sovereignty advocates view any attempt to establish global norms as REALPOLITIK being practiced by a particular state for its OWN interests/aims.**

- **Cyber sovereignty** is a critical component of a state's cyber power and its overall power.
- A state needs to control its own “cyberterritory” to be a cyber power.
- A nation which depends on another power to defend its critical infrastructure from attacks, is considered to be a weak cyber power.
- A state which cedes sovereign authority to an international organization to create cybersecurity as a collective good is displaying weakness.

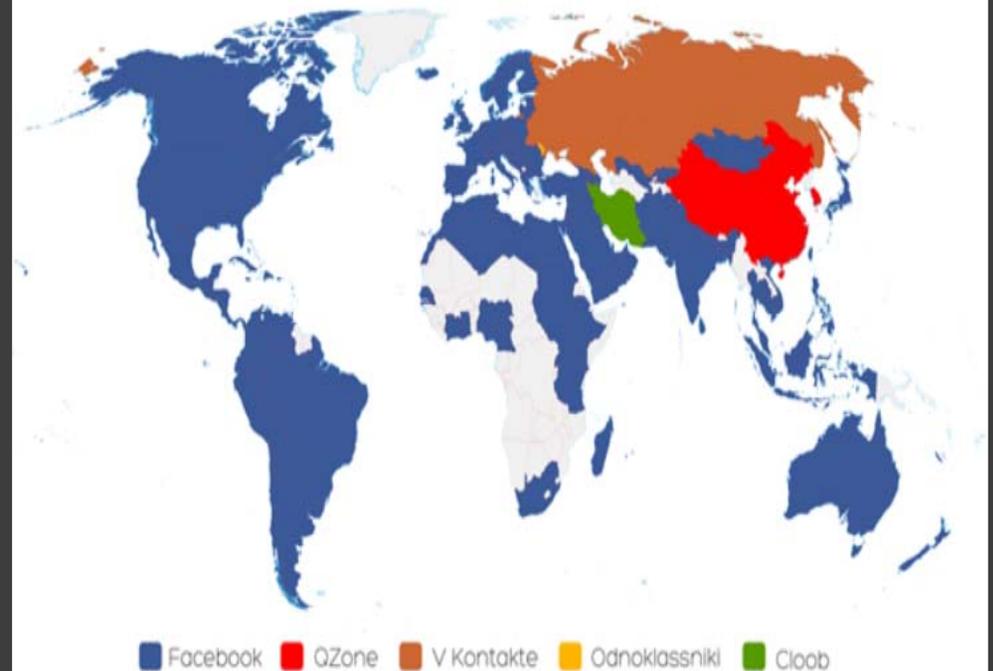
DANGERS OF FULL CYBER SOVEREIGNTY: THE “SPLINTERNET”

Not one international internet,
Instead, a system in which there
are multiple different internets.

A Russian internet which reflects
Russian values and interests, an
American internet and a Chinese
internet, for example

WORLD MAP OF SOCIAL NETWORKS

December 2012



WHAT IS GLOBAL GOVERNANCE?

4 facets

- **Internationalization of policymaking**
 - **Diffusion of authority beyond the state,**
 - **The development of procedural norms on a level beyond the state, Distribution of governing resources among an increasing range of actors**
- **governance as a form of deliberate steering, aimed at rule-making.**
 - **Order is created, rather than merely evolving spontaneously or from the bottom up.**
 - **intentional interventions directed towards solving public policy problems and enhancing the common good.**

OPTION 3: WHAT IS MULTISTAKEHOLDER GOVERNANCE?

- administering and deconflicting international issues in cyberspace often involves a process which includes the participation of a **broad coalition of actors** – from states to civil society organizations, to education organizations, to business to technical specialists



MULTISTAKEHOLDER GOVERNANCE: A BRIEF HISTORY

- 2003: United Nations-backed World Summit on the Information Society (WSIS)
 - WSIS formulated the **Geneva Declaration of Principles**.
 - “International management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, and civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the internet, taking into account multilingualism.”
- 2012: Dubai Summit of the WSIS. Many states signed onto an agreement which would give many internet governance functions over to the supervision of the United Nations. The United States, however, opposed this measure and passed a Congressional statement voicing their opposition to either national sovereignty or international organization vision of internet governance.

FOR FURTHER DISCUSSION

- What Constitutes a Violation of sovereignty in Cyberspace? What are the Controversies regarding these principles?