CYBER POLITICS AND POLICIES

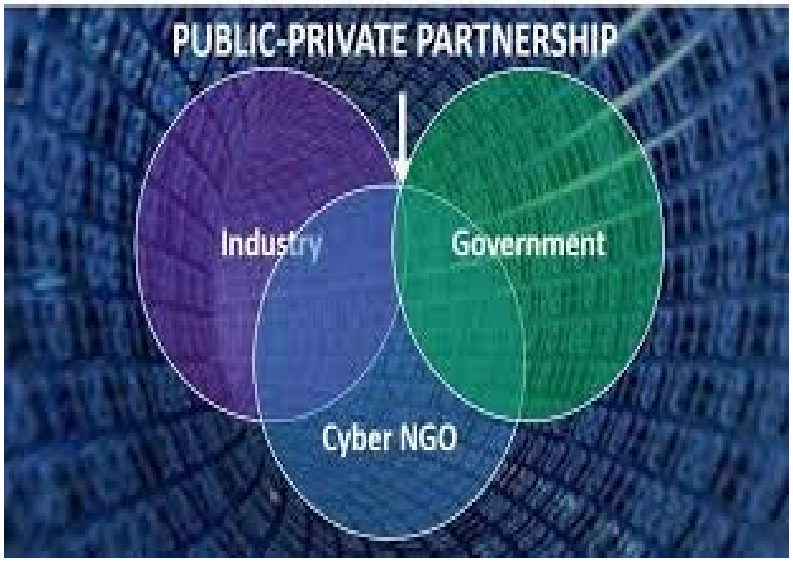
CHAPTER 9: STATES AND PRIVATE ACTORS IN THE PROVISION OF CYBERSECURITY

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

- List at least three ethical, political, economic and social issues associated with the provision of services by Public Private Partnerships
- 1.Compare and contrast the ways in which technological innovation is carried out in an authoritarian vs. a democratic regime
- 1.Define military industrial complex and cyber industrial complex and describe the political, legal and ethical issues raised by the existence of both

WHAT IS A PUBLIC-PRIVATE PARTNERSHIP?

- An arrangement whereby certain aspects of governmental activities have been privatized.
- These functions are carried out by a private, for-profit corporation, through an agreement made with the state.
- The PPP is thus a hybrid arrangement, existing halfway between a totally free market and a state-run economy

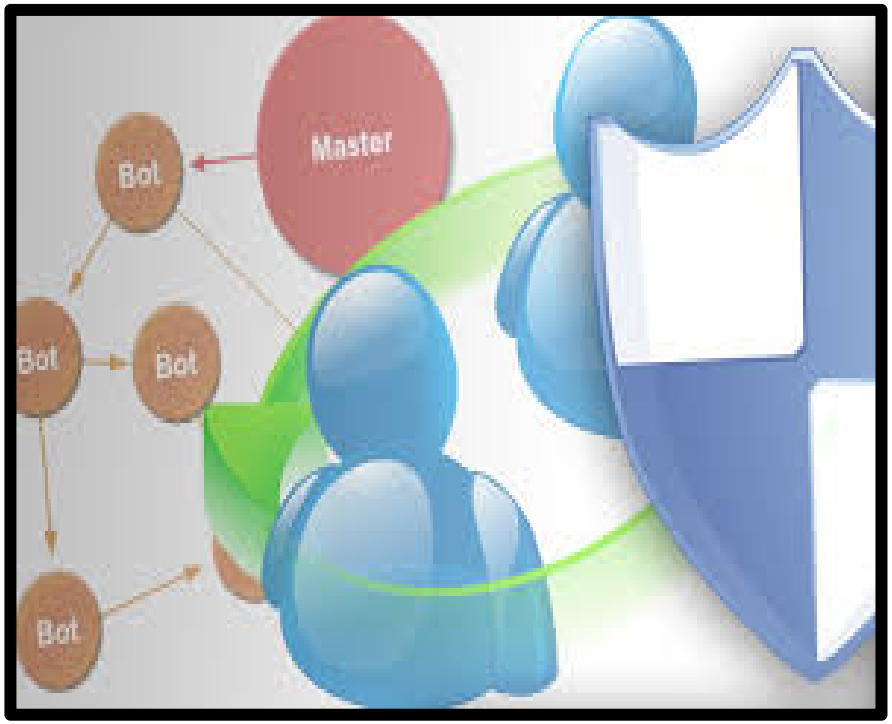


WHY CAN'T STATES PROVIDE CYBERSECURITY THEMSELVES?

- in an ideal world, each state might like to be fully self-sufficient and able to provide its own cybersecurity through government agencies, including its own cybercommand.
- Realist's preferred scenario
- 'sovereignty gap' : states do not have the ability to singlehandedly guarantee and provide cybersecurity within their regions, even if they wished to do so. Rather, they are dependent on technology actors to work with them to provide this public good.

FOUR TYPES OF COOPERATION

- **'Botnet takedowns' – disrupting networks of infected computers used by transnational crime groups.**
- **Identify and disrupt zero-day exploits, through sharing patches for software vulnerabilities.**
- **Attribution activities, working with national governments to identify the perpetrators of online attacks.**
- **Working to defend private-owned systems and networks from sophisticated nation-state sponsored attackers.**

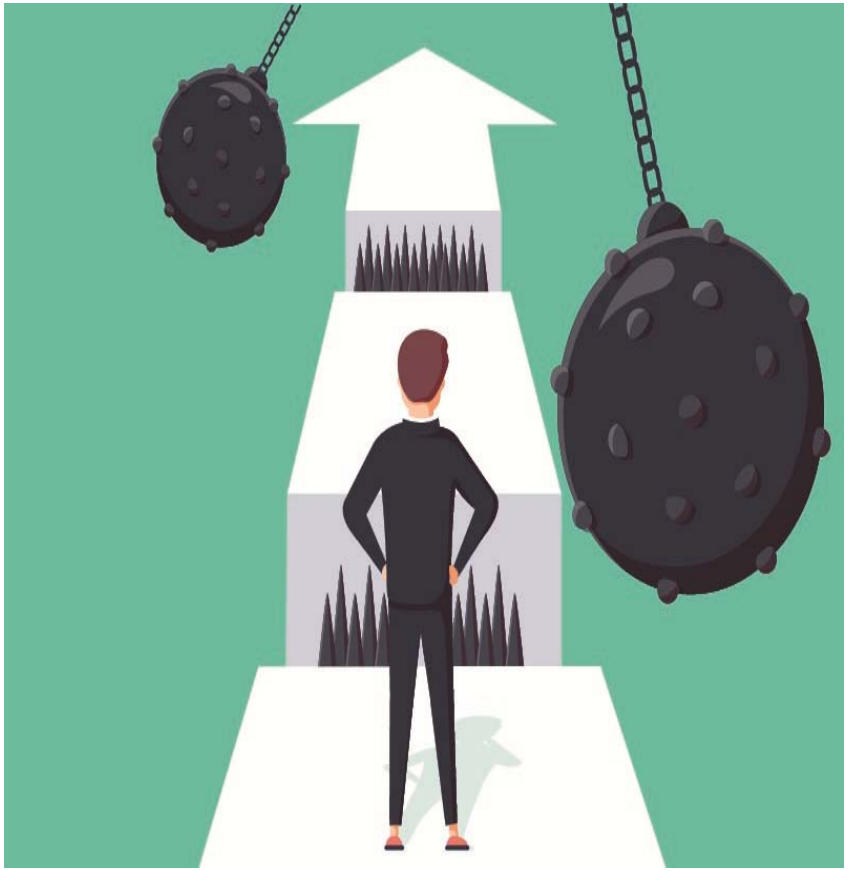


PPP'S AND CYBERWAR: THE WHOLE OF NATION APPROACH

- "integrated capability model of cyber power'
- cyber powerful nation should be able to carry out actions on a host of different activities – from responding to natural disasters, to protecting critical infrastructure to responding to cyber-attacks.
- nation needs to be able to work with a variety of international alliances and partnerships – like NATO and the UN as well as with groups like ICANN.
- needs to be able to work with 'non-state cyber elements' to include private actors including those associated with critical infrastructure

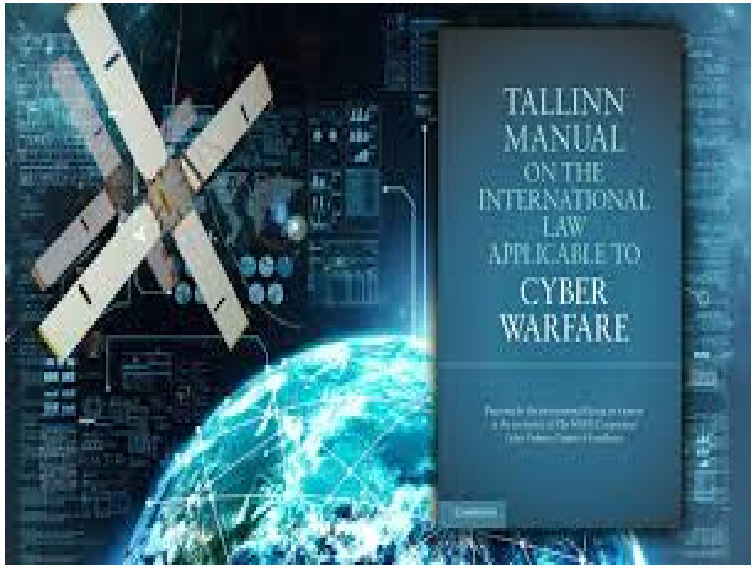
OBSTACLES TO PRIVATE-PUBLIC COOPERATION

- Private industries may not have the same values and goals as government agencies.
- Private corporations may be less committed to safeguarding the privacy rights of citizens.
- Government actions which result in sharing classified information about vulnerabilities with private actors create new threats.
- Problems with trust between commercial and government actors in the cybersecurity sector.



CRITIQUES OF PPP APPROACH

- States have already begun ceding their leading role in the shaping of cyberspace to global technology actors. In doing so, they have created a vacuum or lack of authority which other actors have been forced to step in to fill. (I.E. NATO stepping in to author the Tallinn Manual)
- States might wish to 'hide behind' the PPP rather than taking full responsibility for their actions in cyberspace.
- Efforts by actors like Microsoft, which has put forth its own initiatives regarding what norms should apply to cyberspace in areas like security and freedom of speech



FUNCTIONAL CRITIQUES

- PPP's erode the boundary between what the state does and what corporations do.
- Corporations are taking on political roles which they may not wish to have, and which their customers may not be aware that they have.
- PPP arrangements do not always clearly specify how risks will be shared between both parties,
- Difficult to determine under what circumstances a non-state actor is liable for any negative consequences which result from the arrangement

IDEOLOGICAL CRITIQUES

- **Cyber industrial complex**
- In the aftermath of the 911 terrorist attacks, many people began to ask questions regarding the ways in which private corporations had been aware of NSA surveillance.
- In some instances, corporations had even seemingly been supportive of these activities, and had shared citizen information with the NSA.

THE HONEYMOON'S OVER

- Honeymoon phase through the 1990s and up until 2013 – in which Washington and Silicon Valley shared a vision of the internet as a borderless 'territory' characterized by ideas like freedom and open access.
- Today, however, Silicon Valley has interests which have diverged from the stated policy positions of the US.

- Some international companies have attempted to create what they call a **Digital Geneva Convention,** which would be focused on the needs of civilian or private internet users, rather than the needs of states.
- Many companies act as 'first responders' when citizens have their data stolen.
- Many of the victims are private citizens in cyberwar, unlike conventional war.

CLOUD COMPUTING

- Refers to models of computing in which calculations and services are not carried out on an individual user's computer, or where data and information is not stored on an individual's computer.
- "A networking solution in which everything from computing power to computing infrastructure, applications, business processes to personal collaboration can be delivered to you as a service wherever and whenever you need it."

THE WAR CLOUD

- 10 billion dollar project
- Proposal began circulating in 2017
- Would allow Pentagon to use Artificial Intelligence functions to automate, speed up and enhance warfighting capabilities
- Ethical issues related to whether Amazon should support development of this technology

THE CLOUD ACT, 2018

- Clarifying Lawful Use of Overseas Data
- European Commission: legislation regarding so-called e-Evidence to the European Parliament.
- Supporters: These initiatives are necessary in order to modernize existing legal understandings regarding how data can be used and shared,
- Detractors: Both the CLOUD Act and the proposed EU legislation represent a threat to user privacy rights.
- Electronic Frontier Foundation: The CLOUD Act provides the United States government and the foreign governments with which it makes bilateral Executive Agreements with unprecedented access to user data across a variety of platforms

LEGAL CHALLENGES IN CLOUD COMPUTING

- Unique challenge to policymakers today largely because of how quickly the technology has developed
- The development of mechanisms to govern, regulate and harmonize state approaches to these issues have lagged behind the technological developments themselves.

FOR FURTHER DISCUSSION

- In her essay on public-private cybersecurity, analyst Kristen Eichensehr argues that when it comes to working with private sector corporations as actors in the international system, "the state may sometimes act more like a market PARTICIPANT than like a regulator – as government functions are contracted out to private parties."
- What do you see as the dangers associated with state reliance upon private sector actors, either as participants working together with the state, or even in a leading role vis a vis the state?
- How would a Realist respond to this question? A Liberal Internationalist? A constructivist?