Lecture 1: The securitization and militarization of cyber space

Sarah Backman
PhD Candidate in International Relations,
Stockholm University/Swedish Defence University

Lecture 1: the securitization and militarization of cyberspace

1. The development of cyberspace: governance and culture
2. The securitization of cyberspace
3. The militarization of cyberspace
4. Q&A

Aim: after these lectures, you should be able to
1) reflect around socio-technical vulnerabilities as a basis for dangers in cyberspace/incidents and
2) Reflect critically around developments in the international cyber(security) landscape.

Lecture 2: sociotechnical perspectives on dangers in cyberspace

1. Sociotechnical (non antagonist based) perspectives on dangers in cyberspace
2. A sociotechnical perspective on large-scale cyber incidents affecting critical infrastructure
3. Normal Accidents & High Reliability Organizations /sociotechnical systems perspectives
4. Q&A

1.The development of cyberspace: governance and culture

The development of cyberspace: governance and culture

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

–John Perry Barlow "A Declaration of the Independence of Cyberspace, 1996

- the utopian anarchic vision for the internet shared by many of the internet's founders and pioneers.
- Emphasized consensus and transboundary freedom, rejected authority and hierarchy.

The development of cyberspace: governance and culture

- This culture of the early internet, captured by the memorable phrase "We reject: kings, presidents, and voting. We believe in: rough consensus and running code," coined by David Clark in 1992, still echoes in the governance structures, communities and inventions of the internet today.
- It is prevalent in hacker and coding communities
- reflected in inventions such as cryptocurrency and blockchains
- and in the informal manners of internet governance bodies such as the Internet Engineering Taskforce (IETF) who, to avoid formal votes and authority, famously make decisions by humming.

The development of cyberspace: governance and culture

- From a small experimental research project in the U.S (Advanced Research Projects Agency Network (ARPANET) → an indispensable and integral part of societies globally and a fundamental pillar of the global economy.
- → increasing state control and governance of the internet.
- Although the internet is global and transboundary, it also depends on physical infrastructure that is placed in states and subjected to national law.
- Indeed, the uniqueness of cyber space as a world separated from the “ordinary” physical world (in culture, governance and ideology) has decreased over time as it has become more of an extension of the physical world.

The development of cyberspace: governance and culture

- In this context, internet governance has proved infamously difficult to achieve.
- In 2004, the UN formed a Group of Governmental Experts (GGE), with the aim of strengthening global cyber security, and discussing global cyber norms.
- the group failed to deliver its fifth report, since no consensus could be reached on whether international humanitarian law applies to cyber operations.
- The number of actors involved in the governance of cyberspace, and the variety of institutional and legal approaches and solutions adopted to govern it, have created conceptual confusion (“What is Cyber?”), but also a lack of common understanding regarding responsibility, accountability and transparency in cyber space.

The development of cyberspace: governance and culture

- Cyberspace remains a highly contested arena for policy making, and its current institutional architecture is dominated by a multiplicity of tensions over who is entitled to decide on issues that goes beyond the traditional functions of the state and what practices of governing are most appropriate in this context.

- Cyberspace has a tendency to blur important dichotomies, including internal/external, technical/strategic and civilian/military.

- Cyberspace is global and transboundary, but not stateless.

The development of cyberspace: governance and culture: conclusion

- The challenges of international cybersecurity governance cannot be divorced from ideas about what cyberspace once was, and what it is becoming, from an idealistic point of view.
- Clashes of values, battle of frames.
- Privacy vs “security”, state control and governance vs the founding ideas of the internet influenced by the anarchist movement.
- What are we protecting? What norms are we setting through our actions in cyberspace?
- What will the internet of tomorrow look like? The social construction of cyber space.

Discussion - 10 min

1. Form groups of 4-5

2. Discuss the following question for 10 minutes

Question: How do you think the anarchic culture of the early internet (rejection of authority/hierarchy) creates clashes or challenges with the way the internet is operated today (including increasing governance ambitions from states)?

2. International cybersecurity and the securitization of cyberspace

How has international cybersecurity been studied?

The traditionalists point of view:

- Leaning towards a neo-realist worldview: analysis is oriented around the 4 S's: States, Strategy, Status Quo and Science
- Focused on classical security questions: How does traditional security concepts such as war, power, deterrence and coercion translate to cyber space?
- Practical focus: how do we counter the rising cyber threat (with the state as referent object) from (especially) undemocratic nation states
  - (for example) through deterrence
- How can cyber warfare be conducted in line with International law and Just War principles?
  - (Jus ad Bellum): Just cause, last resort, declared by proper authority, right intention etc.
  - (Jus in Bellum): Discrimination, proportionality, responsibility

The securitization of cyberspace

1. What is it?
2. How does it happen?
3. Why is it not necessarily a good thing? (consequences)

What is securitization?

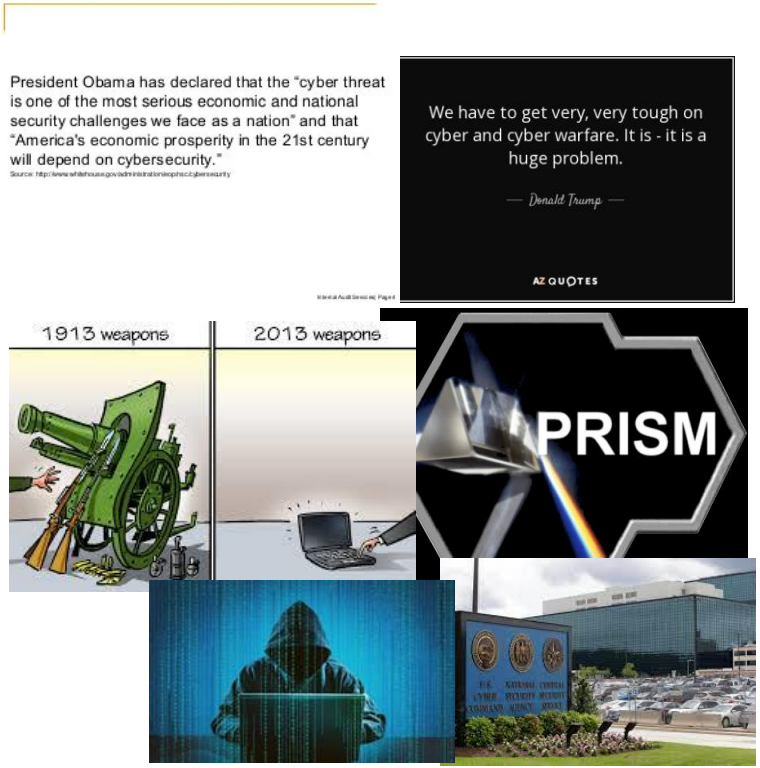
Securitization: how an issue is moved from the realm of “normal politics” to exceptionality – giving way for exceptional measures and politics.

”..an intersubjective practice of meaning making that triggers a particular security-oriented mindset and shapes the perception of both the nature of the problem and actions undertaken to deal with it.” (Stepka 2022).

What is the securitization of cyber space?

- The process of making cybersecurity a **national security priority**, linking it closer to **intelligence and military agencies**, actors and issues. Making space for **exceptional measures** to protect "referent object" (often the state) from what is constructed as an **existential threat** to it.

"..an intersubjective practice of meaning making that triggers a particular security-oriented mindset and shapes the perception of both the nature of the problem and actions undertaken to deal with it." (Stepka 2022).



How has cyberspace been securitized? 1

- Securitization happens through so called speech acts, which fuels a hype and a fear surrounding the issue.
- In speech acts, key leaders/actors argue that there is an existential threat to states stemming from cyber space and that it therefore must become a national security priority.
- If accepted by key audiences, resources and windows of opportunity for exceptional measures are granted, which otherwise would not have been acceptable by the public (for instance surveillance or secret offensive action).

How has cyberspace been securitized? 2

- In these speech acts, analogies and imaginaries referring to previous existential security threats are often made.
  - In the securitizing speech acts surrounding cyber, references are often made to catastrophic military events such as pearl harbor or 9/11.
    - tendency of using military terms and battlefield analogies to describe happenings in cyber space, even the same event in the physical space would not be labelled as such.

      ..for example, the term “cyber-attack” has been used to describe anything from online protests to criminal fraud, spreading of rumors and sabotage
    - tendency to deploy a broader definition to what constitutes warfare in the virtual space than in the physical space

What about the empirical basis for these claims?

- Despite speech acts talking about the pending cyber doom due to cyberattacks, nothing even coming close to the catastrophic scenarios depicted in these narratives have yet occurred.
- Cyber warfare entails largely espionage and very limited operations more like physical sabotage than bombings.
- Cyber terrorism has not been realized.
- Large-scale cyber incidents affecting critical infrastructure (the most feared of scenarios) has so far not been catastrophic, and they have often been the result of collateral damage rather than directed attacks from antagonist actors (more about this next lecture).
    - These events are primarily managed by civilian actors (such as civilian CERTS and private actors) rather than intelligence or military actors.

Why is securitization of cyberspace not necessarily a good thing?

- According to scholars from this perspective, these imaginaries contributes to oversimplified, unrealistic and deflated depictions of dangers in cyberspace.
- It diverts attention from and skews the real situational pictures and the security problems connected to both antagonistic and non-antagonistic problems in cyberspace.
- Bringing the issue of national cybersecurity closer to military and intelligence actors and agencies leads to less transparency and more secrecy surrounding what happens and what actions are taken.
- Fueling fear around and hyping cyber is not necessarily “apolitical” but is an activity often undertaken by actors with an invested interest in the securitization of cyberspace, such as the military-industrial complex, the cybersecurity private sector, etc.

  Cyber is linked to power and resources

Discussion - 10 min

1. Form groups of 4-5
2. Discuss the following question for 10 minutes

Question: What are the consequences of an increasingly securitized cyberspace globally?

The securitization of cyberspace
Q&A
+10 min break

3. The militarization of cyberspace

What is the militarization of cyberspace? 1

- Militarization is the process by which a society prepares and organizes itself for military conflict and violence.
- Preparing for cyber war/warfare
- The development & deployment of cyber force
  - Cyber “soldiers”
  - Defensive+offensive capabilities
  - Defensive+offensive cybercops
  - “Cyber swagger”/Posturing
  - Deterrence

	Technical	Crime-Espionage	Military / Civil defence
Main actors	• Computer experts • Anti-virus industry	• Law enforcement • Intelligence community	• National security experts • Military • Civil defence establishment / Homeland security
Main referent object	• Computers • Computer networks	• Private sector (business networks) • Classified information (government networks)	• Networked armed forces (military networks) • Critical (information) infrastructures
Main Threat	• Malware • Network disruptions • Hackers (all kinds)	• Advanced Persistent Threats • Cyber Criminals • Cyber mercenaries • States (foreign intelligence)	• Catastrophic attacks on critical infrastructures • Cyber terrorists • States (cyber commands)

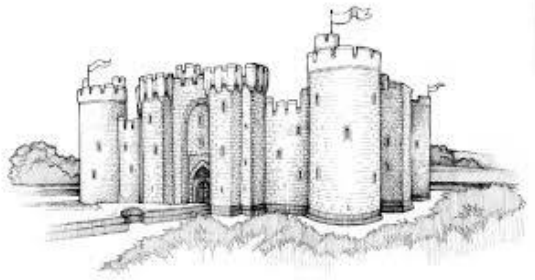
Table: Dunn Cavelty 2012

What is the militarization of cyberspace? 2

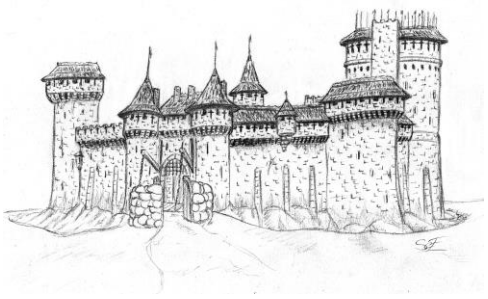
- Cyberspace has been declared a new domain of military operations, and an increasing number of states are developing offensive cyber capabilities (OCC)
  - human, technical and virtual tools to destroy, disrupt and/or exploit the computer networks of an adversary for strategic advantage.
- There are an estimated 60 states with military or intelligence agency-based cyber units, and 29 of those possess declared OCC (as opposed to defensive cyber capabilities).
- A variety of international actors are now developing and using offensive cyber tools for a broad range of strategic purposes, including espionage, subversion, coercion,war-fighting and hybrid warfare campaigns.
- The prospects of cyberwar has become an overwhelming preoccupation in the cyber-security discipline over the past two decades, which has structured debates about cyber security as well as perceptions of the field.

Why might the militarization of cyberspace lead to less rather than more international security?

- Triggered security dilemmas (causing international arms races and stockpiling of vulnerabilities)
    - Increased proliferation of offensive tools and willingness to use them
    - Less trust, leading to less international collaboration and information sharing
    - and more suspicion and fear (which is linked to an increased risk of escalation)
    - When offense is easier than defence, war is more likely.
- This happens in an unstable environment legally and normatively. For example, states have different understandings and thresholds for retaliation in case of serious cyberattacks.



The security dilemma: More security **in** the castles (through better and more ”weapons”, etc.) leads to a less secure environment **between** ”the castles”, in which escalation and war becomes more likely



Critique of a neo-realist perspective on international cybersecurity/ or why we can't easily transfer a cold war analysis to contemporary cyber conflict

- Analytical state-centricism
- The applicability of "rational actor" models in a normatively and legally unstable environment (the ability to foresee responses and reactions of opponent)
- The ability of actors to "control" malware as a precision weapon (on both sides)
- The ability to neatly translate the traditional deterrence concept to cyberspace

Discussion - 10 min

1. Form groups of 4-5
2. Discuss the following question for 10 minutes

Question: What are the consequences of an increasingly militarized cyberspace globally?

Thank you!
Q&A