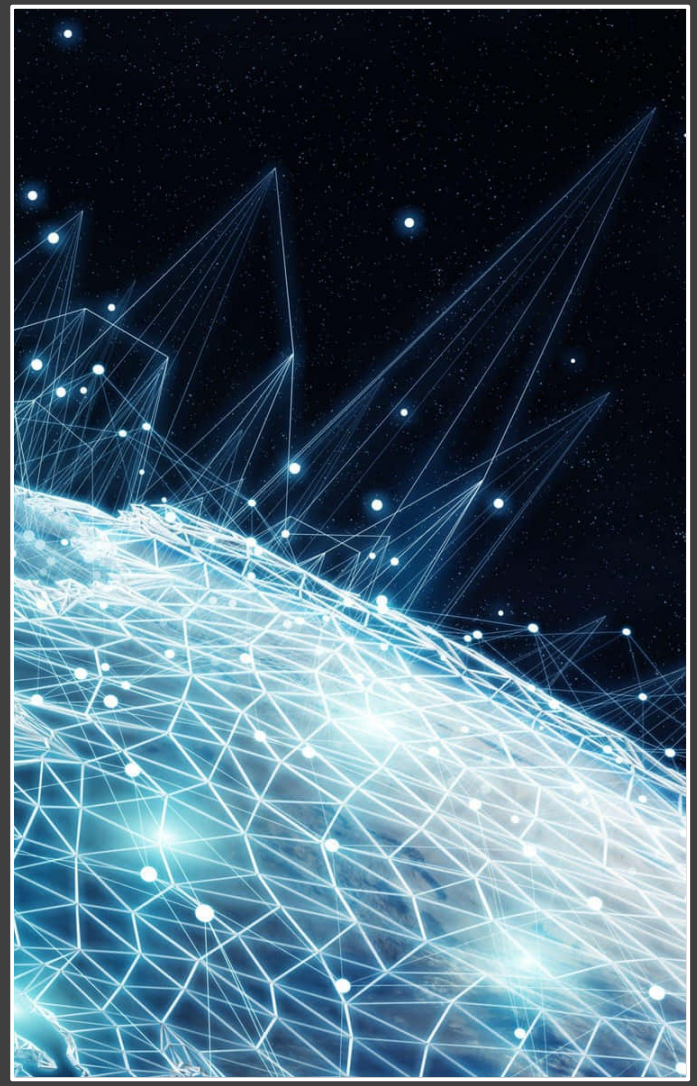
# Connectivity & Security

Technological and economic dependency, cybersecurity and cyberwar

Teresa Hong



# Agenda

Introduction

- Connectivity and security
- Attribution of cyberattacks
- Regulations

Conclusion

# Introduction

**Connectivity**

Increasing dependence on digital technologies and global tech infrastructures.

States use the cyberspace to project their cyber power to exert their influence on others

*Connectivity dilemma*

- Creates economic opportunities but also vulnerabilities.

Lines between cyber and physical security are blurring as our critical infrastructure becomes increasingly digitized and interconnected

**Cybersecurity:** Protecting data, networks, and digital and critical infrastructure becomes essential.

- Aim to prevent cyberattacks, data theft, surveillance, and disruptions to critical systems.

# Cyberattack

**Deliberate attempt to compromise CIA**

Types of cyberattacker and their possible motivation

- Cyber espionage: data collection
- Financial cybercriminals: make money
- Hacktivists: make a political statement

With the rise of AI, more sophisticated and scalable cyberattacks, able to evade detection and easy to use, even by people with little knowledge of the field.

- 80% of cyberattacks found to use AI

# Hypotheses

1. Increasing connectivity increases surface areas for attacks
2. Different states have cyber capabilities, borderless nature and anonymity makes it difficult to attribute cyberattacks to groups
3. There is a lack of consensus on how cyberspace should be regulated,

# 1. Increasing connectivity increases surface areas for attacks

Nodes of potential entry points

Nodes can improve security up to an optimal point

- Decentralization, increases attack costs <--> difficult to manage all the nodes, more pathways for attacks
- Individual nodes maybe vulnerable to targeted attacks
  - Regular patches are important

# 2. Different states have cyber capabilities, borderless nature and anonymity makes it difficult to attribute cyberattacks to groups

Different levels of development

- Different priorities and resources of states

Anonymity

- Ability obfuscation or mislead the investigation
  - Difficult to attribute responsibility

Wrong attribution may result in unintended consequences

# 3. Lack of consensus on how cyberspace should be regulated

Cyberspace is an interdisciplinary domain

- E.g. Change Healthcare, 2026, Stuxnet (2010)

International law, under the International Court of Justice (ICJ) unclear to apply to cyberspace

- Issues of attribution, sovereignty
- Different perspective of cyber governance: Open internet (e.g., US) vs Cyber sovereignty (e.g., China and Russia)

Regional Cooperation

- Association of Southeast Asian Nations (ASEAN): Cyber Security Cooperation Strategy (2021-2025)
- African Common Position on the Application of International Law to Cyberspace (2024)

International Cooperation

- UN Cybercrime Convention (2024) – binding resolution
  - Attribution, due diligence and disagreements on how specific rules should be interpreted, creating legal ambiguity remains key challenges

# Conclusion

- Connectivity has allowed for unprecedented (AI-powered) cyberattacks with ripple effects to other industries or geopolitical implications.
- Due to differing levels of cyber capabilities, borderless nature online and anonymity of cybercriminals, it is difficult to identify cybercriminals with absolute certainty to apply international law.
- Sovereignty and different interpretation of international law hinders how international law should apply effectively

# References


- https://techblog.comsoc.org/2026/01/16/fiber-optic-networks-subsea-cable-systems-as-the-foundation-for-ai-and-cloud-services/?replytocom=25081#respond
- https://www.yahoo.com/news/world/articles/undersea-cable-connecting-egypt-syria-133139856.html
- https://arxiv.org/abs/2510.07192
- https://www.security.org/identity-theft/breach/change-healthcare/