63rd FITCE
INTERNATIONAL CONGRESS

Krakow, Poland 26-28 September 2024

Techno-Economics of IoT and OT security

Morten Falch & Reza Tadayoni

AALBORG UNIVERSITY
COPENHAGEN

Research question:

- What are the economic characteristics of Cybersecurity issues in IoT and OT, and what are the regulatory implications
- Hypothesis:
  1. The importance and economic charateristics of cybersecurity justifies public regulation. NIS2 provides a regulatory response, but regulation is still under development.
  2. Cybersecurity includes a wide range of remedies with different economic characteristics.

Agenda

- Motivation
- Economic research on Cybersecurity
- Definition of Cybersecurity
- Technical aspects of cybersecurity
- The market for Cybersecurity
- Conclusion and tentative implications

Motivation/Background

- World Economic Forum has nominated cybersecurity to be among the top 10 global risks
- Cybersecurity is a hot topic everywhere including Aalborg University
- AAU has established a new engineering education in Cyber Security in Copenhagen
- Mostly focus on technical aspects, but Cyber Security is an interdisciplinary topic
- Want also to look at economic, organisational, and regulatory aspects
- Developing a course in IT security and Regulation
- Just completed a paper on Cybersecurity institutions in EU

Why look at cybersecurity in IoT and OT?

- Still more OT equipment is connected to the Internet.
- Intrusions and their impacts on organizations have worsened (Fortinet, 2024)
- IoT is used for attacks on other IT systems
- Security solutions are designed to be implemented in a typical IT environment. Security solutions tailored to an OT environment are needed (Fortinet, 2024).

- Want to look at the economic aspects.
- Work in progress

Economics of Cybersecurity: Research areas

Limited research available often inspired by information economics (Kianpour, 2021)

Core issues

- Budgetting and economic efficiency
- Cybersecurity as an economic good. What are the characteristics?
- Information asymmetry and moral hazards
- Network effects and externalities
- Economics of Cybercrime

Cyber Security includes many different kinds of products

Papers on the economic characteristics often treat cyber security as one product.

It is necessary to look at the market for cybercrime and preventive measures in more detail.

We want to look at the economics of cybersecurity measures for IoT and OT.

Definition of Cybersecurity

- *"cybersecurity aims at protecting the cyberspace (which includes both information and infrastructures) from any cyber threat or cyber-attack"* (Lezzi, Lazoi, & Corallo, 2018)

Privacy, Information security, and cybersecurity

- Privacy (GDPR)
  - Deals only with personal information
- Information security
  - Deals with protection of information
- Cybersecurity
  - Deals with protection of digital information and digital infrastructures
  - Does not include off-line data and infrastructures

Economic research in Cybersecurity: Results

- Inspired by the research in Information Economics
- Cybersecurity shares economic characteristics with public goods
  - Non rivalrous
  - External effects
- Economic characteristics and Spill-over effects provides arguments for regulation
- Looks at cyberscurity at an aggregate level

	Excludable	Non-Excludable
Rivalrous	**Private Goods** Food, clothes, cars and other consumer goods	**Common Goods** Fish, timber, coal
Non-Rivalrous	**Club Goods** Cinemas, private parks, satellite TV	**Public Goods** air, national defence

Disaggregating Cybersecurity: The CIA Triad

- Confidentiality
- Integrity
- Availability

- Supplementary measure:
  - Non-repudiation
  - Accountability
  - Authenticity
  - Reliability

How to protect: The NIST Framework

- National Institute of Standards and Technology (NIST)
- Created in US, but also used in EU
- Includes five core functions, which must be addressed
  - **Identify** includes identification of the critical processes and resources.
  - **Protect** includes protection of the sensitive data identified above.
  - **Detect** includes monitoring of IT-systems in order to detect any cybersecurity events
  - **Respond** includes guidelines for how to react if a cybersecurity attack is detected
  - **Recover** includes plans for recovery of data and system
- Includes organisational as well as technical measures

Protection of IoT and OT devices

- Device level (decentralized):
  - Software based solutions
  - Hardware based solutions
  - Actors involved: equipments manufacures, service providers

- Network level (centralized)
  - Solutions built into the network
  - Actors involved: Network operators

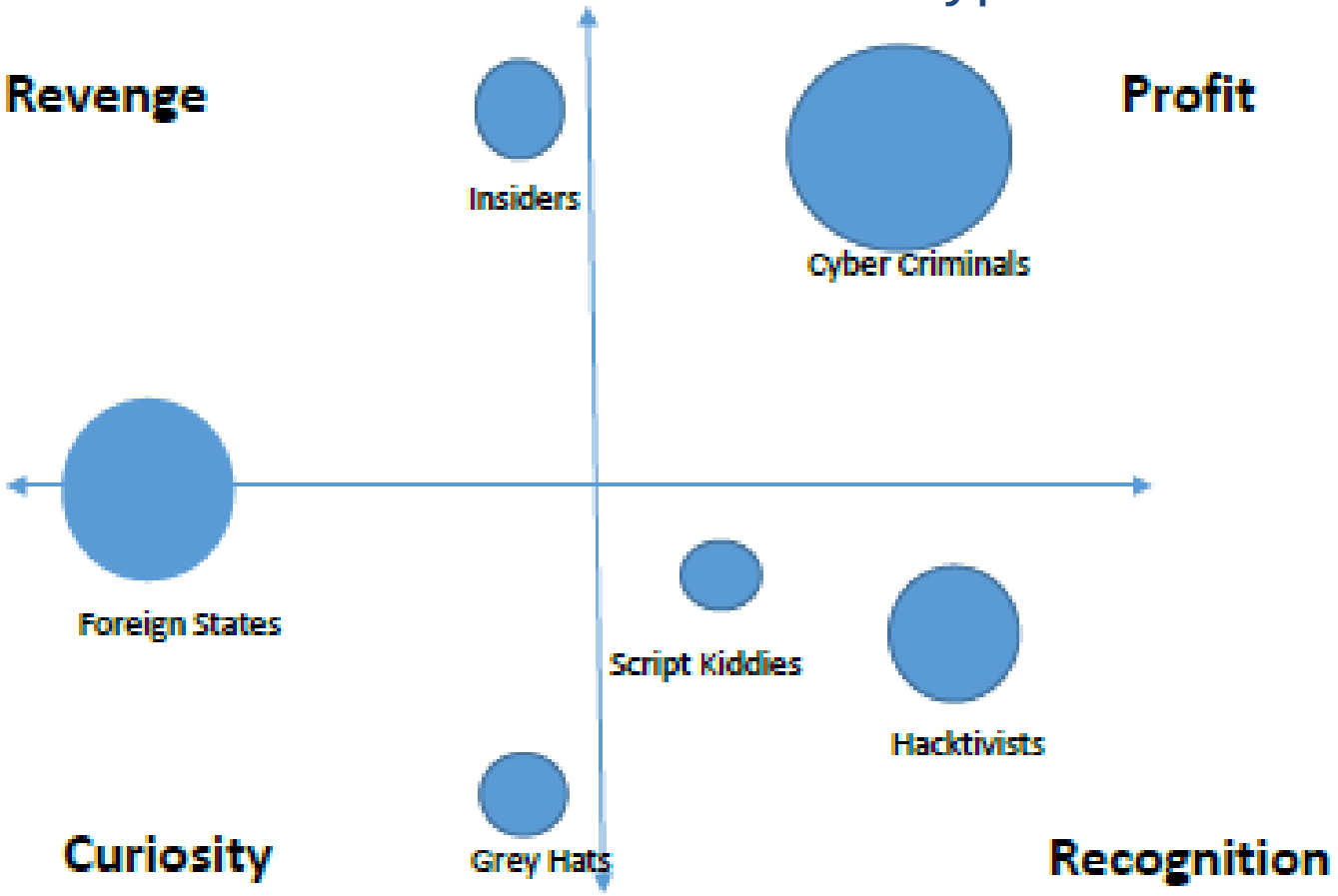
IoT and OT challenges

- Limited computing power
- Constraints in power supply
- Implies that cryptography solutions are difficult to implement
- Increasing connectivity of OT devices
- Often outdated old software
- Physical accessibility

Cybersecurity Market: Prime Threads (ENISA THREAT Landscape Nov. 2022)

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

Cybersecurity Market II: Motivations and hacker types



Cybersecurity Network Effects and Externalities

- Network effect and Externalities related to infomation economics and privacy
  - Breach in information security for others (e.g. Privacy)
- DDOS attacks
  - Vulnerable devices e.g. sensors
- Supply Chain risk attacks
  - Companies can be attacked via vulnerable business partners
- Encouragement and Strengthening of hackers
- Interuption in provision of services
  - Especially relevant for public utilities and other key sectors

Is Cybersecurity of IoT and OT a public good?

- Information is usually seen as a public good, as it is non rivalrous and partly non-excludable
- Public good characteristics relate mainly to **protect** and **detect** in the NIST framework.
- Anti-virus software, Firewalls and other intrusion prevention systems are all private goods.
- If devices are used for attaciking others, externalities are created
- Threat intelligence, vulnerability information sharing, collective response to cyber-attacks, integrity of elections, and critical infrastructure protection have the characteristics of public goods

Conclusion on economic characteristics of Cybersecurity

- Economic characteristics depend on the kind of core functions of cybersecurity which are in focus
- Cybersecurity share characteristics with public goods.
- Cybersecurity exposes considerable positive externalities.
- End users do not perceive adequate incentives to secure their machines, in part due to insufficient information.

Tentative policy implications

- Standardization and certification of devices in order to protect attacks on devices
  - Mandatory or voluntary?
  - What about existing devices?
- Protection at network level:
  - Possible to protect both old and new devices?

Thank you for your attention

Privacy, Information security, and cybersecurity

- Privacy (GDPR)
  - Deals only with personal information
- Information security
  - Deals with protection of information
- Cybersecurity
  - Deals with protection of digital information and digital infrastructures
  - Does not include off-line data and infrastructures