8th Annual Industrial Control Systems Security Workshop
(co-located with ACSAC'22)

Cybersecurity in the Smart Grid: Practitioners' Perspective

Jacqueline Meyer, Giovanni Apruzzese

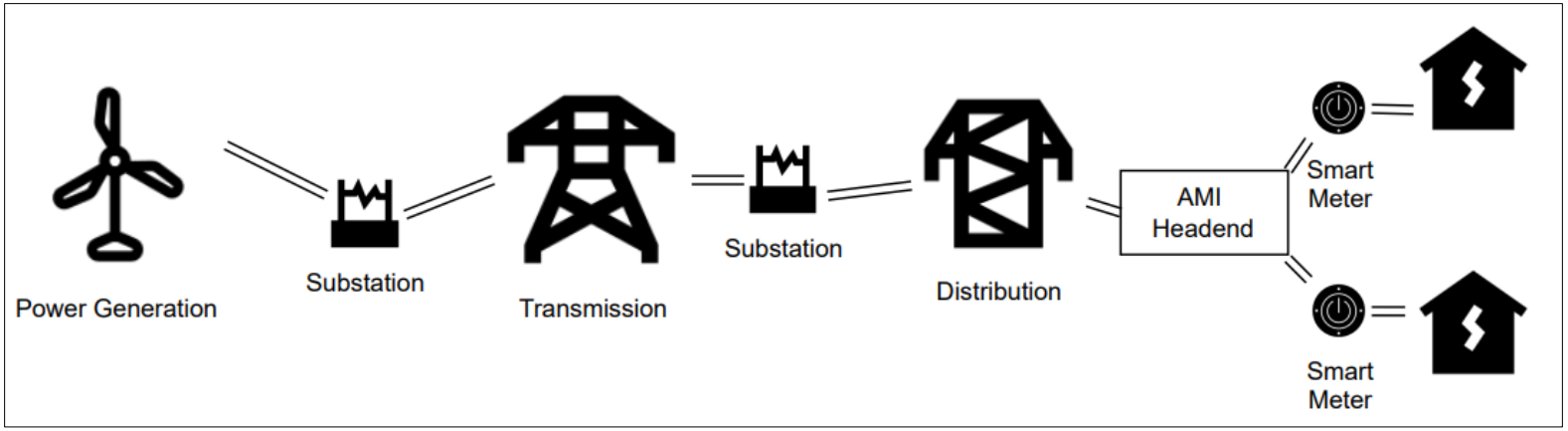
UNIVERSITÄT LIECHTENSTEIN

December 6th, 2022

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

The Smart Grid (SG) – aka: the lifeforce of our society

- The SG has seen the take-off of digitalisation in recent years



- **Pro: improved efficiency**
- **Con: enormous (and attractive!) attack surface**

- Example: Ukraine 2015 → **225'000** households affected
- Worst case scenario cyber attack on SG in Switzerland → **12 billion CHF = 2% of GDP**

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What do we (don't) know?

Abundant research efforts studied the cybersecurity of the Smart Grid, **BUT**

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What do we (don't) know?

Abundant research efforts studied the cybersecurity of the Smart Grid, **BUT**

- Original Attacks (and countermeasures)
  - Often studied in testbeds -> **no real-world confirmation**
  - E.g. Mathematical analysis of impact (Xiang et al., 2017)
- Literature reviews
  - Based on scientific papers -> **limited practical relevance**
  - E.g. elaboration of SG cyber-security strategy (El Mrabet et al., 2018)
- Case Studies
  - Only focus on past (reported) attacks -> **unclear value today**
  - E.g., Stuxnet occurred in 2006
- Interviews
  - Few studies, of limited scope -> **no comprehensive overview**
  - E.g. Stakeholders (Fischer-Hübner et al., 2021) or info-sharing in the USA (Randall and Allen, 2021)

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What do we (don't) know?

Abundant research efforts studied the cybersecurity of the Smart Grid, **BUT**

- Original Attacks (and countermeasures)
  - Often studied in testbeds -> **no real-world confirmation**
  - E.g. Mathematical analysis of impact (Xiang et al., 2017)
- Literature reviews
  - Based on scientific papers -> **limited practical relevance**
  - E.g. elaboration of SG cyber-security strategy (El Mrabet et al., 2018)
- Case Studies
  - Only focus on past (reported) attacks -> **unclear value today**
  - E.g., Stuxnet occurred in 2006
- Interviews
  - Few studies, of limited scope -> **no comprehensive overview**
  - E.g. Stakeholders (Fischer-Hübner et al., 2021) or info-sharing in the USA (Randall and Allen, 2021)

In this work, we elucidate:
- the (internal) perspective of SG's **practitioners**;
- an **holistic** and **recent** vision on the problem.

→ Highly constructive for future endeavours (beneficial for the real SG)

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Holistic view – why?

The SG is a complex system, which entails various stakeholders.

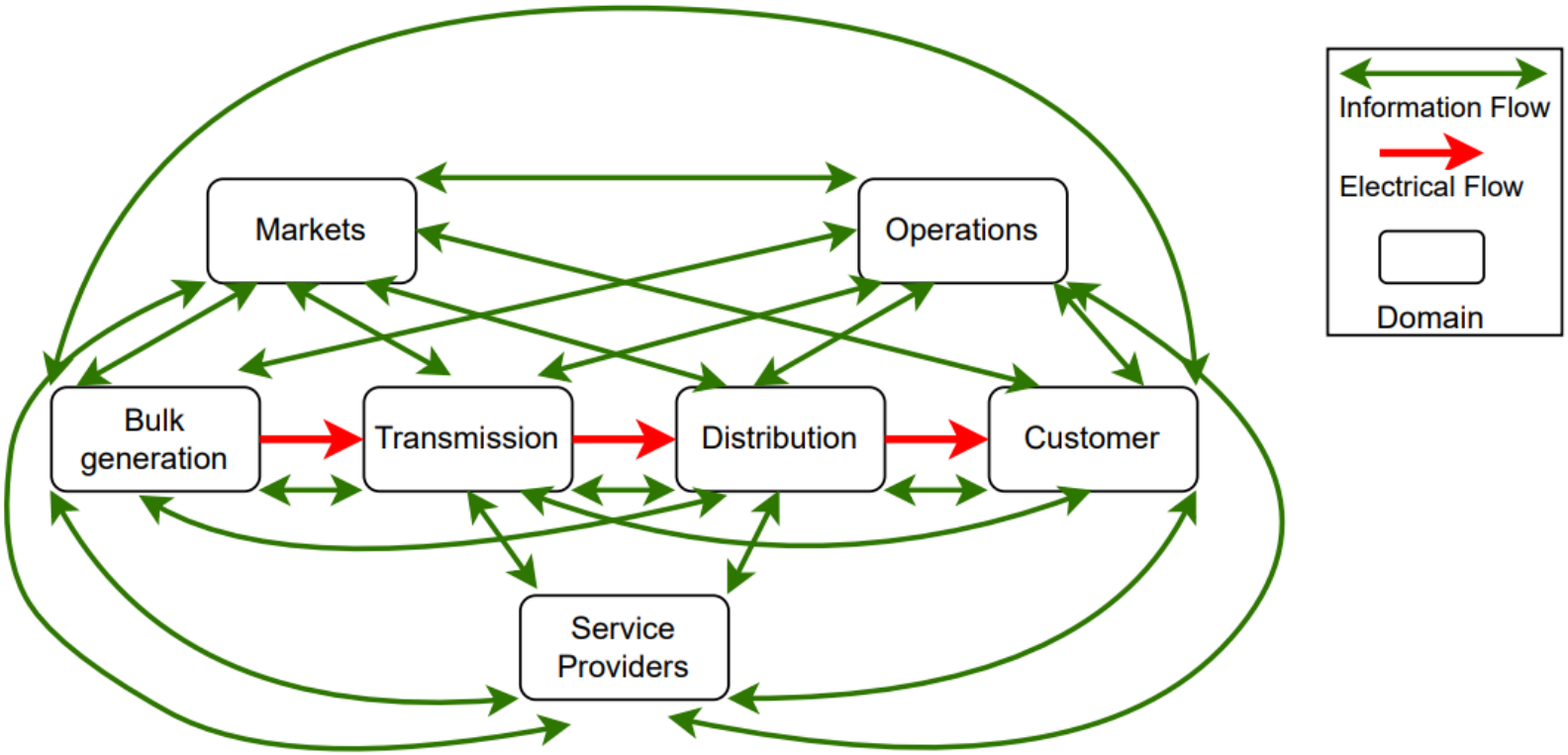


Fig. 3: The NIST conceptual model of the SG, spanning across 7 domains—all of which are covered in our research.

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Our objective

- We began our study by asking ourselves a broad research question:

  “What is the state-of-the-art of cyber-security in the European SG?”

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Our objective

- We began our study by asking ourselves a broad research question:

  "What is the state-of-the-art of cyber-security in the European SG?"

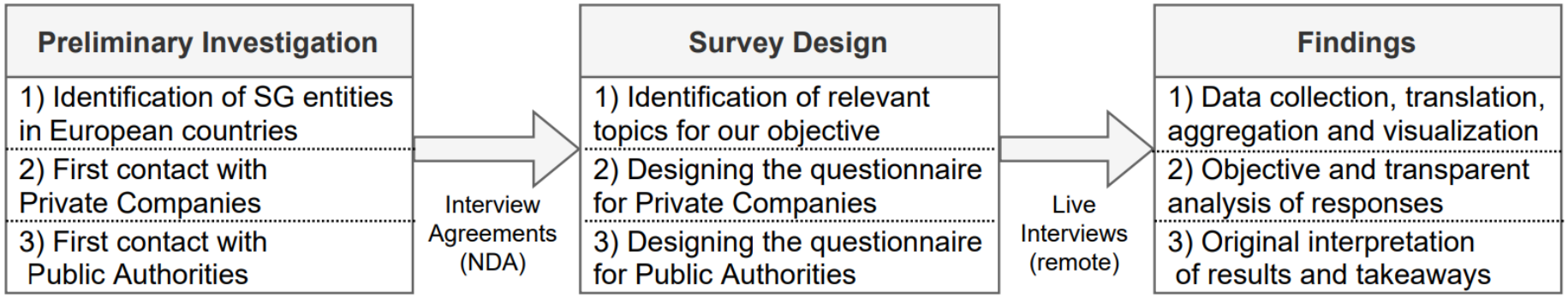
- We aimed to elucidate:
  1. Experiences with *past cyber-attacks*
  2. General security landscape of *companies operating the SG*
  3. Cyber-security related *risk-assessment strategies*
  4. *Perceived threat* of various attack scenarios
  5. *New technologies* and trends in the SG
  6. The opinion of *public authorities* w.r.t. the companies' managed cybersecurity

- As we will show, however, some finding surprised us
  - This is why we wrote this paper! ☺

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What we did

- Structured interviews with 18 entities related to the SG:
  - 14 private companies (operating the SG in diverse countries in Europe)
  - 4 public authorities (operating in the countries of the private companies' headquarters)

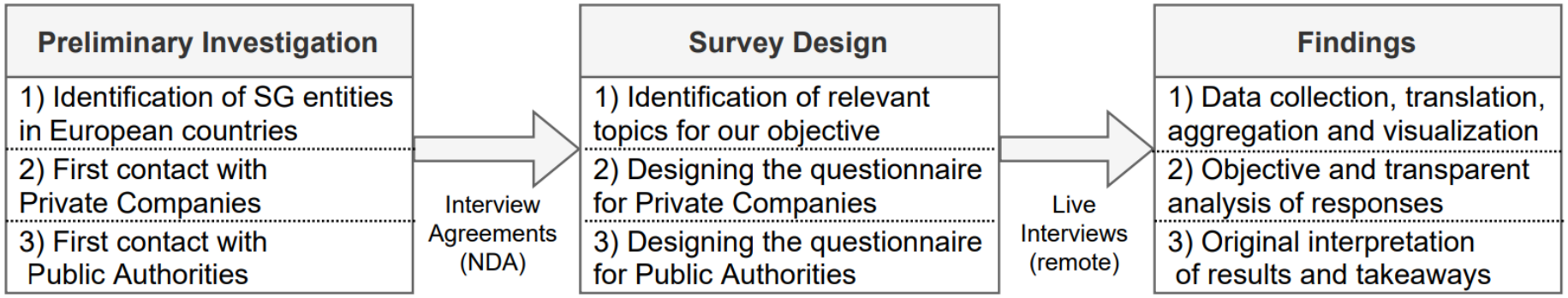


(timeframe: January to March 2022)

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What we did (& challenges)

- Structured interviews with 18 entities related to the SG:
  - 14 private companies (operating the SG in diverse countries in Europe)
  - 4 public authorities (operating in the countries of the private companies' headquarters)



(timeframe: January to March 2022)

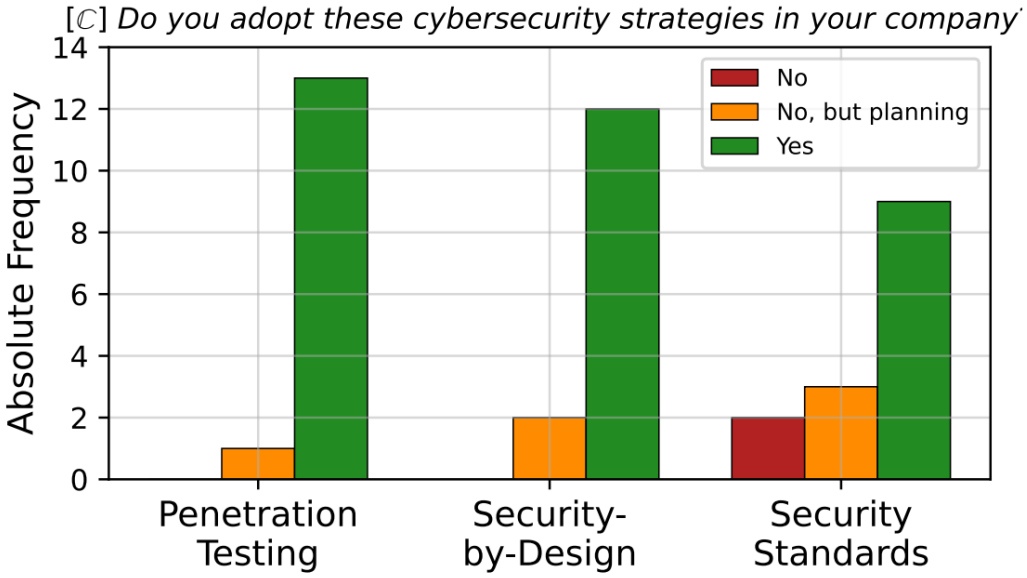
Challenges

- We aimed to interview more than 30 companies, but only 14 accepted
- 5 companies agreed to help us only after phone calls lasting more than 60 minutes
- Only 5 interviews with the private companies were carried out on the scheduled date
- We sent a total of 145 emails (between Nov. 2021 and Feb. 2022)
- Different language

UNIVERSITÄT LIECHTENSTEIN

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Generic 1 (ℂ = Private Companies, 𝔸= Public Authorities)

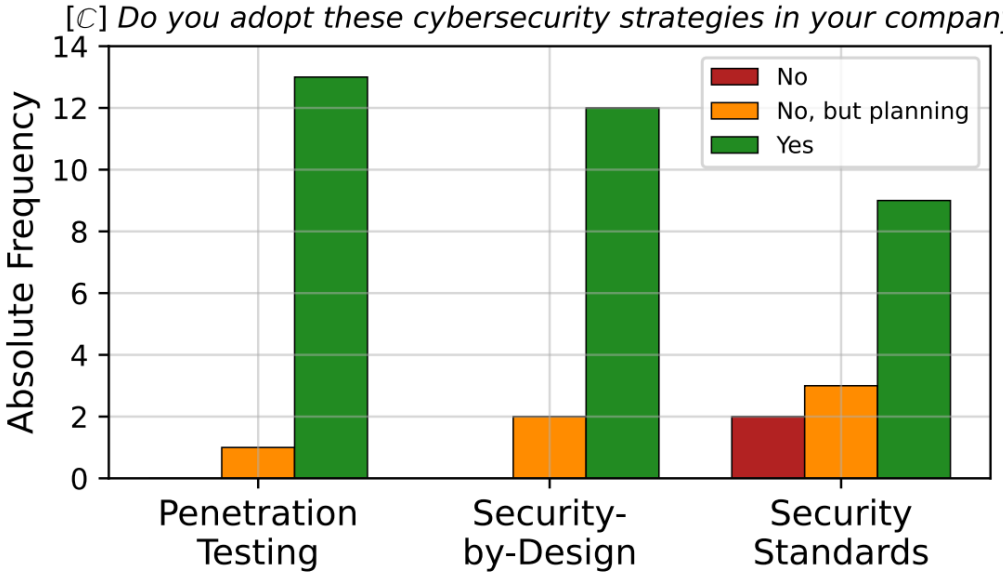


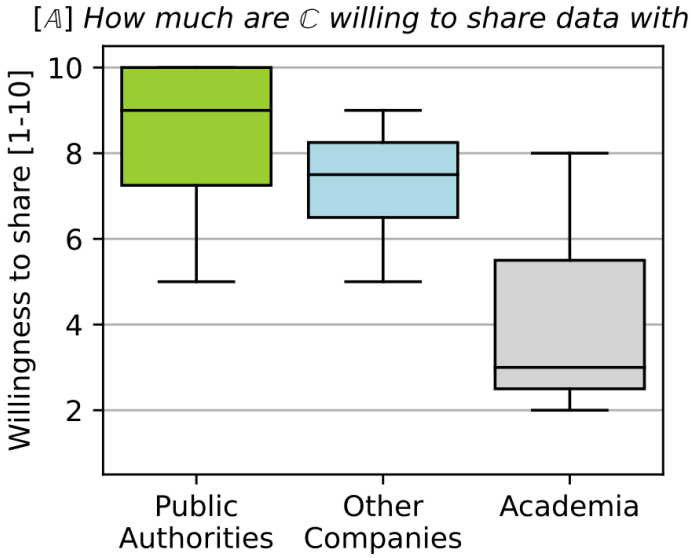
Mid-/Top-level management	
Option	*Freq.*
They are fully aware of the risks and prioritise cyber-security	64.29%
They are fully aware of the risks, but cyber-security is not a priority	21.43%
They are not aware of the risks, but are educated on the topic	7.14%
No answer	7.14%

Employees	
Option	*Freq.*
They are aware fully of the risks and education is evaluated regularly	50.00%
They are not fully aware of the risks, but are educated on the topic	42.86%
They are not aware of the risks, and unlikely to improve in the short-term	0.00%
No answer	7.14%

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Generic 1 (ℂ = Private Companies, 𝔸= Public Authorities)





Mid-/Top-level management	
Option	*Freq.*
They are fully aware of the risks and prioritise cyber-security	64.29%
They are fully aware of the risks, but cyber-security is not a priority	21.43%
They are not aware of the risks, but are educated on the topic	7.14%
No answer	7.14%

Employees	
Option	*Freq.*
They are aware fully of the risks and education is evaluated regularly	50.00%
They are not fully aware of the risks, but are educated on the topic	42.86%
They are not aware of the risks, and unlikely to improve in the short-term	0.00%
No answer	7.14%

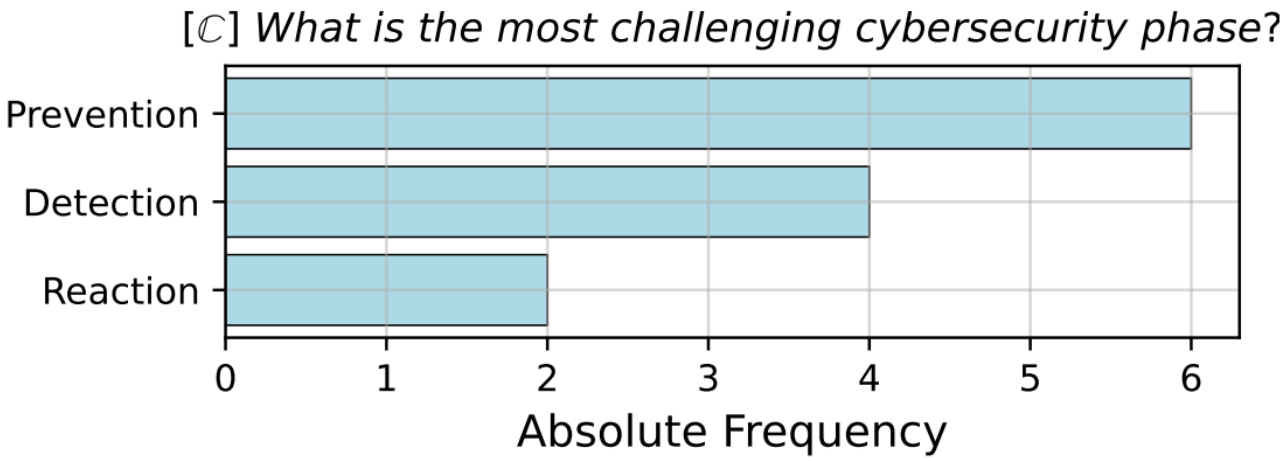
Capabilities (perception)

- None of 𝔸 believe ℂ to have "excellent" capabilities w.r.t. "detection" and "prevention"…
- …but 25% of 𝔸 believe that ℂ have "excellent" capabilities w.r.t. "reaction".

mismatch!

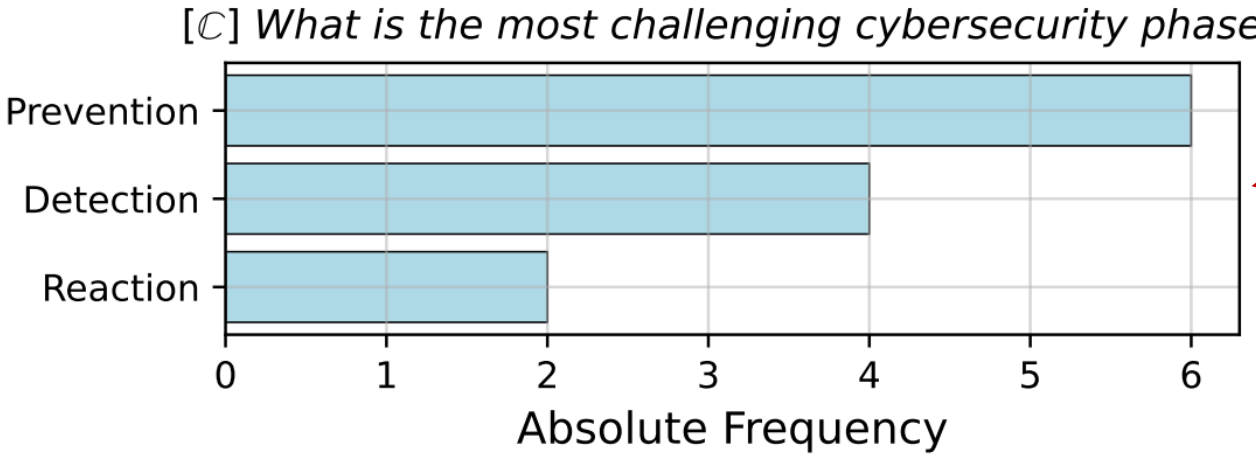
Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Generic 2 (ℂ = Private Companies, 𝔸= Public Authorities)



Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Generic 2 (ℂ = Private Companies, 𝔸= Public Authorities)

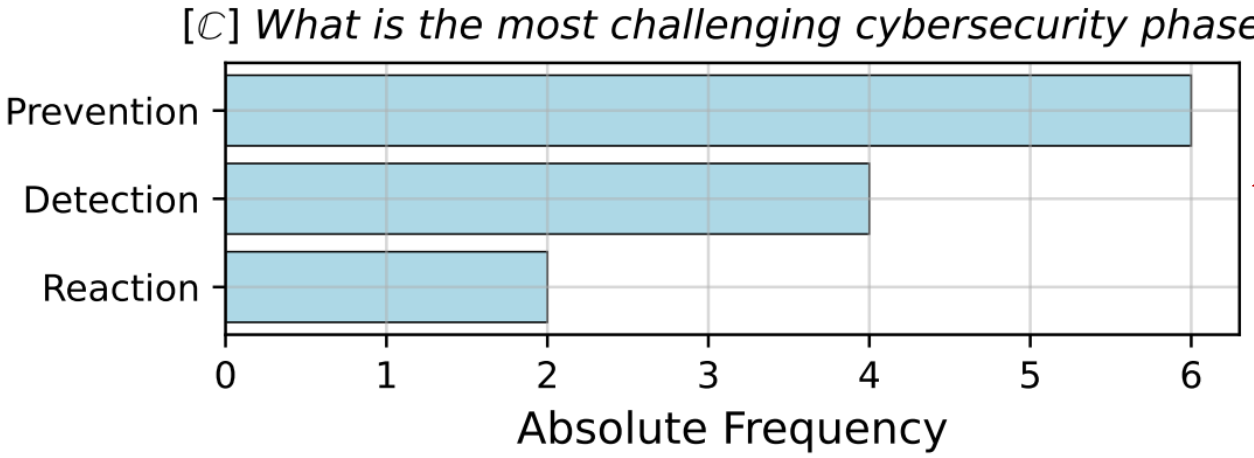


mismatch!

All of 𝔸 believe that "detection" is the toughest phase!

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Generic 2 (ℂ = Private Companies, 𝔸= Public Authorities)



mismatch!

All of 𝔸 believe that "detection" is the toughest phase!

What about **research** (papers)?

- Few focus on "reaction"
- Most focus on "detection"

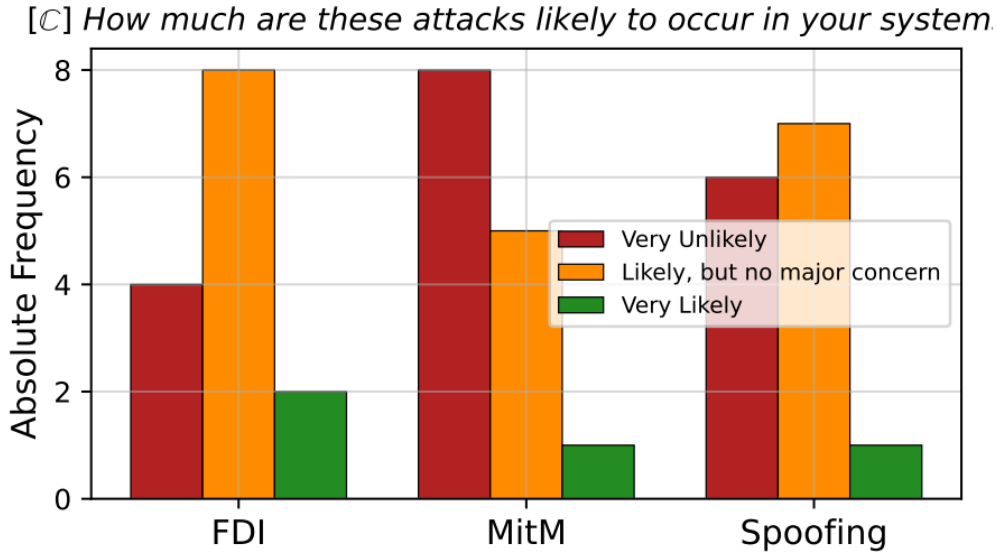
(Salazar and Cardenas, 2019)

mismatch!

UNIVERSITÄT LIECHTENSTEIN

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

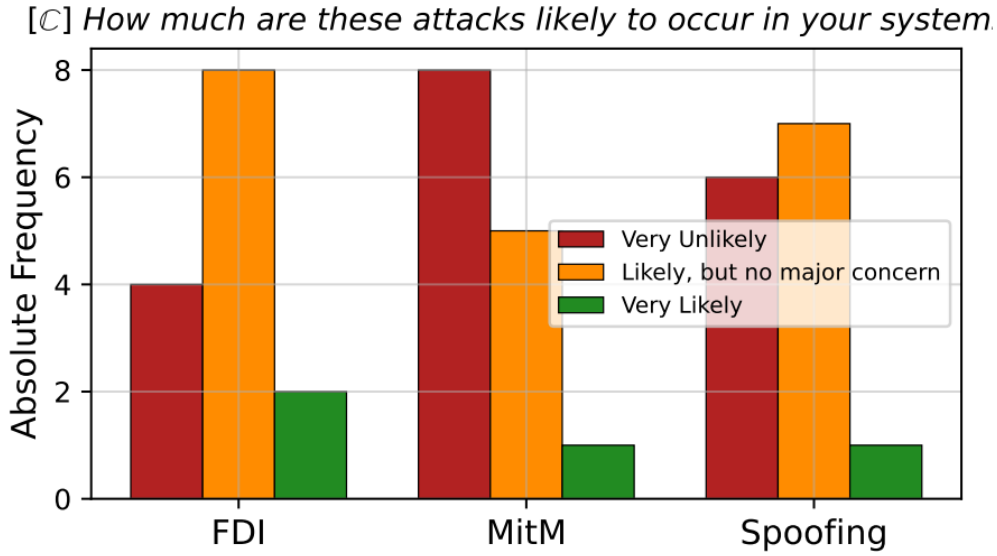
Findings – Threats (ℂ = Private Companies, 𝔸= Public Authorities)

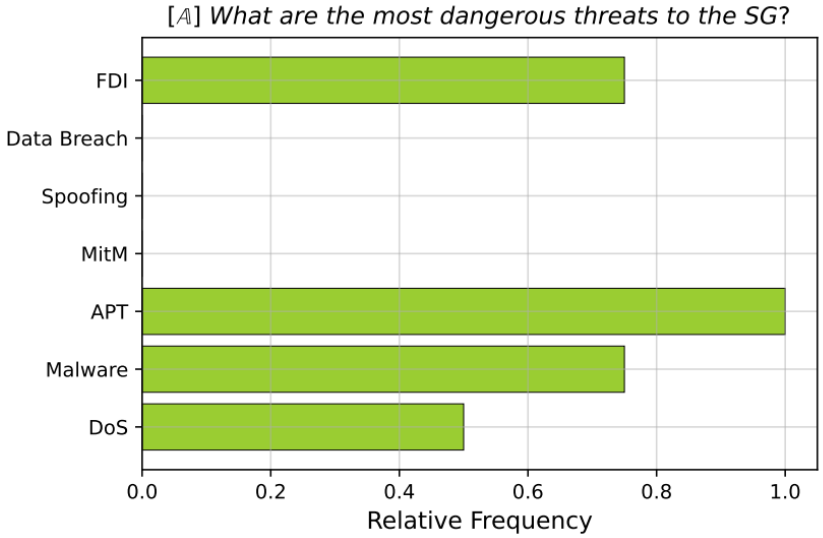


- 100% of ℂ consider their systems to be at risk from **APT**
- 86% of ℂ consider **illegitimate access to customer data** to be 'threatening' (and data confidentiality is problematic)
- 0% of ℂ consider **DoS** to be problematic

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Threats (ℂ = Private Companies, 𝔸= Public Authorities)

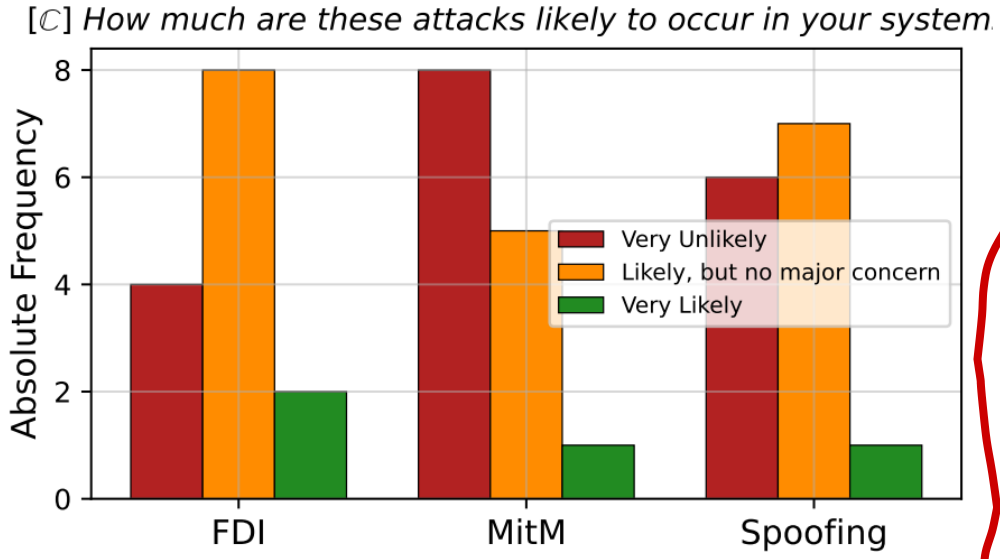


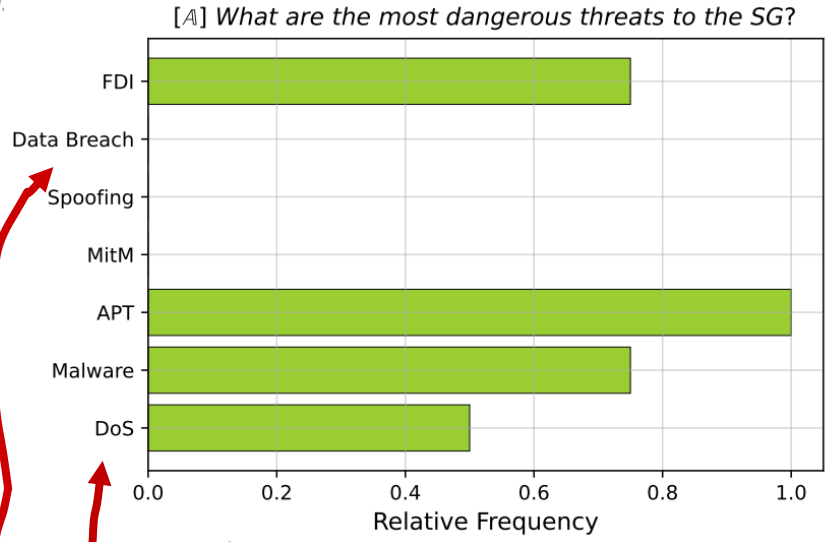


- 100% of ℂ consider their systems to be at risk from **APT**
- 86% of ℂ consider **illegitimate access to customer data** to be 'threatening' (and data confidentiality is problematic)
- 0% of ℂ consider **DoS** to be problematic

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Threats (ℂ = Private Companies, 𝔸= Public Authorities)





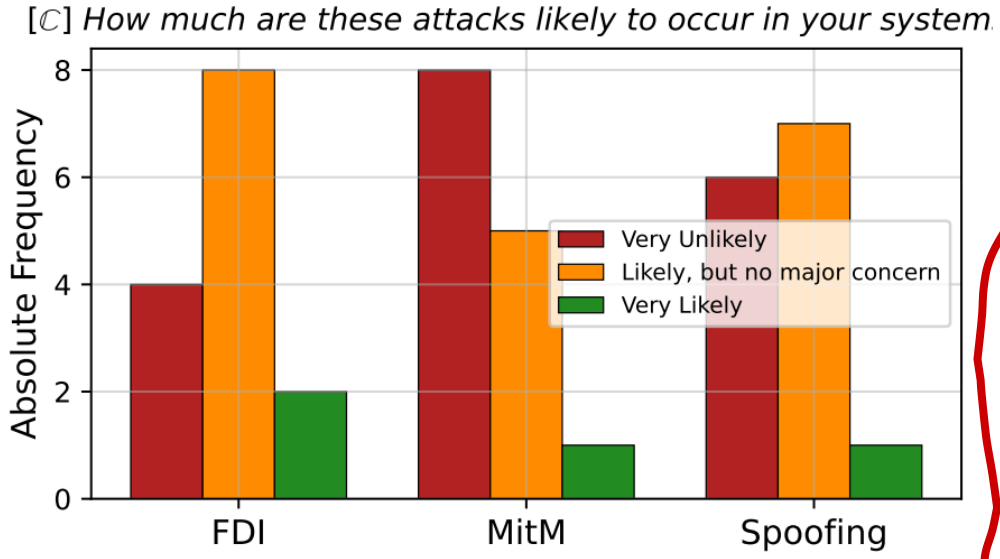
- 100% of ℂ consider their systems to be at risk from **APT**
- 86% of ℂ consider **illegitimate access to customer data** to be 'threatening' (and data confidentiality is problematic)
- 0% of ℂ consider **DoS** to be problematic

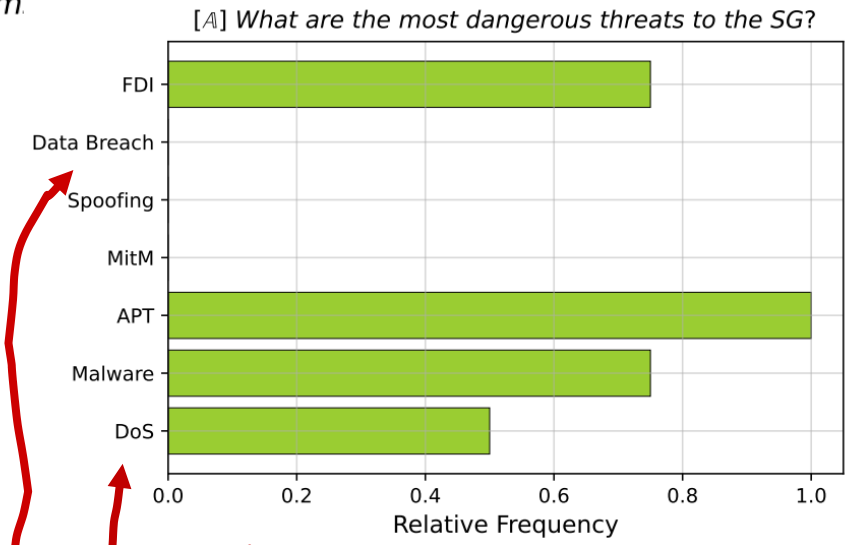
mismatch!

UNIVERSITÄT LIECHTENSTEIN

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Threats (ℂ = Private Companies, 𝔸= Public Authorities)





- 100% of ℂ consider their systems to be at risk from **APT**
- 86% of ℂ consider **illegitimate access to customer data** to be 'threatening' (and data confidentiality is problematic)
- 0% of ℂ consider **DoS** to be problematic

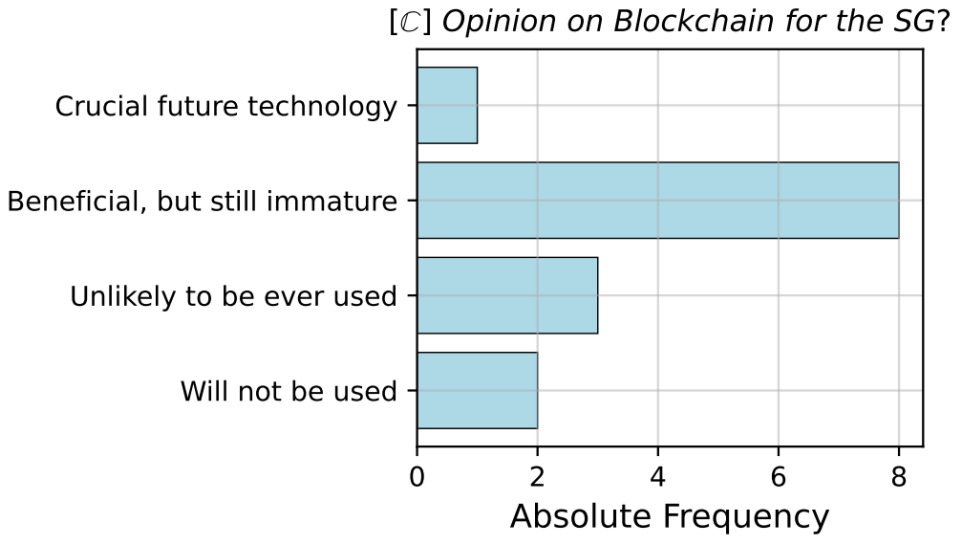
mismatch!

What about **research** (papers)?

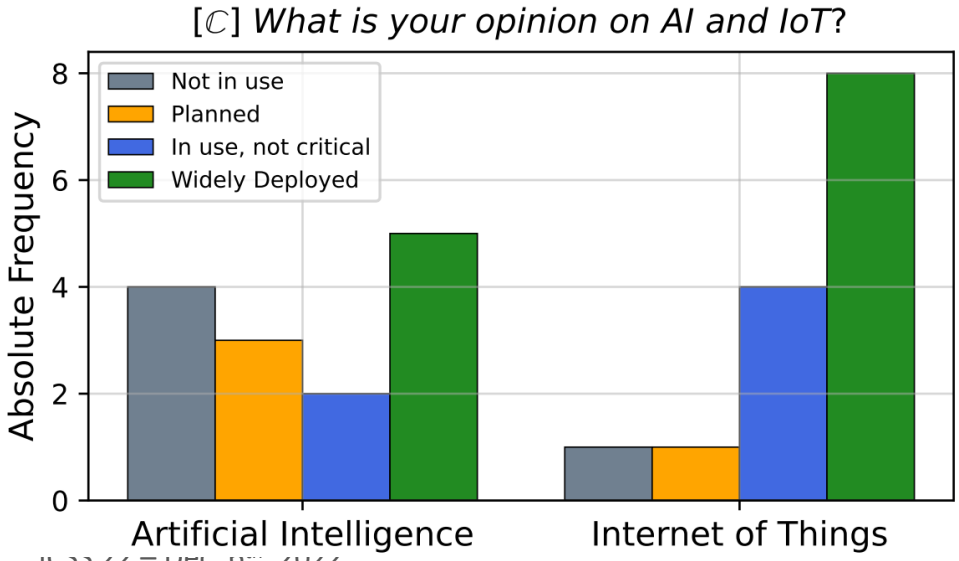
- Researchers claim that **DoS** are a serious threat to the SG…
  - Although ℂ are not worried about them!
- …and the same goes for **Spoofing** and **MitM**!
  - But ℂ and 𝔸 both agree that they are not problematic!

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Tech (ℂ = Private Companies, 𝔸= Public Authorities)



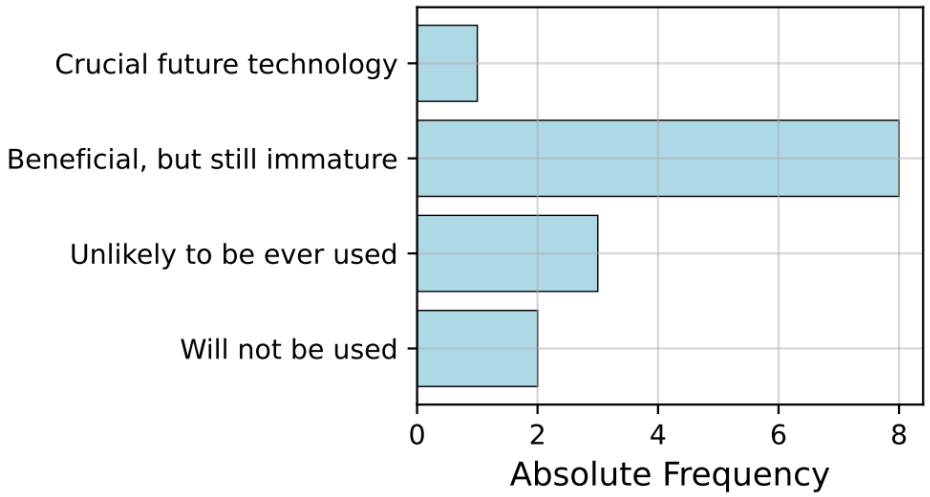
- 93% of ℂ already use Cloud solutions



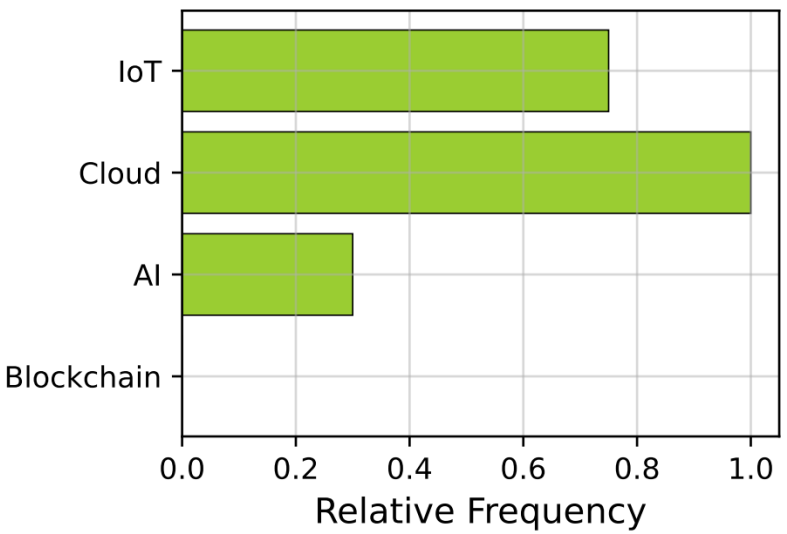
Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Tech (ℂ = Private Companies, 𝔸= Public Authorities)

[ℂ] *Opinion on Blockchain for the SG?*

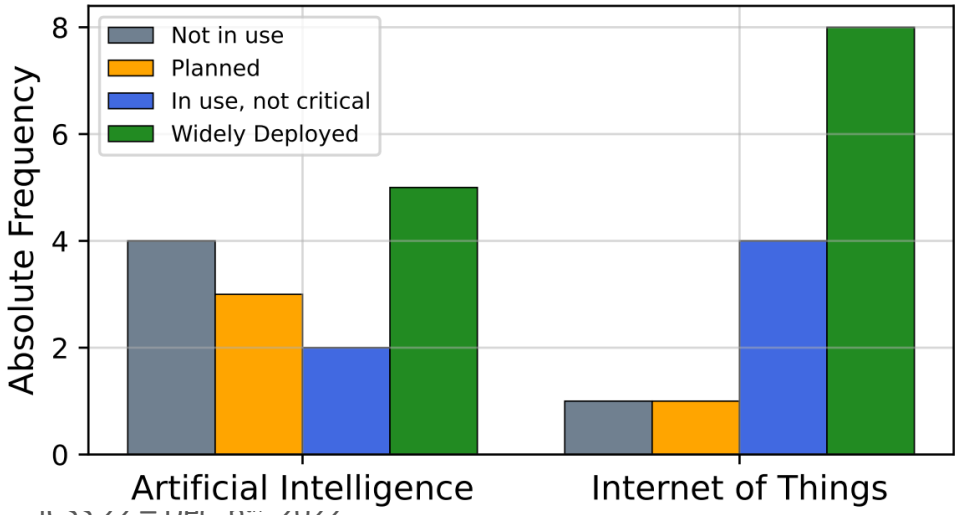


[𝔸] *Key technologies for future SG?*



- 93% of ℂ already use Cloud solutions

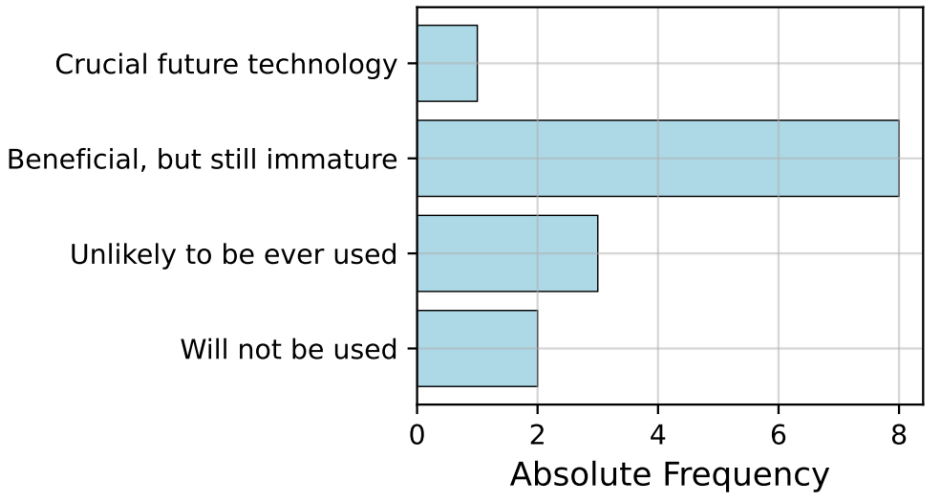
[ℂ] *What is your opinion on AI and IoT?*



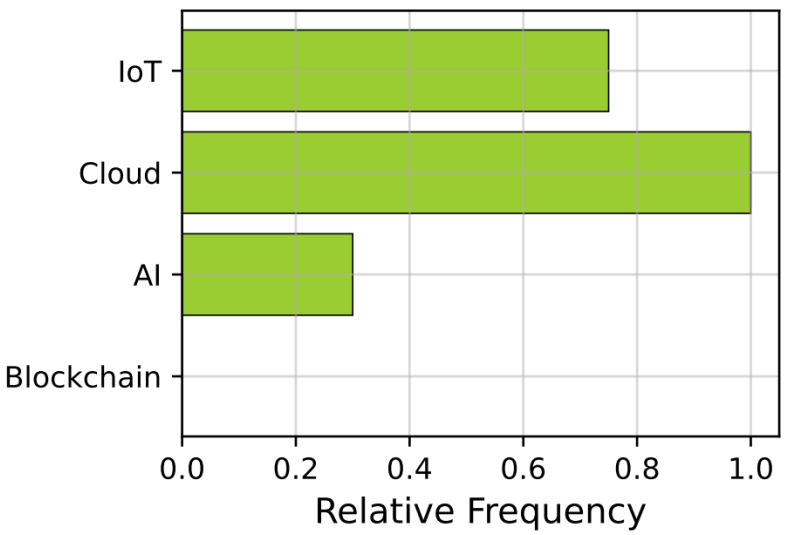
Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – Tech (ℂ = Private Companies, 𝔸= Public Authorities)

[ℂ] *Opinion on Blockchain for the SG?*

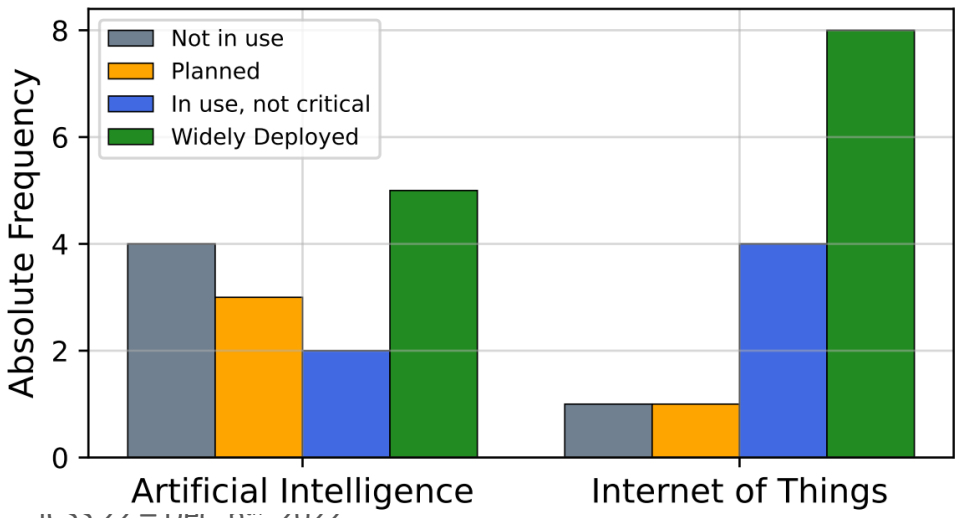


[𝔸] *Key technologies for future SG?*



- 93% of ℂ already use Cloud solutions

[ℂ] *What is your opinion on AI and IoT?*



What about **research** (papers)?

- **AI** is often claimed to be a panacea
- **Blockchain** is also depicted as a go-to

mismatch!

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – "Killware" (ℂ = Private Companies, 𝔸= Public Authorities)

Voster, 2021 (Gartner)

Eddy and Pelroth, 2020 (The New York Times)

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – "Killware" (ℂ = Private Companies, 𝔸= Public Authorities)

Voster, 2021 (Gartner)

Eddy and Pelroth, 2020 (The New York Times)

What about **research** (papers)?

- Some recent works already used the term "killware" (from (Voster, 2021))
- Many research papers are citing (Eddy and Pelroth, 2020) to claim that exploiting cyber-vulnerabilities can lead to "human death".

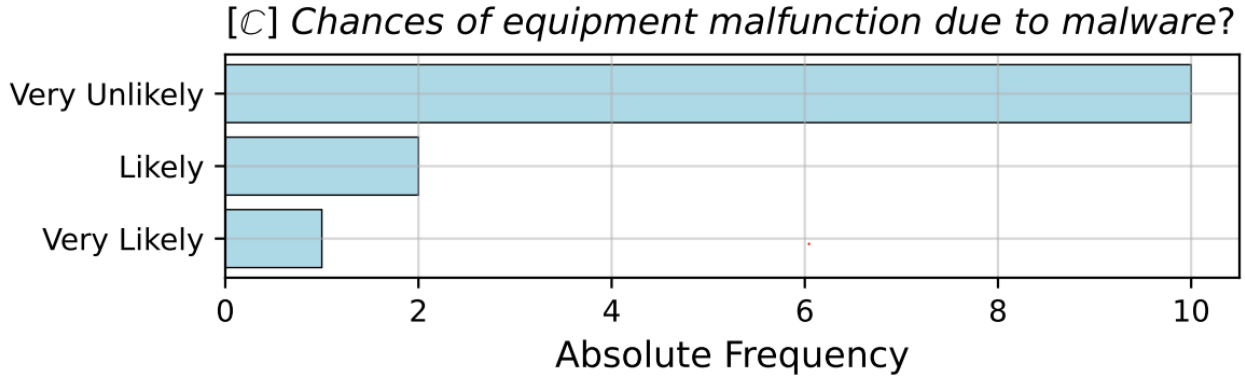
According to Google Scholar, (Eddy and Pelroth, 2020) has 33 citations as of today.

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Findings – "Killware" (ℂ = Private Companies, 𝔸= Public Authorities)

Voster, 2021 (Gartner)

Eddy and Pelroth, 2020 (The New York Times)



"How likely it is that malware can lead to human death?" (*killware*)

- According to ℂ : 15% unrealistic; 70% unlikely
- According to 𝔸 : 50% very likely; 50% likely

What about **research** (papers)?

- Some recent works already used the term "killware" (from (Voster, 2021))
- Many research papers are citing (Eddy and Pelroth, 2020) to claim that exploiting cyber-vulnerabilities can lead to "human death".

According to Google Scholar, (Eddy and Pelroth, 2020) has 33 citations as of today.

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Mismatch (and interpretation)

- Practitioners ($\mathbb{C}$ and $\mathbb{A}$) vs Research:
  - MitM and Spoofing
  - Blockchain
  - Artificial Intelligence
  - Reaction Phase

- Private ($\mathbb{C}$) vs Public ($\mathbb{A}$) entities:
  - Prevention Phase
  - Capabilities
  - Data Confidentiality and Replication
  - FDI and DoS

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What about sovereign and legislative bodies?

- After elaborating some comments received by $\mathbb{C}$, we derived an original model that explains the role of **regulations** in the context of the SG

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

What about sovereign and legislative bodies?

- After elaborating some comments received by ℂ, we derived an original model that explains the role of **regulations** in the context of the SG

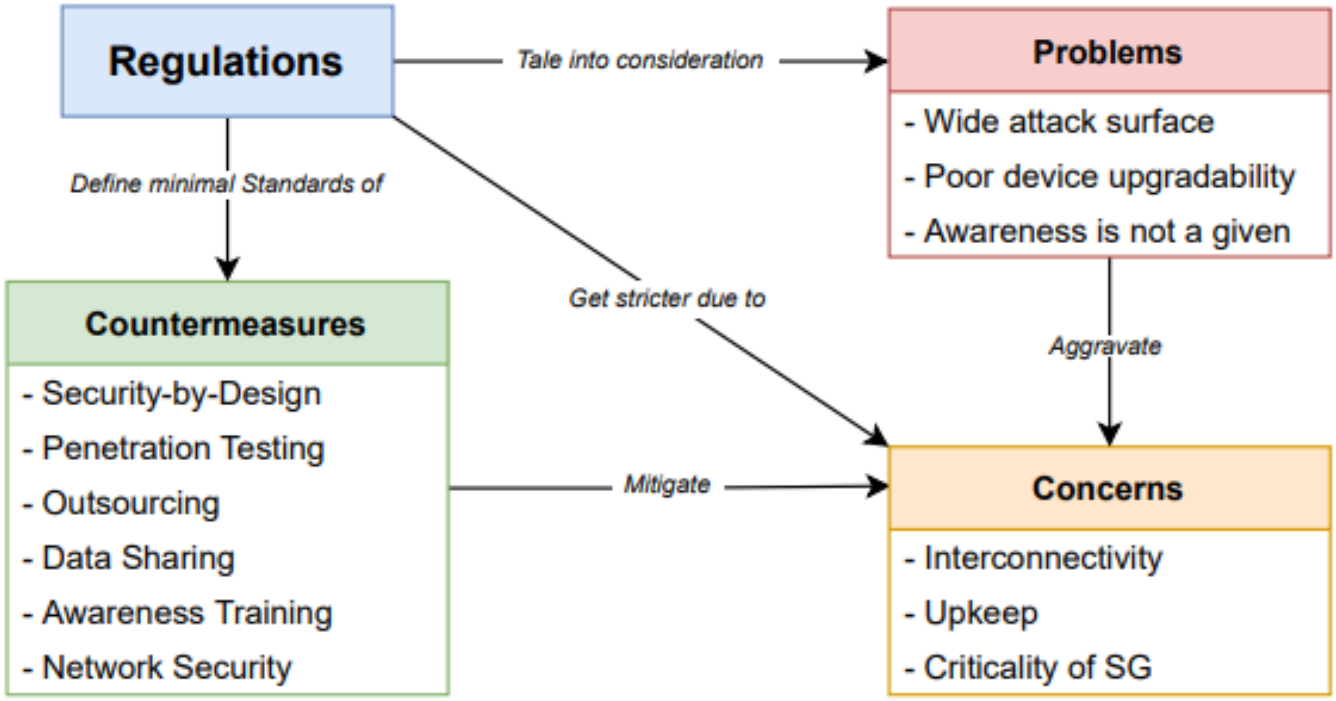


Fig. 13: Our original model displaying the relationships between *regulations* the cybersecurity of the SG.

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Takeaways

Private Companies

Public Authorities

Researchers

Regulatory Bodies

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Takeaways

Private Companies more open in cooperating with research institutions.

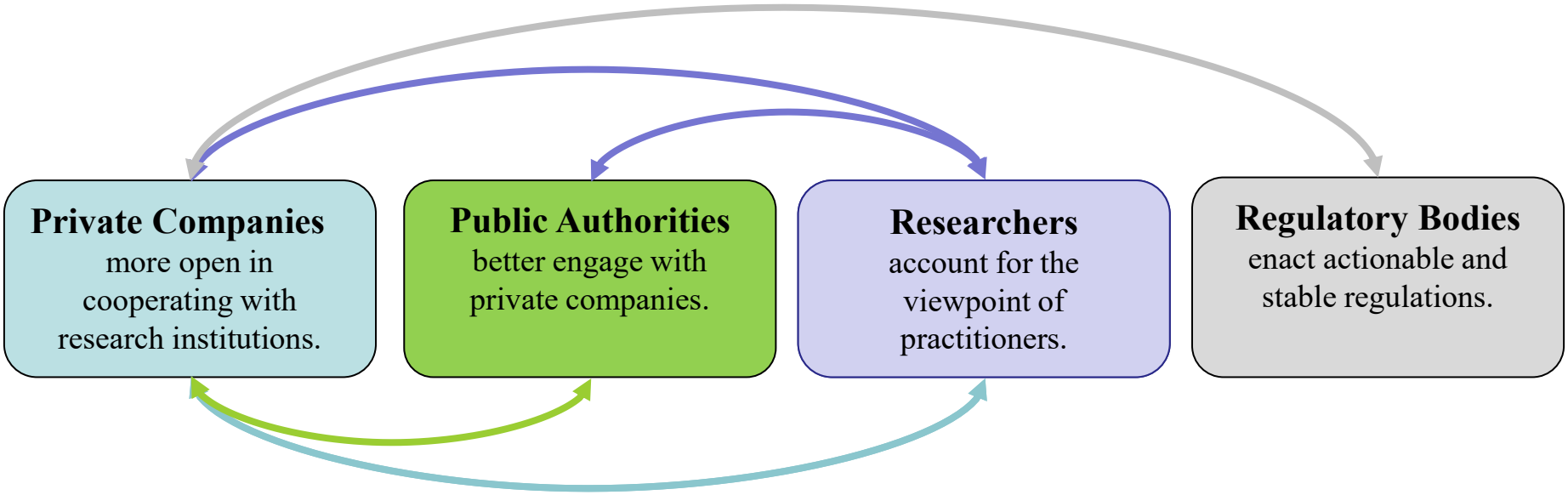
Public Authorities better engage with private companies.

Researchers account for the viewpoint of practitioners.

Regulatory Bodies enact actionable and stable regulations.

Giovanni Apruzzese, *PhD*
giovanni.apruzzese@uni.li

Takeaways



Recommendation: all such spheres should better communicate and interact with each other. Ultimately, they have a *common goal*: improving the security of the SG.

8th Annual Industrial Control Systems Security Workshop
(co-located with ACSAC'22)

Cybersecurity in the Smart Grid: Practitioners' Perspective

Jacqueline Meyer, Giovanni Apruzzese

UNIVERSITÄT LIECHTENSTEIN

December 6th, 2022