Are we ready for an outage of the digital infrastructures? – Lessons learned from Ukraine

Cyberwarfare Activities: Denmark

- Increased number of cyberattacks since 2022 Russian invasion in Ukraine
- Attacks conducted mostly without definite attribution, with ”hacktivists” taking responsibility
- Scope: so far mostly short-term and short-impact
  - However, cumulative effects might apply
  - Future attacks are an open question

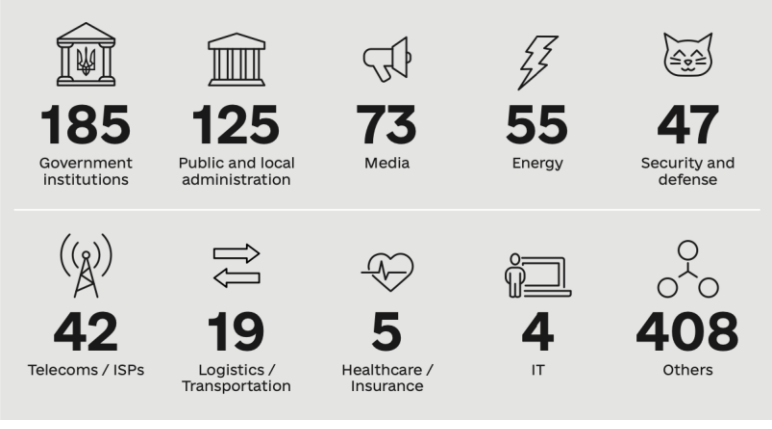
	Threat level
Cyber espionage	**Very high**
Cyber crime	**Very high**
Cyber activism	High
Destructive cyber attacks	Medium

Source: CFCS

Cyberwarfare Activities: Ukraine

- Increasing rate of overall cyber incidents since 2022 → However, decreasing number of critical incidents

- Commonly targetted sectors: government, energy, media, security and defense, telecommunications…



Source: SSSCIP

Optimising Denmark's Cyber Emergency

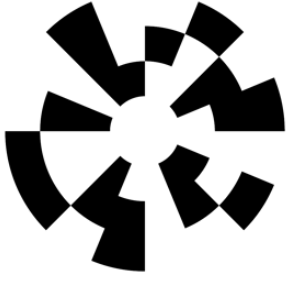
- Funded by the National Defence Technology Center as a pilot project

- Partners
  - IT University of Copenhagen (Oksana Kulyk, Yuliia Storm Larsen, Jari Kichbusch)
  - University of Southern Denmark (Peter Mayer)
  - The Danish Institute of Fire and Security Technology (Jorge Ivan Contreras-Cardeno)

IT UNIVERSITY OF CPH

SDU
Syddansk Universitet

DBI



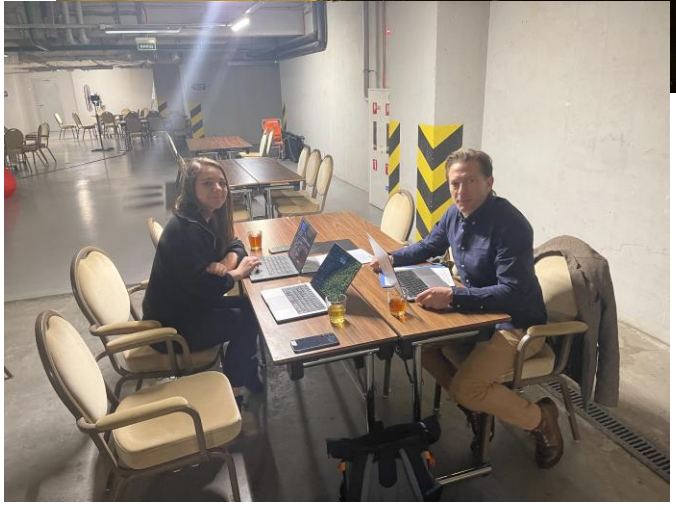
Nationalt Forsvarsteknologisk Center

Our Research

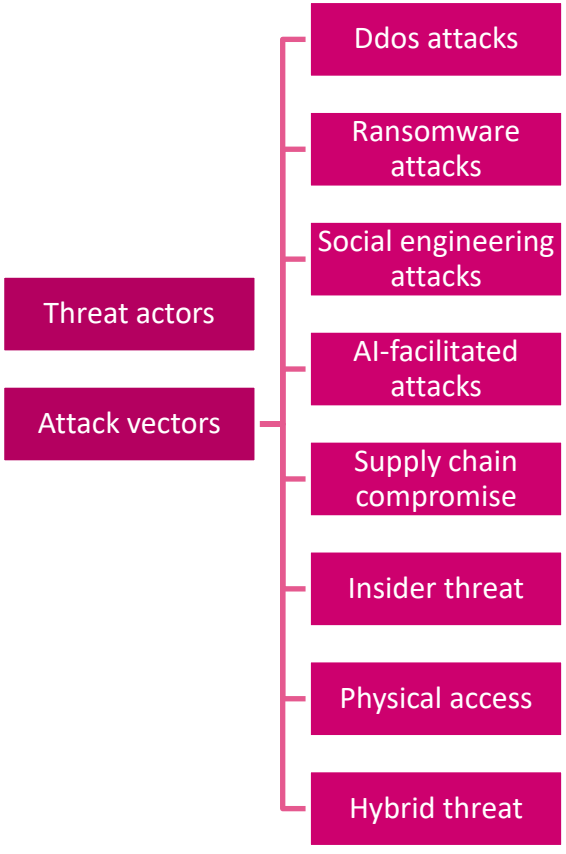
- Field investigation in Ukraine in May 2025
- Interviews in Denmark in 2025

- Methodology
  - Conduct interviews with civilians, company representatives and governmental officials
  - Analyse interviews to understand the scope and impact of information warfare activities

- Findings:
  - Relevant threats related to cyberwarfare
  - Harms for society
  - Mitigations of harms
  - Challenges and open questions



Threats

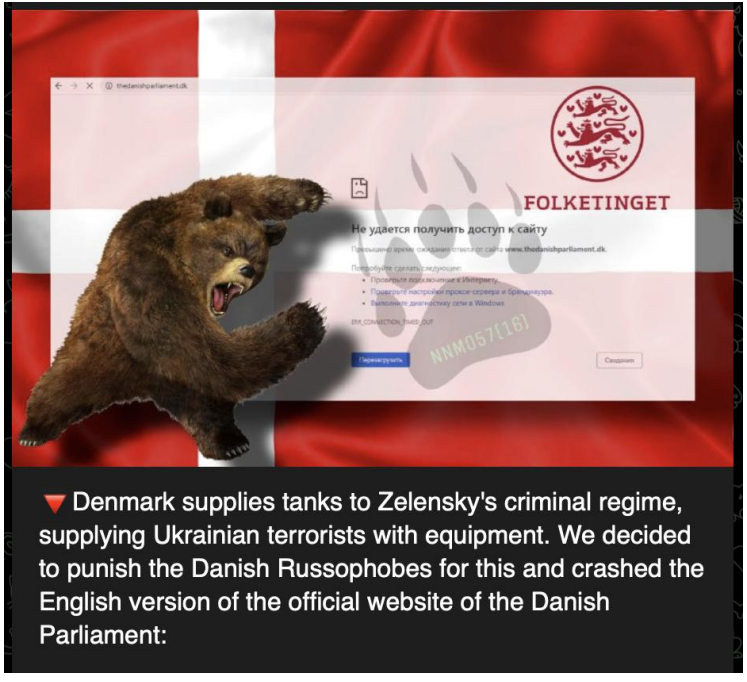

Threat actors
Attack vectors
Ddos attacks
Ransomware attacks
Social engineering attacks
AI-facilitated attacks
Supply chain compromise
Insider threat
Physical access
Hybrid threat

Threat Actors

- Cyberattacks and information warfare from state actors considered a threat
- Number of state actors mentioned, either as attributed attacks or potential threats
  - Ukraine: mostly Russia, also China
  - Denmark: Russia, China, potentially USA
- Goal: espionage, damage to critical infrastructure, political influence
- Sometimes focus on persistent and covert presence, to collect data and/or prepare for future attacks

DDoS Attacks and Ransomware

- Ddos attacks
  - Very common, but in most cases a nuissance rather than a real threat
  - Common tool of hacktivists
- Ransomware attacks
  - Can be very damaging, including to critical infrastructure
  - Attacks require more skills compare to Ddos, but hacking for hire services are available



Social Engineering and AI-facilitated Attacks

- Social engineering
  - Phishing as an initial access vector; ”hack the human, not the system”
  - Information influence campaigns, e.g. disinformation

- Role of AI
  - Social engineering made easier, e.g. through personalised messages or deepfakes
  - Other uses of AI, e.g. through malicious or unrustworthy AI applications

“We got a lot of phishing attacks to our employees. Also, vishing, we identified all sorts of. [..] So this is the important part because the human, you know, they can make a lot of mistakes.” UA

“…the second someone starts putting data into [Chinese-developed AI systems], it all goes to the Chinese. […] People don't think before they put data into AI just because they think they're using something friendly - but they're not..” DK

Supply Chain Compromise and Insider Threat

- Supply chain compromise
  - Malicious supplier, supplier with insufficient security, supplier that has been taken over e.g. via conventional warfare…
  - Controls required to reduce trust in third parties

- Insider threat
  - Privileged access through coercion, bribery or persuation
  - Often successful in absense of checks on valid accounts

"At the beginning of the war [...] representatives of the Russian Federation, namely, representatives of FSB, repeatedly tried to establish contacts with [our organisation]. [...] They were interested in all kinds of information, databases, all information about all departments. [...] In return, they offered promotions, career advancement, and so on at different levels. When they win." UA

Physical Access and Hybrid Threat

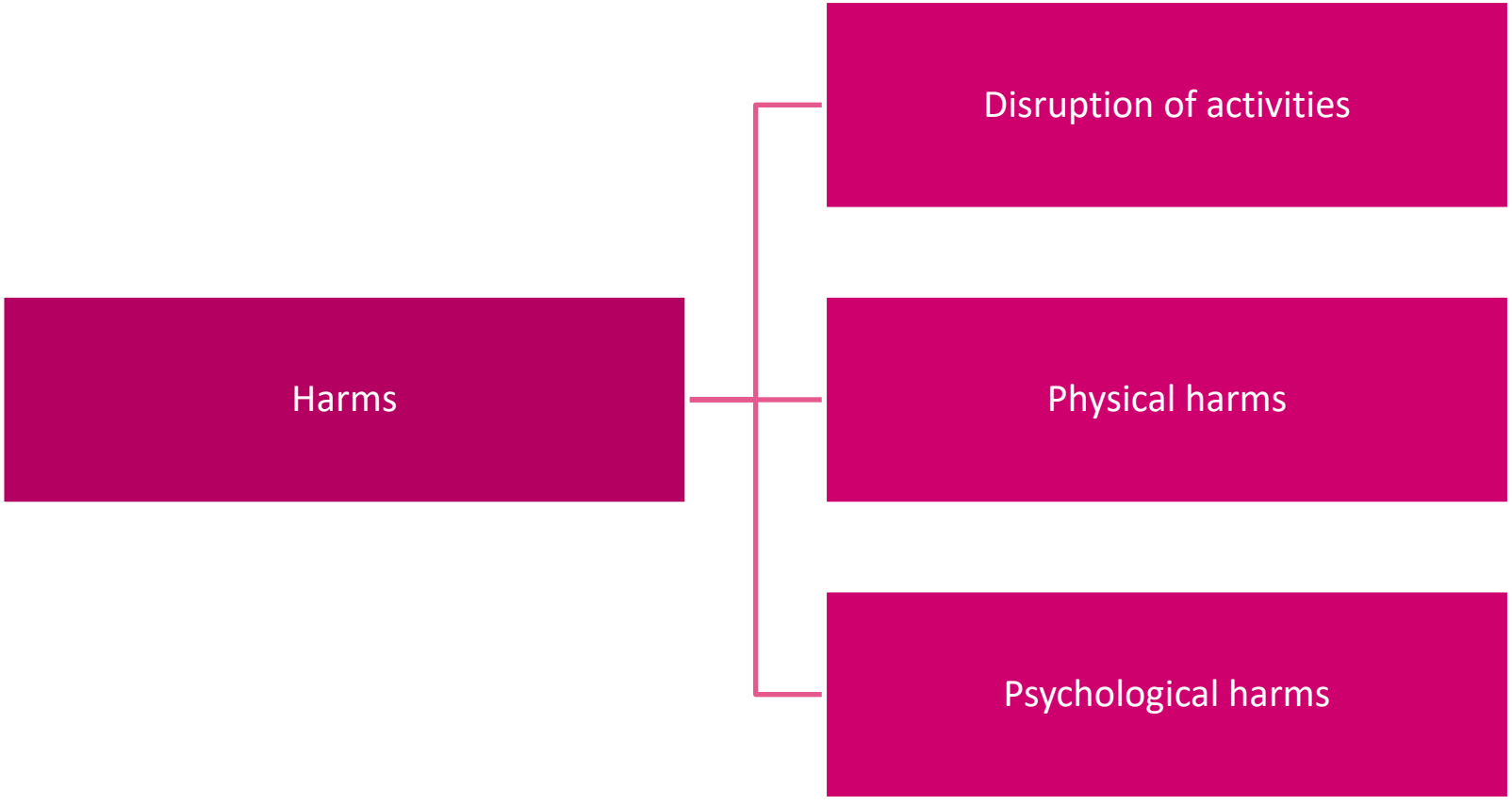
- Physical access
  - Use of physical access to security-critical systems
  - Done through social engineering, insider threats, military occupation…

"…they took some territory of Ukraine […] our base stations, through them, [the attackers] try to penetrate our environment." UA

- Hybrid threat
  - Use of multiple attacks vectors to achieve objective
  - Physical attacks, e.g. damaging connection cables
  - Attacks on other sectors, e.g. electricity

"When we talk about submarine cables, we are more vulnerable, because there are many submarine cables but not a huge amount and if you hit several of them, it will start to get critical." DK

Harms


Harms
Disruption of activities
Physical harms
Psychological harms

Disruption of Activities

- Inability to uses daily services, e.g. payment systems/telecommunications → **especially relevant in highly digitalised countries**
- Inability to access critical services, e.g. healthcare
- Vulnerable groups might be especially affected, e.g. refugees or people in need for governmental assistance

"So we are all used to the comfort of just picking up your phone when you want to connect or call someone and when you don't have it, it is like well, what shall I do? So no one died, it didn't affect us like that, but it was difficult and tasks that we were used to perform fast took a long time" UA

"But it won't be of much help if we find ourselves in a situation like in Spain as an example, right? You can't get cash. Can't go down in a shop and buy food because you can't pay because your credit card does not work, because there is no electricity. You cannot withdraw cash at an ATM because there's no cash." DK

Physical Harms

- Resulting from lack of access to critical services
  - Outage of hospital systems → no treating patients
  - Outage of telecommunication → no way to call the doctor
  - Outage of transportation → no way to get sick people to healthcare facilities

- Chain reactions, the longer the crisis persists

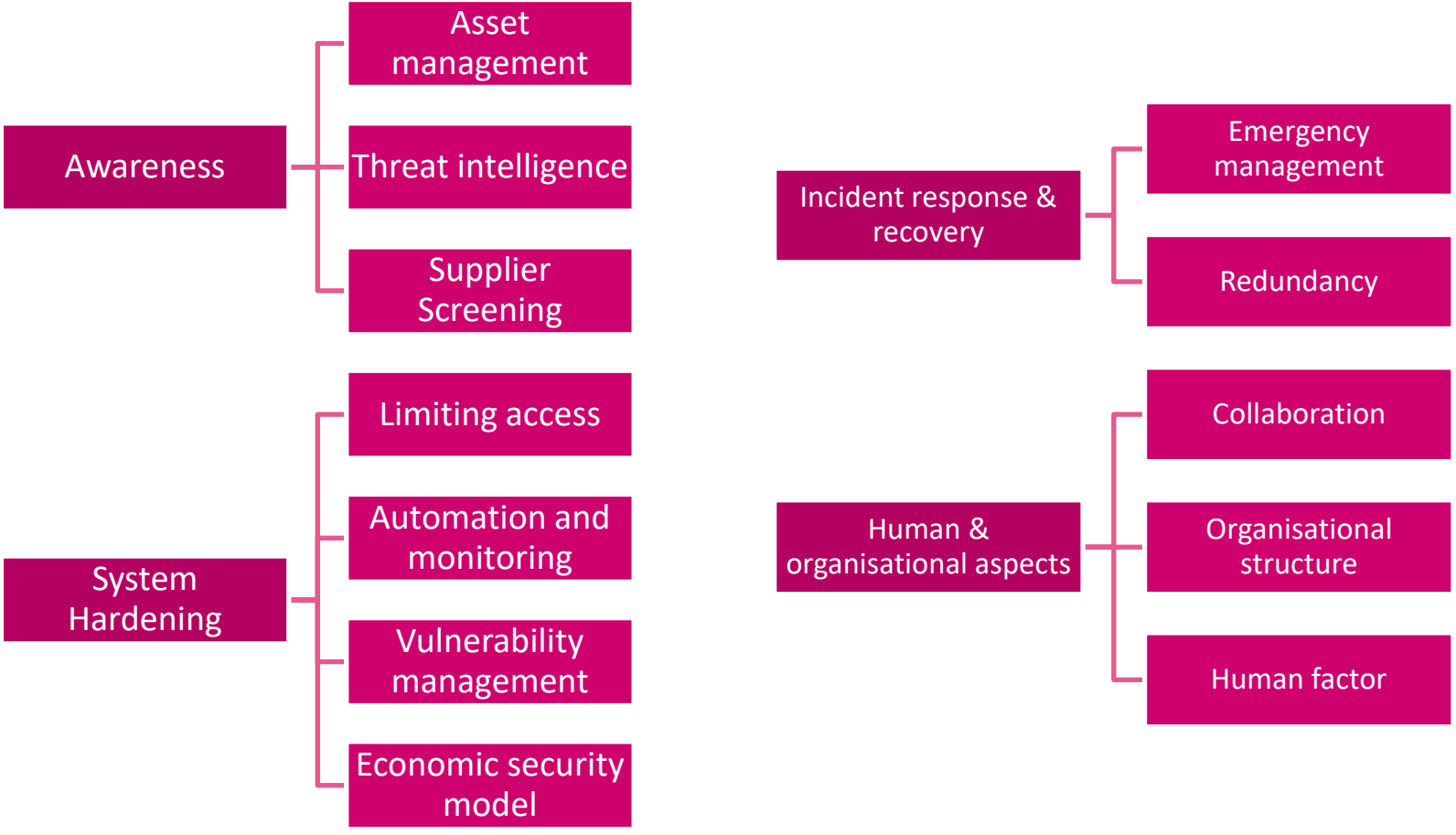
"So one of my patients, suddenly he didn't have Internet connection and no mobile phone connection. What to do? He was in pain, took ibuprofens. Paracetamol. That's all. Then he began to vomit and feel nausea. And then when he came to me 5 or 10 days later and he had a big myocardial infarction and could only be saved by a heart transplantation. And he lost the time, the gold time for cure." UA

Psychological Harms

- Stress due to unknown situation, inability to get in touch with affected family/friends…
- Lack of community support (e.g. if there is no way to get in touch with others)
- General panic, distrust, fear…
- Potential for influence operations

"In the time of war you really want to stay connected with your family and with your friends, because it's the only thing which preserves you, is that you are not alone, that you are part of a bigger group or a bigger mechanism. You will not survive on your own. You want to survive with others and probably that's one of the critical social things that mobile connection provides to the citizens." UA

Mitigations of Harms



Awareness of Threats

- Identify the assets vulnerable to threats

"Asset management is very important. So you need to understand, how many assets do you have in the company? Which of them is critical? Identify how you are protecting them. This is the first thing what you need to do." UA

- Sharing of threat intelligence among peers and competitors

"We can see a lot more and if we merged with the other telecoms, we could see everything. That is also what we're are going to suggest; that we should all look into this the threat we are facing now together." DK

- Coordination along full supply chain is needed to prevent attacks

"We had this kind of issue previous year in 2024, in May, when our supplier didn't know that the infrastructure is infected. And, Russian guys, they penetrate through the environment through some asset like, found their way, and then they try to join our environment." UA

System Hardening

- Limiting access through zero-trust approaches

> *"The conclusion would be that anyone could be a victim of that type of incident and that it proves that the zero-trust approach is the only viable approach."* UA

- Monitoring and automation can limit the burden even when under heavy attack, especially for AI driven attacks

> *"With the rise of AI, cybersecurity needs much more automation. We need automated responses to counter automated attacks. Instead of focusing on specific hacker tools, we should look holistically at the techniques being used, since there might be many exploits created daily, but the underlying techniques remain similar. Only about four new techniques emerge annually."* DK

- The government can help organizations to meet their cybersecurity needs

> *"We are actually trying to establish a community, which will facilitate the hiring process, identify the best candidate in hiring process, we support the onboarding, the training, the retraining, the reskilling, upskilling, sharing best practices and everything."* UA

Incident Response & Recovery

- Planning for emergencies must be baked into the organizational culture

- Telecommunications providers have a special responsibility due to the harms that can occur when citizens cannot reach emergency services

"We didn't have any contingency plan. We had nothing. We did it on the go. It was surprising that we succeeded but has something to do with experience. Now, we have made a contingency plan. We are also training it. Do we practice enough? No, we are probably not, but we do it at least once a year ." DK

"To my knowledge we never practiced something like a big telecommunication breakdown in Denmark." DK

Human & Organisational Aspects

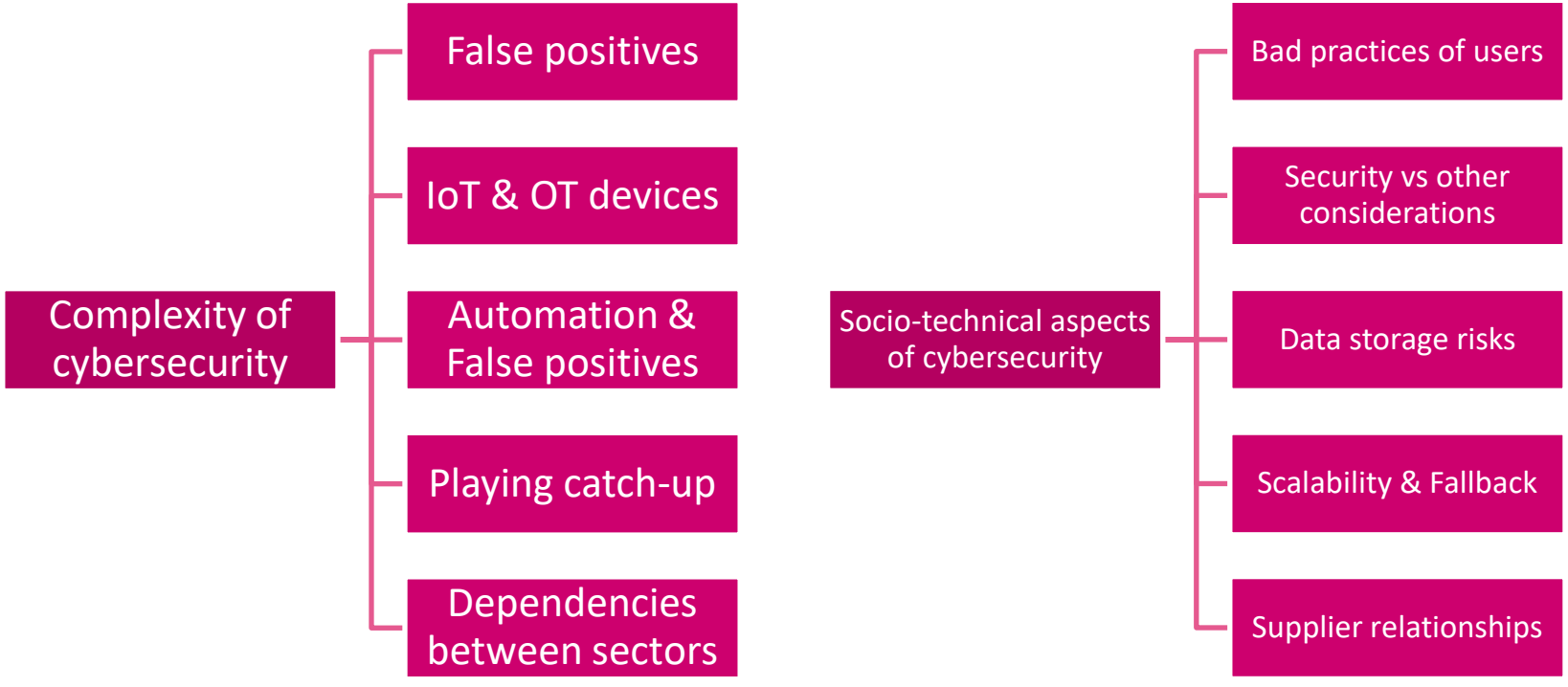
- Collaboration between public entities and private organizations needs to be improved
- Also international collaboration must be strengthened
- Denmark's societal trust also applies to critical infrastructures

"The police focused on finding the criminals and not to help us. So they needed X number of people to help find the criminals and we had to say that it's more important for our company to survive than to find the criminals." DK

"It would be beneficial to strengthen cooperation with the Swedes because they have a solid concept where they train collaboration between telecom providers and authorities. They conduct exercises where providers repair cables together in the mud, ignoring competitive concerns. We should do the same in Denmark." DK

"We haven't considered something like Starlink yet. […] We trust the critical infrastructure." DK

Challenges


Complexity of cybersecurity
False positives
IoT & OT devices
Automation & False positives
Playing catch-up
Dependencies between sectors
Socio-technical aspects of cybersecurity
Bad practices of users
Security vs other considerations
Data storage risks
Scalability & Fallback
Supplier relationships

Challenges

- Some critical infrastructure organizations rely heavily on not only OT, but also IoT devices which can lead to larger attack surfaces

"It happens everywhere - from full access for cars to expensive medications. If you want them, go to all places with Bluetooth devices. It doesn't matter - we are really bad at physical security." DK

- Sometimes legislation gets in the way of enacting proper protections

"We tried to be honest, to get out of the Ukraine because it would be really safe. And now, while there are some rules from the government side that we cannot because we are critical infrastructure. And we cannot move the personal data to out of the country." UA

- Foreign vendors do their own risk assessments and their products might not remain available

"But we saw another issue when some vendors, they just left Ukraine without notification, without anything. […] We have support here. And then like just that they leave us without any support. […] But when it comes to the BCP, business continuity plan, it's not exactly like that they are described here. Because you cannot even imagine during the war, the critical vendor can leave the country without the support. So that's the big issue, because I face it, is that I didn't expect at all." UA

Summary

- State actors are a concern due to their capability for large-scale attacks
- Multiple attack vectors, from relatively easy to mitigate (DDoS) to more challenging (supply chain compromise)
- Potential for societal harms, including physical harms/loss of life
- Cooperation between companies and countries creates a win-win situation
- Government support crucial through action and legislation