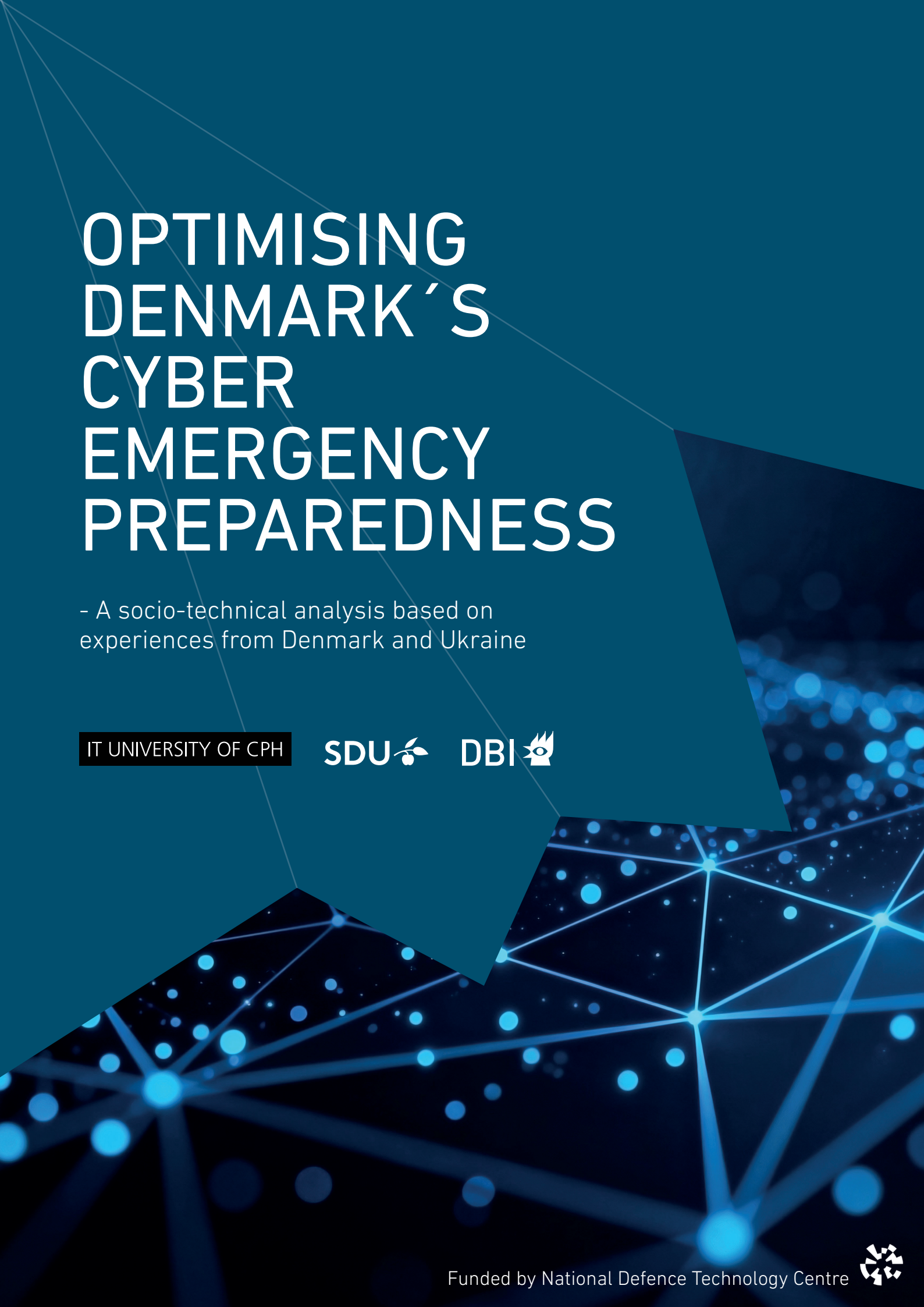
OPTIMISING DENMARK´S CYBER EMERGENCY PREPAREDNESS

- A socio-technical analysis based on experiences from Denmark and Ukraine

IT UNIVERSITY OF CPH
SDU
DBI



Funded by National Defence Technology Centre

AUTHORS

ITU: Oksana Kulyk, Yuliia Storm Larsen & Jari Kickbusch

SDU: Peter Mayer

DBI: Jorge Ivan Contreras-Cardeño & Vega Kirstine Tran

Funded by: The National Defence Technology Centre, NFC.

Layout: Line Auchenberg

Published by: Resilience Center Denmark

SPECIAL THANKS

Special thanks to the Danish and Ukrainian participants whose insights made this report possible, as well as to the relevant Danish and Ukrainian authorities for their valuable cooperation and support.

12/2025

What is the Resilience Center Denmark?

Resilience Center Denmark (RC-D) is a national collaboration between the Alexandra Institute, Bioneer, DBI, DFM, DHI, FORCE Technology, and the Danish Technological Institute. The center is supported by the Ministry of Higher Education and Research's performance contract funds with an annual grant during the period 2025-2028.

This publication is produced as part of the work of Resilience Center Denmark (RC-D), whose mission is to strengthen Denmark's technological capacity and societal preparedness. The report created by ITU, SDU, and DBI directly supports RC-D's goal of developing knowledge and technologies that enhance national resilience.

The findings contribute to RC-D's efforts to understand emerging cyber threats, assess vulnerabilities across critical sectors, and inform future strategies for strengthening Denmark's security and crisis response capabilities. The report thus forms an evidence-based foundation for RC-D's ongoing work to improve societal resilience in the 2025–2028 period.

CONTENT

EXECUTIVE SUMMARY

Denmark's digital infrastructure is among the most advanced globally, but this digital leadership also exposes the country to heightened cybersecurity risks. In light of increasing geopolitical tensions and the evolving nature of cyberwarfare, this report presents a socio-technical analysis of Denmark's cyber emergency preparedness, informed by qualitative interviews with stakeholders; 17 in Denmark and 12 in Ukraine. The participants represent private sectors (including healthcare, telecommunications, and transportation), government, and academia.

The study identifies experienced and potential harms in Denmark and Ukraine due to cyberattacks and outages of critical infrastructure services, including telecommunication, such as:

- **Physical Harms:** Cyber-attacks have led to real-world consequences, such as disruptions in critical infrastructure (e.g., energy, healthcare), which can endanger lives and public safety.
- **Disruption of Daily Activities:** Attacks have caused significant interruptions in public services, transportation, and communication systems, affecting both individuals and organisations.
- **Psychological Harms:** Victims of cyber-attacks, including employees and citizens, have reported stress and anxiety due to general uncertainty resulting from the attack and their inability to connect to their family or community.

Further, the report describes key threats, which pose significant risks to critical infrastructure, daily societal functions, and the well-being of citizens. These threats are categorised into eight major types, including:

- DDoS
- Social engineering
- Ransomware
- AI-facilitated attacks
- Supply chain compromises
- Physical access breaches
- Insider threats
- Hybrid threats.

The study highlights challenges in cybersecurity and describes:

- System complexity
- False positives
- IoT vulnerabilities
- Socio-technical issues like user behaviour and supplier dependencies.

The defence strategies which proved in practice most effective against the aforementioned threats while considering the prevalent challenges are multi-layered and follow zero-trust approaches. The aspects effective strategies need to cover range from preparedness, to technical hardening, incident response, as well as human and organisational factors.

The report concludes that Denmark's high level of digitalisation, while beneficial, significantly increases its exposure to cyber threats. The experiences of Ukraine underscore the real-world consequences of cyberwarfare and highlight the importance of proactive, multi-layered, and collaborative approaches to cybersecurity. Denmark must enhance its preparedness by integrating technical, organisational, and societal measures, ensuring resilience not only within individual organisations but across the entire national infrastructure.

Organisational Recommendations

- **Planning is essential:** Business continuity, disaster recovery, and emergency plans must involve the right people to avoid coordination failures and unnecessary costs.
- **Beyond technology:** Robust systems are foundational, but practice, evaluation, and third-party assessments are critical for preparedness.
- **Human factors matter:** Organisations should assess:
  - Crisis behaviour of their structure
  - Staff capabilities (e.g., technical, first aid)
  - Cultural differences
  - Sectoral and international interdependencies
  - Communication protocols and crisis agreements
- **Systemic thinking:** Adopt a holistic approach to infrastructure protection and decision-making, including revising procurement processes for critical tech services.

Recommendations for Future Research

1. **Sector Interdependencies:** Move beyond isolated sector studies (e.g., telecom) to analyse cross-sector and international dependencies for better societal resilience.
2. **Alternative Communication Channels:** Develop resilient telecom alternatives (e.g., Starlink), considering technical and social accessibility.
3. **Public Preparedness:** Create guidelines for citizens based on Ukraine's experience (e.g., backup SIMs, satellite phones, paper-based methods).
4. **Attack Simulations:** Design effective, context-specific simulations (e.g., as a part of red team exercise) that enhance security without harming trust or increasing vulnerability.

1 INTRODUCTION

As one of the most digitised societies in the world (United Nations, 2024), Denmark relies heavily on its telecommunications infrastructure to support critical societal functions, economic activity, and national security.

1 INTRODUCTION

As one of the most digitised societies in the world (United Nations, 2024), Denmark relies heavily on its telecommunications infrastructure to support critical societal functions, economic activity, and national security.

The Danish telecommunications sector is characterised by a high degree of digital maturity, with widespread broadband access, advanced mobile networks, and a population that is among the most digitally literate in the world. According to the European Commission's Digital Economy and Society Index (DESI) (European Commission, 2022), Denmark consistently ranks among the top EU countries in terms of digital performance. While this digital advancement brings numerous benefits, it also introduces complex cybersecurity challenges. The interconnected nature of telecommunications systems means that a successful cyberattack can have cascading effects, disrupting not only communication services but also critical sectors such as healthcare, finance, transportation, and energy.

According to the Danish Styrelsen for Samfundssikkerhed (SAMSIK) (Styrelsen for Samfundssikkerhed, 2025), the cyber threat landscape facing the telecommunications sector has intensified significantly. In March 2025, SAMSIK raised the cyber espionage threat level for the telecommunications sector from "medium" to" high", citing a surge in cyberattacks by foreign state actors, particularly from China, Russia, and Iran. These actors are targeting telecom infrastructure to access sensitive data such as communication patterns, location data, and user metadata. This information can be exploited for surveillance, intelligence gathering, and even preparation for physical or cyber sabotage.

In the assessment, cybercrime remains the most persistent and severe threat, with SAMSIK maintaining a "very high" threat level for ransomware and other financially motivated attacks. Organised criminal groups frequently target telecom operators to encrypt critical systems and demand ransom payments, causing widespread operational disruptions. These attacks not only threaten the financial stability of telecom companies but also jeopardise national security by potentially disabling emergency communication systems and critical infrastructure.

The threat from cyber activism has also been elevated to "high", particularly in the wake of geopolitical tensions such as Russia's invasion of Ukraine and the Danish government's support to Ukraine. Hacktivist groups may target telecom networks to amplify ideological messages or disrupt services as a form of protest. In addition, destructive cyberattacks, which aim to cripple systems rather than steal data, are assessed at a medium threat level. These attacks could paralyse telecom services, affecting everything from emergency response to economic operations.

In recent years, Denmark has experienced several high-profile cyber incidents that underscore the vulnerability of its infrastructure and the need for robust cybersecurity measures. In early 2023, Denmark's central bank and seven private banks, including Jyske Bank and Sydbank, were hit by Distributed Denial of Service (DDoS) attacks (Prakash, Schrøder, & Moltke, 2023). Later in 2023, Denmark was hit by its most extensive cyberattack to date, targeting the energy sector. According to a report by SektorCERT, a nonprofit cybersecurity center for critical sectors, hackers gained unauthorised access to the systems of 22 energy companies across the country (SektorCert, 2023).

In response to the geopolitical tensions and the escalating series of cyber and hybrid threats, particularly attributed to Russian state actors, Denmark has taken significant political and institutional steps to bolster its national security, including the establishment of the Ministry for Society Security and Emergency Preparedness and SAMSIK – the Danish Civil Protection Authority (Ministeriet for Samfundssikkerhed og Beredskab, 2025). SAMSIK has launched nationwide public awareness campaigns to

educate citizens about digital threats and crisis readiness, including the folder "Be Prepared for Crises", which encourages households to be self-sufficient for three days during a crisis, allowing authorities to focus on the most vulnerable (Danish Emergency Management Agency, kein Datum). In the folder, SAMSIK emphasises that Denmark's highly digitalised infrastructure while efficient is also vulnerable. Therefore, telecommunication is a key part of individual and household preparedness. At the same time, SAMSIK, recognises that in a crisis, access to digital communication may be disrupted. The recognition of both the importance and vulnerability of telecommunication leaves us with an open question:

How prepared is the Danish society, businesses, and citisens for outages of digital infrastructure and services, including telecommunication outages?

This technical report, Optimising Denmark's Cyber Emergency Preparedness, presents a comprehensive analysis of the cyber threat landscape, the harms these threats can inflict, and the countermeasures necessary to mitigate them. Drawing on insights from 29 in-depth interviews with stakeholders in Denmark and Ukraine, the report offers a nuanced understanding of the challenges and opportunities in strengthening Denmark's cyber emergency preparedness from a business, civil society, and citisen perspective.

The urgency of this work is underscored by the experiences of Ukraine, which has endured sustained and aggressive cyberattacks from Russian state and state-sponsored actors since 2014, with a marked increase in intensity following the full-scale invasion since 2022. These attacks have targeted critical infrastructure, disrupted essential services, and inflicted psychological and physical harm on civilians. By incorporating Ukrainian perspectives, this report not only highlights the real-world consequences of cyberwarfare but also provides valuable lessons for Denmark and other nations seeking to bolster their cyber defences.

2 METHODOLOGIES

We conducted a total of 29 interviews, 17 with Danish and 12 with Ukrainian stakeholders.

2 METHODOLOGIES

We conducted a total of 29 interviews, 17 with Danish and 12 with Ukrainian stakeholders.

The stakeholders included representatives of government and private sector, covering critical infrastructure with the focus on telecommunication, as well as individuals impacted by cyberattacks on critical infrastructure in their organisations or private lives.

Table 1 shows of our participants by country and sector. For the sake of confidentiality, we will not mention any identifying information about participants or the organisations they work for and will instead refer to them as "Danish participant" or "Ukrainian participant" when quoting them in describing our results.

Sector	Denmark	Ukraine	Total
Healthcare	5	3	8
Telecommunications	4	2	6
Individual/other private sector	1	6	6
Government	5	1	6
Transportation	1	-	1
Academia	1	-	1
Total	**17**	**12**	**29**

Table 1. Number of interviews by country and sector

3 RESULTS

We structure our results into four discussions: threats, harms these threats have caused or can potentially cause, countermeasures against the threats, and challenges in protection against the threats.

3 RESULTS

We structure our results into four discussions: threats, harms these threats have caused or can potentially cause, countermeasures against the threats, and challenges in prote

3.1 THREATS

In the following, we discuss the threat actors conducting cyberattacks, including cybersecurity threats related to the geopolitical situation, as well as attribution of these threats. We continue discussing the specific attack vectors that are considered relevant by our participants.

3.1.1 Threat actors

Our participants acknowledge the need to consider geopolitical threats when planning for cybersecurity readiness. The threat landscape is directly affected by geopolitical tensions, with Russia being the most frequently mentioned threat.

"As international cooperation becomes more destabilised, countries like Russia have greater incentives to target nations like Denmark." (Danish participant)

Other actors that were mentioned as a geopolitical threat in cyberspace were China, Iran, and, due to recent developments during the second Trump presidential term, the USA. Digital sovereignty was a recurring theme that was motivated by these (emerging) geo-political threats.

"We're closely monitoring statements from the US and what Trump is saying, especially regarding Greenland, where he hasn't excluded the use of military power. Due to these comments, we're evaluating how to approach the products we currently use." (Danish participant)

While the goals of some of threat actors might be data exfiltration and intellectual property theft, other attacks are more destructive in their goals, aiming to damage or destroy systems rather than access sensitive data. The motivation behind these threats might be destabilisation of society, disruption of critical infrastructure and influencing the political decisions in the targeted country.

"Right now, if Russia can change public opinion, that's perfect for them. If they can take down hospitals, power supply, or water supply, then people stop caring about the war because they care about their own welfare" (Danish participant)

"If the attackers aim to create fear, then you could look at what happened last year when Danmark's National bank was down. Jyske Bank went down as well and it lasted a few days. And looking at the articles about those attacks, I think you can say that these were successful attacks, because the goal was to create awareness. It caused us trouble, and it was insane amounts of data that were sent and some were handled, and others were unfortunately not." (Danish participant)

Among the Danish participants there were also concerns about to what extent, they were prepared to defend themselves, especially if the attacks should intensify.

"The threat is constantly lurking out there. It is no longer a question of whether we will be hit by an attack. It's a question of when we'll get attacked. That is also why the threat level against Denmark has never been higher. We are pushed to the forefront now." (Danish participant)

"I am worried that the first thing an enemy would do is to attack our communication channels either physically or virtually. And I don't want to think about a scenario where people cannot use their mobile phones and all kinds of other communication devices. It will be a state of panic. Just remember when Mette Frederiksen said no need to stock toilet paper. Everybody went out to buy toilet paper." (Danish participant)

Threat actors will also conduct attacks in several stages, with the attacker gaining initial access and establishing persistence, and then either staying in the network to conduct further reconnaissance and prepare for the next stage or remaining dormant until there is time for acting upon the intended objectives.

"...it is perhaps a model that we also see from China. It is that they want to place themselves on the network in a way so that in an escalating situation, they can basically go in and shut down our network." (Danish participant)

Correspondingly, our participants mentioned specific cyberattacks conducted by foreign state actors, either experienced by their organisations or themselves in their private lives. These attacks were attributed either to a specific country (based, e.g., on the IP addresses observed in the attack) or specific attacker group, such as NoName057 or Sandworm.

"We have threat intelligence also here. So, seeing where it comes, the threat. Also, we find the Russian IP addresses." (Ukrainian participant)

"Russian activist groups like NoName057 might claim that they did it, but it's hard to know. We see those statements, where they take responsibility for this and that attack, whether they have actually done it. My immediate guess would be that yes, they probably have." (Danish participant)

3.1.2 Attack vectors

Some of the attack vectors discussed in this section are clearly associated with attacks conducted by foreign state actors. Others, while at times used by foreign state actors as well, are not always clearly attributed, and therefore represent a general cybersecurity challenge to organisations.

3.1.2.1 (d)dos attacks

Denial of service attacks were mentioned as a very common on-going attack vector.

"It's a DDos attack. It happens often that our ordinary website is under attack, I think most Danish authorities and larger companies' websites are. Those attacks are considered to be pretty standard attacks. " (Danish participant)

Even if most of the attacks generally did not have a critical impact, and were referred to our participants as "annoying" or "easy to mitigate", they could nonetheless cause disruption in the organisation's operations:

"So DDos is a relatively simple attack technique, but it is not always simple to mitigate, because the amount of data that we're attacked with per second, can be equal of the amount of data from a medium-sized Danish city and the data has to go somewhere. You can't get it to dissolve itself. That's why it's essential to have control over the black hole so that you can channel the data into that. So this is manageable." (Danish participant)

"The last notable incidents were DoS attacks where attackers used new techniques to flood our routers, preventing external connections. We had about 30 minutes of disruption before resolving the issue." (Danish participant)

3.1.2.2 Social engineering attacks

Attacks aimed at exploiting the human factor, such as phishing, were furthermore mentioned as a common attack vector, and the one with a potential to cause significant impact. In particular, phishing emails or other kinds of similar attacks such as vishing (voice phishing) were used by attackers as a way to get initial access to the systems.

"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." (Ukrainian participant)

In addition to social engineering attacks used for getting access into the target's IT systems, social engineering is furthermore used on a broader scale, by changing people's minds and behaviour via disinformation campaigns.

"Our weakest point is the people, because we get attacked with information. Right now, the biggest problem is misinformation attacks." (Ukrainian participant)

3.1.2.3 Ransomware attacks

Ransomware, that is, software which encrypt one's data and demands a ransom for decrypting it, has the potential of causing significant damage. Our participants mentioned reports from other countries such as the UK, but also incidents in Denmark that involved critical infrastructure being targeted by ransomware:

"Yes, there was a ransomware incident where one of our doctors was using network drives. The ransomware not only encrypted local files but also mapped network drives, including a connection to two Asure servers containing blood analysis results. The recent blood test data was encrypted." (Danish participant)

Also, participants from businesses that are not directly a part of the critical infrastructure, mentioned experiences with ransomware attacks.

"It was blackmailing. All the files were encrypted, and we could only open one file consisting of a picture and two Protonmail addresses. I remember this like it was yesterday. We were sitting in a meeting; I sat in front of the top management. And there were these two addresses and at the time we didn't know if we could recreate and if they had been into our backup. We had no idea, and we risked that we couldn't recreate anything. Our management told me to write to these addresses and I refused. I had a lot of servers that didn't work. I had a huge amount of PC's that did not work, and they wanted me to write to these criminals. Seriously, I'm not doing that, I said … It turned out they didn't encrypt our backup. Thank god, because if they had, then I usually say there would have been 3 options. First option would be to restore, but they had our data so that was not a real option. In the second option we could pay and in the third one we could go bankrupt … We were super lucky with the ransomware version that we got. They did not steal our data. Today, they steal your data first, quietly. They slowly get the data out of your system and then they encrypt it." (Danish participant)

As ransomware is specialised software that has to be delivered and activated on the target's system, some of our participants argued that it requires "more sophisticated equipment" and "considerable skill" from the attackers. Others mentioned the necessary tooling being easily accessible on the darknet:

"The cybersecurity network on the darknet is quite advanced. With about $2,000-$3,000, you can buy a ransomware attack software complete with 24/7 support." (Danish participant)

3.1.2.4 AI-facilitated attacks

The use of AI in cyberattacks was mentioned as an emerging attack vector, and the one that has a potential to become even more prevalent and dangerous in the future due to rapid developments in AI technologies.

"AI is evolving extremely rapidly, making it challenging for anyone to keep pace. Artificial intelligence represents one of our biggest security concerns, so we're focusing on understanding what's possible and developing strategies to block, mitigate, or prevent malicious AI applications." (Danish participant)

AI was mentioned as a way of facilitating social engineering attacks, such as generating convincing phishing emails or deepfake videos. Furthermore, the prevalent use of AI systems that are developed by non-trustworthy actors can present risks due to sensitive data being shared with these systems:

"...the second someone starts putting data into [Chinese-developed AI systems], it all goes to the Chinese. The AI race right now is quite scary because you have no clue what's going to happen and what data they steal. People don't think before they put data into AI just because they think they're using something friendly - but they're not." (Danish participant)

3.1.2.5 Supply chain compromise

Targeting the supply chain has been mentioned as an effective method for infiltrating the target's system, in case the target itself is well-protected, but their trusted suppliers are not.

"When they didn't find how to penetrate our perimeter, they tried to use our third-party suppliers, through them to penetrate to our environment." (Ukrainian participant)

Such attacks can be challenging to avoid, since they require trusting third parties not only regarding their intent, but also regarding their security perimeter and ability to withstand attacks that can be used for accessing other supply chain components.

"It's not because the companies are doing a bad job. It's about the fact that we have supply chains for all technology. And in Denmark, we are not particular punctual with upgrades, with taking security seriously, with updating passwords and so on. So, we have a lot of open flanks in our critical infrastructure." (Danish participant)

3.1.2.6 Physical access

Obtaining physical access to the target's system components can be used as a stepping stone for further infiltration, if the attacker can use the access to reach parts of the system that are closed to the outside.

"My biggest concern is physical security. If someone can bypass 80% of our defences simply by connecting to our network inside the building, that's a serious problem." (Danish participant)

Gaining access to the facility can also be seen as an act of social engineering – gaining enough trust to infiltrate the facility and make people comfortable enough so they will share all their secrets. Because co-workers need to collaborate and help each other in order for organisations to work, attackers can exploit this trust among members in an organisation.

In more extreme cases, the attacker can take over full control over the physical facilities of the target. Such access has been used in attacks by Russia on Ukrainian infrastructure, as the Russians were able to take over the infrastructure on occupied territories and use it for attacks on the Ukrainian parts:

"...they took some territory of Ukraine [...] there are our base stations, through them, they try to penetrate our environment." (Ukrainian participant)

Such use of captured facilities can furthermore be used to compensate for own lack or scarcity of resources, or as a way to save up own resources by using the facilities of their enemies, e.g. In using Ukrainian facilities against Ukraine.

3.1.2.7 Insider threat

Use of insider access has been mentioned as a way to get privileged access into the systems, which can be especially dangerous if the organisation prioritised security measures protecting against external attacks, but did not focus on considering the use of valid internal accounts for attacks. Such insider threats can be used by state actors, e.g., by using state authorities to convince nationals of these countries working abroad to collaborate with their home country.

"...even if you have lived, for example, in Denmark and worked here for, let's say, the last 20 years, you are still obliged to support the Russian state if they call you, as long as you are a Russian citizen. And they do that sometimes, and they contact people and say, well, we need you to help us. And if you refuse, it can have consequences both in relation to if you at some point travel back to Russia and have to visit family, then you can simply be arrested, or it can have consequences for your family in Russia" (Danish participant)

Such attempts to recruit insiders are not limited to foreign nationals, though. State actors or other interested parties might reach out to organisation members to convince or bribe the person into collaborating with the attacker.

"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." (Ukrainian participant)

In extreme cases, if bribery or other persuasion techniques fail, intimidation can be used to force insiders to collaborate, e.g. using private data (gained e.g. through previous data breaches)

"After some time, [people from Russia trying to recruit collaborators in Ukraine] wrote to me from an anonymous account in a private Telegram message. They asked if we had changed our mind about cooperation. We immediately refused. And they sent me a large amount of my personal data, screenshots. They sent me a scan of my passport, taxpayer code, and information from the register about my place of residence. A few of my phone numbers and emails. And once again they asked if I had changed my mind.". (Ukrainian participant)

3.1.2.8 Hybrid threat

Organisations can be affected by cyberattacks that are not directly targeted on the IT systems of the target, but on the underlying infrastructure that ensures the target's operations. For example, attackers can disable digital operations of many organisations by damaging connection cables, which has a potential to cause significant damage in Denmark and has, according to our participants, already been attempted by malicious actors.

"In principle, they are not really doing anything illegal. [...] They sail around with their many antennas, we don't know if they are in the process of planting something so that [...] one day, they can press a button and take out all the submarine cables, let's say for all telecom companies in Denmark. [...] That would hurt." (Danish participant)

Beside the submarine cables, some of the participants also raised concerns about attacks on the mobile masts.

"It is clear that they are vulnerable. Our mobile masts are a part of the infrastructure, and they are out there on the countryside. So, it's clear that there we place ourselves in the first trench" (Danish participant)

Similarly, attacks on other critical sectors (e.g. energy) can be used to disrupt the organisation's operations, even if the systems belonging to the organisation itself are not attacked directly.

"And if the power goes out, if we have a situation like the one we saw in Spain, well then the telecommunication network goes too, because it runs on electricity. (Danish participant)

3.2 HARMS

We discuss the harms that can be caused by malfunctioning or failure of digital systems. While we focus on harms, actual or potential, that result from cyberattacks, our participants also provided examples of harms that were a result of an accidental failure, or a kinetic attack that impacted IT infrastructure. Most importantly, this included the total or partial collapse of digital infrastructure or the functioning of parts of the society that is sustained by the digital infrastructure. In the remainder of this section, we focus on concrete harms.

3.2.1 Physical harms

The impact of some cyberattacks can include physical harms, causing damage to someone's physical health or – in the most extreme of cases – loss of life. These cyberattacks usually involve disrupting critical infrastructure, so that, e.g., hospitals can no longer provide healthcare to people in need.

"The worst outcome [of a cyberattack on a hospital] is definitely loss of patient life. While data leaks of personal information are serious, the worst-case scenario is having a patient on an operating table when something goes wrong with the digital systems, potentially causing loss of life." (Danish participant)

Aside from attacks on healthcare infrastructure, physical harms can be caused by attacks on telecommunication sector, if it results in people being unable to get in touch with critical services in emergency situations.

"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." (Ukrainian participant)

In case of people requiring transportation to a medical facility (e.g. for access to equipment or specialists not available in their present location, or their present location not being safe enough), transportation sector outages can furthermore cause health issues.

"The latest massive disruption happened in June. It affected the Ukrainian railways for several weeks, I think for two or three weeks. We couldn't buy any railway tickets and for some families it was definitely a critical issue because some of them had planned medical operations in the western part of Ukraine, in the relatively safer area." (Ukrainian participant)

3.2.2 Disruption of daily activities

Cyberattacks that prevent access to digital systems, either targeting telecommunications or energy infrastructure, lead to inability of perform ordinary tasks such as buying groceries, withdrawing cash from ATMs or performing their job duties.

"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" (Ukrainian participant)

Such disruptions are more prominent, the more digitalised society is. In particular, Ukraine has been affected by cyberattacks on their IT infrastructure, due their recent developments in digitalisation.

"Since 2019, and even some time before, Ukraine has been very proactive in introducing digital tools and digital alternatives for obtaining social services, for obtaining sealed documentation for confirmation of marriages, birth status, death certificates or for applying for compensation. And the Internet disruptions make all these services unavailable for people residing in frontline communities. And we are talking about thousands of people, residents of Ukraine, who live in such dire conditions." (Ukrainian participant)

Many businesses rely completely on telecommunication and on having access to their digital systems. Hence, the consequences are harsh and mitigation difficult, when a cyberattack blocks all access to all digital services.

"You couldn't communicate with anyone. [...] When I arrived to the head quarter very early that morning, people were already pulling out cables in the server room and we put up some whiteboards at the entrance saying, "don't turn on your computer". But of course, that whiteboard couldn't be seen by the employees in Japan or in the US. We simply couldn't communicate with them. [...] Obviously, it costed us a lot of money, like a lot of money." (Danish participant)

Similarly, other countries that rely on digital services would be at risk of such disruptions.

"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. All these things that most people are affected by, those will be the problem" (Danish participant)

Lack of access to digital documentation and services can also be a particularly critical problem for vulnerable populations, e.g., refugees or other people in need of state services such as social welfare. The issue becomes more prominent in highly digitalised states, where paper-based documentation and services are not widely used or may not be available at all. In Ukraine, such problems affected people from frontline areas trying to file requests for compensation for damage to their property, as they could not submit their application due to network outages.

"Internet interruptions affect directly. For example, people can lose their documents in the course of war. I can tell you about families who tried to apply for a state-run program, which is funded by the World Bank for compensation for damaged and destroyed property [but for that] they have to go online. [...] In frontline areas, people often do not have the opportunity to submit compensation claims using a mobile application." (Ukrainian participant)

Similarly, timely access to digital services can be of critical importance for people with special needs, e.g., people in war zone in need of evacuation. Lack of access to this information (e.g., evacuation announcements) in most extreme cases can be a life and death matter.

"Unfortunately, it goes in the direction of more and more territories getting occupied and the families there sometimes do not have access to Internet and when they do not have access to information, they could miss the announcement of mandatory evacuation of families with kids or mandatory evacuation of all the residents. This type of information can be vital. It's a question of life and death basically." (Ukrainian participant)

3.2.3 Psychological harms

The danger of physical harms and disruption of daily activities can have a mental toll on the affected people, especially in presence of uncertainty caused by a crisis situation. Similarly, lack of possibility of getting in touch with one's family (especially if they are known to be at risk, e.g. being in a frontline area) or in general, to other people who might be able to provide practical as well as emotional support can have a toll on people's ability to withstand the crisis.

"In the time of war, you really want to stay connected with your family and with your friends, because 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." (Ukrainian participant)

3.3 COUNTERMEASURES

3.3.1 Being aware of potential threats

Having preparations for possible threats, including preparations for incident response and recovery plans, is a significant part of being able to respond to these threats.

3.3.1.1 Asset management and risk assessment

The preparations start with being aware of important assets within the organisation. Their security protection status is crucial in understanding which security protection measures need to be applied. Understanding assets can then help in conducting risk assessments and anticipating potential attacks.

"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." (Ukrainian participant)

3.3.1.2 Threat intelligence

For better preparedness for cyberattacks, cyber threat intelligence information can be of great importance, allowing to anticipate specific upcoming threats. Such information can include data from other incidents, vendor reports on attacks and vulnerabilities, or general reports on current threat landscape. Communication and knowledge sharing between companies, government and other organisations in possession of relevant information is crucial, especially given that threat actors often use the same tactics to attack different targets

"We have to inform [the government] if you have cyber incidents with providing the details like CERT-UA or Security Service of Ukraine. So, we have to provide it and share this information with them. Also, they are sharing with us [..] So, we are immediately paying attention with that." (Ukrainian participant)

Some of the Danish participants requested better and more detailed sharing of intelligence and more collaboration between the telecom sector and the government institutions.

"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. [...] We can't just base our defenses on a report that comes from [SAMSIK]." (Danish participant)

3.3.1.3 Supplier screening

Being proactive and prepared for incidents and emergencies includes paying attention to suppliers, especially considering supply chain compromise attacks (see Supply chain compromise). Supplier screening can include taking factors such as supplier's level of cybersecurity preparedness, but also their origin or known affiliations, into decision making processes, e.g., by avoiding products of certain countries or vendors.

"We're very cautious about what software is being used, what systems, and which suppliers. It's no secret that we're skeptical of anything Russian or Chinese-related due to the geopolitical atmosphere and our own experiences. [...] We're also considering blocking access to emerging AI tools like what Musk is developing with "X AI." (Danish participant)

Communications with suppliers might also need to involve negotiations on security controls to ensure that the suppliers ensure the proper level of security of their products and services. Such controls might include requirements towards specific certifications, or towards providing monitoring opportunities, e.g., by requiring a supplier to set up EDR (endpoint detection and response) systems on the components they control, or to inform the organisation receiving their products or services about cyberattacks in their environment.

"With the critical customers, we talk at the beginning. Of course, you need to be prepared because you are providing us with services. So, for example, you need to review your assets. You need to check your infrastructure. Prepare, providing cybersecurity awareness to your employees. Have to have at least an EDR solution on the laptops because you need to manage the malware or, let's say, unauthorised access to the files." (Ukrainian participant)

Furthermore, ongoing relationships with the suppliers need to include the option of further close communications with suppliers and monitoring of supplier infrastructure, e.g., to detect compromise and alert the supplier or take other measures.

"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." (Ukrainian participant)

3.3.2 Hardening the system via preventive and detective technical measures

Implementing technical security measures within the system is critical for preventing and detecting cyberattacks.

3.3.2.1 Limiting access

One of the foundational building blocks of cybersecurity protection is ensuring well-designed and well-implemented access control policies and other policies limiting access to assets to people/devices/system components depending on who needs and has the right to this access. Such policies can include both technical controls (e.g., authentication mechanisms, including multi-factor authentication for important accounts) and organisational measures (e.g., data protection agreements outlining policies regarding access to personal data).

"To mitigate [unauthorised access], we employ multi-factor authentication for important services, requiring more than just passwords - something you have, like a phone, or something you are, like a fingerprint. This makes it much harder for attackers who only have password information." (Danish participant)

In particular zero-trust approaches, i.e., treating each access request as potentially malicious, and defend forward approaches, i.e., actively disrupting malicious cyber activity in foreign networks, have proven themselves to be highly effective. Implementing a zero-trust architecture is thereby possible for most companies of all sizes. Defend forward requires dedicated staff that might make it resource-wise infeasible for SMEs.

Having appropriate access control policies, e.g., through zero-trust approaches, furthermore can be used to protect against insider attacks. These approaches also rely on the least privilege principle, ensuring that users or system components only have access to the resources they need. Such principles can also be implemented via network segmentation, ensuring controls over communications between different system components, through blocking the possibility of making modifications to critical parts of the systems that are not expected to be modified as a part of usual operations, or through allowing the use of highly privileged accounts (e.g., administrator accounts) from a secure perimeter only and for administrative tasks only.

"We're implementing privileged access management (PAM) to ensure the right people have the right access to the right programs – and nothing more. This involves considerable manual work to verify that each individual has access only to the systems and documents necessary for their daily work." (Danish participant)

Preventing unauthorised access to data can furthermore involve encryption mechanisms, particularly when the data is considered sensitive. A defence-in-depth approach with multiple complementary layers is thereby the preferred way.

"We have standard procedures and optimisations to ensure sensitive personal data like CPR numbers remain secure. [..] All data is encrypted, and multiple security layers exist to prevent unauthorised access." (Danish participant)

Limiting access to data over network can be furthermore done by storing important data only on local storage, in case this data does not need to be exposed or shared with anyone outside of the organisation.

3.3.2.2 Automation and monitoring

Automation can be used to detect and prevent cyberattacks or security vulnerabilities. One way of doing so is the use of blocklists and filters to prevent malicious actors from accessing the system. Such blocking can be implemented as email filters preventing malicious emails from reaching the users, or geo-blocking, preventing access from countries that are high-risk of being involved in cyberattacks.

"We have an internal list of IP addresses from countries we block from accessing our systems. While this isn't foolproof given how IP addresses, VPNs, and traffic disguising work, it helps clean up automated attacks from "script kiddies" who use readily available tools. Just by implementing geo-blocking, we reduced network-based attacks from these countries by approximately 70%." (Danish participant)

Automation can furthermore be used for data flow monitoring, ensuring that possible exfiltration of sensitive data by malicious actors is detected and prevented in time, endpoint/extended detection and response systems (EDR/XDR) collecting and analysing system logs and behaviour, or by monitoring and checking data uploaded to the organisation's cloud. For developing software, automation can be used for checking the source code of the software for vulnerabilities before it is being deployed. The role of AI furthermore both increases the need for automation and provides further opportunities to make automation more effective.

"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." (Danish participant)

Monitoring of systems, including sufficient log keeping, is an essential part of effective automation. Such monitoring can furthermore include anomaly detection to detect e.g. logins or other kinds of accesses from unusual device or location, or checking for unexpected modifications or modification attempts, especially to critical parts of the system. Such monitoring can either be used to act upon suspicious activity immediately, or for investigating a cyberattack after the fact.

"We have monitoring on all our systems to observe whether something suspicious is happening on machines and servers. Based on that, we determine the best solution or response to a given situation." (Danish participant)

3.3.2.3 Certifications, vulnerability management, and updates

Certification processes were highlighted by several participants as a cornerstone of well-founded security architectures for companies. Specifically, in Ukraine companies are guaranteed certain preferential treatments if they obtain government certification. As part of this certification process organisations are supported in improving their security posture over time.

"So we check the quality and the content of the protection plan for cyber-attack. We approve it and then we [...] monitor how they implement what they are planning in those protection plans." (Ukrainian participant)

This support is taken further than monitoring though, where there are efforts to create a security support community that can lend expertise in situations where organisations are trying to kick-start cybersecurity efforts, e.g., during hiring procedures:

"We are establishing a Chief Information Security Officer (CISO) campus intended to function as a dedicated development and training platform, systematically facilitating the identification, selection, hiring, and comprehensive onboarding of top candidates, while simultaneously providing continuous professional growth through essential re-skilling and up-skilling programs, and community to sustain the collective's knowledge base via the active sharing of best practices." (Ukrainian participant)

Making sure that the system is not vulnerable to known attacks requires being informed about newly discovered vulnerabilities and applying patches as soon as possible. If updating a legacy system is not feasible (e.g. because it reached its end-of-life stage and is no longer supported by its provider), phasing such systems out and replacing them with up-to-date alternatives might be needed. If such replacement is furthermore infeasible due to budget restrictions or other issues, other measures such as making sure that these systems are isolated from potentially untrusted environments might be needed.

"We have plans to either update vulnerable systems or phase them out with newer equipment. This requires convincing directors and budget managers that we need to replace legacy systems, which can be expensive. When funding isn't available, we use alternative approaches like isolating vulnerable systems so they can continue functioning securely while still treating patients." (Danish participant)

3.3.2.4 Economic security model

While preventing an attacker from attempting to break into the system might be infeasible, the economic security model approach would focus on making a possible attack as costly for the attacker as possible. Such an approach can therefore act as a deterrent to an attacker.

"Adding complexity through multiple security layers discourages attackers by making their efforts too difficult or expensive to pursue. [..] Nothing is 100% secure, but the goal is making systems secure enough that breaching them becomes too expensive or infeasible for attackers." (Danish participant)

3.3.3 Ensuring timely incident response and recovery

In addition to security measures aimed at prevention and detection of attacks, proactively planning for mitigation of potential issues requires anticipating that breaches and other incidents might occur, so that procedures need to be in place to recover from them.

3.3.3.1 Emergency management

Emergency planning includes incidence response procedures and business continuity plans for cyberattacks in organisations. To be effective, such procedures must include plans for the detection of threats, reporting channels available and known to all relevant stakeholders, technical measures such as isolation of compromised system components, coordination between the people and organisational units responsible for incident response and recovery, including both technical and non-technical (e.g. communication) personnel. Furthermore, while timely recovery is often a priority in incident response, especially with critical infrastructure services, understanding the attack and the way it happened is also of importance. In this way, the organisation can have a better understanding on how to protect itself against second attempts, especially if such attempts come shortly after the affected systems are restored but not yet sufficiently hardened with regards to security, or if the backups used to restore data have been compromised as well. Incident response plans should therefore include measures to analyse the attack and understand the attacker's tactics. Such plans furthermore need to be tested prior to the incident, ensuring that they work as intended.

"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." (Danish participant)

One way to conduct these tests is through attack simulations and other red team exercises, which might focus both on technical (e.g., vulnerability testing of IT systems) and non-technical (e.g., simulating phishing attacks) aspects of security. The simulations can therefore ensure that everyone is aware of their role in incident response and can therefore fulfil this role efficiently in case an incident happens. Simulations, furthermore, can reveal vulnerabilities and further gaps in defence or planning, including faults in the infrastructure involved in recovery (e.g., errors within backups), which can then be addressed. To be most effective, these simulations furthermore need to be adjusted towards specific threats that the organisation is facing, e.g. focusing on protecting availability if the organisation is known to face a threat actor whose goal is to damage their infrastructure.

In addition to response/recovery plans within the organisation, in case of large-scale attacks on critical infrastructure, country-wide plans are needed to ensure the functioning of critical services in case of critical infrastructure outages.

"When you have worked with emergency response for quite a few years, you get to understand some very basic things. One of those things is that it takes some serious consequences, for people to take action. For example, it is hard to get people to expand their insurance policy to cover something that they have not been exposed to. It's simply because you don't recognise the risk. You haven't practiced and trained it. That's the reason why I always start with exercises when I work with companies. It's "don't tell it, show it". They need to realise how serious things can get, because that increases their appetite. And to my knowledge we never practiced something like a big telecommunication breakdown in Denmark." (Danish participant)

Such plans involve coordination between different stakeholders, including government authorities, emergency services, industry, and the general public. The plans for this coordination should furthermore account for a variety of challenges related to the impact of a cyber-incident, such as ensuring that coordination is possible even if telecommunications are disrupted because of the incident. Correspondingly, simulations and other kinds of exercises across different institutions and sectors might be helpful in evaluating the level of preparedness in such coordination.

"[It is important] that the emergency services can communicate, our military's preparedness. That the police and the ambulances can talk to each other. This kind of communication should have first priority. Next step should be to ensure that the population can make emergency calls and get some information" (Danish participant)

Prioritisation of critical services can furthermore result from some activities being restricted, as long as they are deemed to be less essential.

"Specifically, it's possible to segment internet traffic so that the most critical data gets through. So during an attack, some people might not be able to watch Netflix because streaming traffic is deprioritised, while critical societal functions are prioritised." (Danish participant)

The general population should furthermore be informed about their options to deal with a potential crisis that results from a successful cyberattack, as well as providing advice on how one can be prepared for such a crisis.

"It is a really good idea to inform people about where they can go if electricity disappears, if the phone doesn't work or if there's no Wi-Fi. We can only support working on such solutions locally, but it could also be supported by the ministry." (Danish participant)

For example, locations across the country can be set up that provide the basic needs such as shelter and warmth, but also electricity and internet connection, allowing people to charge their devices, communicate, or use public services. Such locations, called the "points of invincibility", have been set up across Ukraine since the full-scale invasion and have been used by people in case of energy blackouts or telecommunication outages.

Communication towards the population, however, should consider the different levels of access to communication services. People in areas with low level of digitalisation would need to be reached via alternative means. Same considerations hold for people in areas affected by telecommunication outages, so that they do not need to access the affected resources to be informed.

"For example, people in some villages and settlements cannot access the information, which is published on government online resources. The only way for them to get the information is through volunteers and sometimes through the military." (Ukrainian participant)

Emergency preparations should furthermore be adaptable for unexpected situations. While thorough emergency planning is critical for preparedness for certain risks, there always remains a possibility of unpredicted risks, "unknown unknowns". Such risks are even more probable in times of instability, such as during an on-going war or other kind of crisis. Emergency plans and involved systems should therefore be designed to be sufficiently flexible to adapt to these uncertainties in case they occur. This might involve adapting the legislation, e.g., allowing to switch to paper-based communication or store sensitive data outside of the country.

3.3.3.2 Redundancy

One important aspect of emergency management is ensuring the availability of critical services despite their outages, which can result either due to cyberattacks directly, outages in related sectors such as energy or isolation of compromised systems as a part of incident response procedures to prevent further impact. Such availability can be achieved with redundancy, that is, having alternative mechanisms in place that can be used to replace the compromised system components when needed. A related concept is also defence-in-depth, an approach to cybersecurity that focuses on implementing multiple defences that the attacker needs to break through to achieve their target.

"Our approach involves building barriers and robustness, creating multiple defensive layers. If attackers breach one layer, we have several more protecting our systems. This multilayered strategy is fundamental to our security posture." (Danish participant)

An important redundancy mechanism is the use of backups, redundant data centres and other redundant infrastructure, ensuring recovery after data loss. The setup of this infrastructure furthermore needs to be designed to support appropriate speed of restoration, especially in case of an incident affecting large amounts of data or many parts of the system, and therefore, needing extensive restoration procedures. In times of conflict and war, the safety of the disaster recovery site where this infrastructure is physically stored becomes a critical issue, so that the physical location might need to be outside of high-risk areas.

"...in different [..] regions are our data centres. [..] So if they, for example, one of those things went down or destroyed, the second one will work. So it shouldn't be impacted and we tested it, it shouldn't be any impact." (Ukrainian participant)

"[Since the full-scale invasion] the Ukrainian authorities tried to preserve the servers [with state registers] and they moved many of them to the West of Ukraine. They remained in Ukraine, in territory of Ukraine, but Kyiv was at risk of occupation and at that time all the state registers, including civil registry, including state property registry, including registry of movable property like cars and vehicles and some other registers, they were not operative at all due to the obvious reasons. The administrators were trying to rescue the information and the servers, because of the risk that Kyiv should get occupied. It proved to be efficient, an efficient tool and an efficient way of storing such information because you do not have to deal with massive archives in paper and so on. You just need to rescue a server, which is much easier." (Ukrainian participant)

In addition to physical separation of disaster recovery sites, it is important to ensure their separation in other aspects, e.g., organisational structure, so that a cyberattack on one recovery site will not succeed in spreading to others. For instance, a separation of roles with privileged access to the data in the recovery sites provides hardening against the compromise of any one privileged account.

When it comes to telecommunication outages specifically, alternative telecommunication channels are essential not only to ensure the appropriate incident response, but also to support people and organisations affected by the outage so that they are not blocked from use of critical services and other daily functions (see also Harms). Such channels can be provided by the government or other centralised entities, e.g. by establishing alternative communication networks such as SINE, which can be used by selected authorities in crisis situations. The usage of these networks can be restricted to the use of emergency services only, so that their capacity is not overloaded; while such restrictions can still lead to some.

"Today everyone is very dependent on internet and their mobile phones - not least to communicate with the authorities and to receive news - so how do you handle that? Should it be up citizens to make sure they can cope without communication, not least, to and from the authorities – cope without internet and mobile phone connection? - or should we try to provide more robustness, maybe some requirements for certain types

of roaming or for battery backup on mobile masts and internet connection points? Should there be certain known and prepared locations where citizens can go to and obtain communication with authorities – obtain connectivity to internet and with mobile phones?" (Danish participant)

Commercial solutions such as Starlink can furthermore be used as a replacement for telecommunication infrastructure. Starlink has been widely used in Ukraine since the full-scale invasion, both for military communication and by civilians in areas where the communication infrastructure has been damaged or otherwise made unreliable.

"We have the opportunity to make satellite solutions and things like that if need be. That is, if a cable to an island get cut, we can set up such a connection to them. But it's clear that if you say that the entire country is affected then we cannot just switch to satellite solution. We can't. A scenario like that, I have to say that I hope that'll never happen, because Denmark would be in really bad situation." (Danish participant)

"We haven't considered something like Starlink yet. I don't think we are a part of the critical infrastructure and perhaps that's why we haven't considered this. We trust the critical infrastructure." (Danish participant)

While Starlink has an advantage in relatively low costs compared to other solutions and convenience, it is a US company with a CEO who is outspoken on geopolitical matters. This fact can influence the trustworthiness of Starlink, especially if it is used for critical communication (see also Geopolitical Threats and Supply Chain Compromise). There is therefore a need to consider EU-based alternatives, however, these alternatives are at the moment less affordable and offer lower performance.

"I just got an offer for an OneWeb satellite transceivers, and I have to subscribe for a year, so to get that up and running would cost me around 100.000 for a year. Now with Starlink that would be below 10.000." (Danish participant)

Other alternatives to telecommunication can include, e.g., portable radio stations that can be used in emergency situations.

"I bought an analogue radio station, a small, portable one [...] If it happens that there will be no connection in the country, I know where my radio set is, and my mom knows where hers is, and we will always find a connection" (Ukrainian participant)

In case the outage of telecommunications affects only one provider, with other providers still operating, individuals can protect themselves by getting a second SIM card from one of the available providers. Getting a SIM card while the incident is on-going can, however, be challenging due to sudden influx of demand resulting, e.g., in long waiting times or restrictions on behalf of the alternative providers who are not ready for a large intake of new customers. Having such a card ready in advance is, therefore, a preparedness strategy that Ukrainians use.

Similarly, organisations, especially those providing critical services such as healthcare, can ensure redundancy by having multiple communication channels available. Such redundancy can include, for example, contracting several telecommunication providers for ensuring the organisation's needs, so that an outage of one of them does not cause a disruption to the organisations' operations.

Since telecommunications are furthermore dependent on energy supply, and therefore, would be affected in case of energy outage (due to a cyberattack or a kinetic incident) preparedness measures should furthermore ensure that one is able to provide (e.g. as ISP) as well as to receive (as an individual or organisation) network connection in absence of electricity. This can be ensured, for example, by having power generators and power banks available.

"So, also, it's important that the Internet providers have equipment, which would be able to ensure continuation internet services for some period of power outage, like for three or four hours. In Kyiv, for example, there are providers, which can do it for 12 up to 24 hours and this has been a game changer. [...] I would also say that as a citizen, it's crucial to have a power bank and a wire, which can link the power bank to your Wi-Fi router, so that if your internet provider can provide internet connection during a power outage, you are secured. At least until your power bank runs out." (Ukrainian participant)

3.3.4 Considering human/organisational relationships

Dealing with cybersecurity incidents involves not only technical preparations, but also the involvement of human and socio-technical factors, including relationships between individuals and organisations.

3.3.4.1 Collaboration

Due to the interconnected nature of digital technologies and infrastructure supporting them, collaboration is essential to ensure cybersecurity protection, as well as detection and response to cyberattacks. Such collaboration includes working with suppliers (see also Supplier Screening), government, international partners and organisations such as ENISA, security vendors and other organisations that had experience with similar cyberattacks and thus might have further insights on how to protect against these attacks or respond to them (see also Threat Intelligence). In absence of such experience and knowledge sharing, organisations risk reinventing their own protection methods that might be less effective than practices that build upon experiences of others. While such collaboration can emerge, e.g., from informal networks and contacts between the organisations, it can also be facilitated by the government to provide a better reach, including involvement of organisations across different sectors.

"In Denmark, we have [SAMSIK] that works with all regions across Denmark - Copenhagen, Jutland, and others. Their job is to coordinate information about attacks, intrusions, or any potential dangers to the regions. They operate what we call Security Operation Centers and Analysis Centers implemented specifically for the regions." (Danish participant)

Further, some of the participants missed a stronger collaboration between the Danish telecom industry and the government, for example in order to protect the submarine cables.

"Together with other stakeholders, we are trying to establish a collaboration with SAMSIK. Because this is not something that we can solve as an individual operator. It's not something we are going to solve. There has been talk about whether we should monitor our submarine cables because it is critical infrastructure. But we cannot monitor that because we neither have the means for it and the manpower to do it. It is and will remain a national task that the Armed Forces must take care of. Then they say, they don't have the resources for that, they say there no ships for that and so on. So, it's a bit of a Gordian knot." (Danish participant)

"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. (Danish participant)

Collaboration is furthermore essential in coordinating the response to cyberattacks, both in involving different branches of government and emergency services (see also Emergency Management) as well as involving industry stakeholders. Such stakeholders can be organisations in related sectors that might be affected by the cyber-incident via chain reactions and therefore need to take appropriate measures to protect themselves, possibly activating their own response and recovery plans (see also Hybrid Threat), or other organisations in the same sector who might need to help with recovery.

"[SAMSIK] can also contact us. I can't say much more about it, because this system has the highest level of protection. It is a line of communication that has top priority for us and is important in the same way as 112. So, we are redundant, because we can't accept if it goes down. And I can say that there are playbooks and contingency plans on how to handle different scenarios. (Danish participant)

When it comes to outages in telecommunication services, such support with recovery can be accomplished through measures such as national roaming introduced in Ukraine since the full-scale invasion, enabling telecommunication providers to service clients of other providers in case one of them is experiencing issues due to cyberattacks or physical damage on its infrastructure.

"We have [..] national roaming. So if you cannot join to [Telecom provider A], if [Telecom provider A] doesn't work for you, in some regions, for example, if a customer can join to [Telecom provider B] or [Telecom provider C], there is no issue, they can call, they can use internet also. [..] Even the other countries should think about national roaming and they should have the capacity for them because mostly they have covers for their customers but don't have for others. Yeah, they should increase their capacity in case of war, in case of earthquake or something like that." (Ukrainian participant)

Further some of the participants established collaboration with external partners to recover from cyber incidents.

"We had a lot of help from outside the company. We got help from two well-known consultant houses who are specialised in security. I had the philosophy in the beginning, that two was better than one, but I had to admit that it was wrong. We got divergent information, so we ended up with one. We needed to trust only one. From day one and they helped us 24-7. We actually didn't know them before, but they helped us figuring out what kind of code that had infected us, and to calculate backwards and so on. We had not tried this before, so we had to lean on them. We also got a lot of help from Microsoft, for example. Someone arrived almost with white gloves and a stethoscope, and he could help us recreate some things. And then we hired a lot of consultants to re-build servers and restore all data ." (Danish participant)

International collaboration in emergency preparedness can furthermore be of use, for exchange of experiences and coordinating mitigation measures, e.g., if the attack on a critical infrastructure has an impact outside of the targeted country.

"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." (Danish participant)

3.3.4.2 Appropriate organisational structure

Transparent assignment of responsibilities for cybersecurity-related issues is crucial in ensuring that these issues get proper attention.

"For all our internal solutions, we have designated technical people responsible for vendor contact regarding configurations, updates, etc. These individuals should ensure proper identity and access management for their respective systems." (Danish participant)

In small organisations or organisations with limited budget, such responsibility can be distributed among employees whose roles are not directly related to security, of which they need to be made aware. Alternatively, dedicated security operation centres can ensure that security issues are properly handled, and cyber-incidents are detected and responded to in a timely manner.

3.3.4.3 Considering the human factor

As human error and social engineering remain among the most exploited vulnerabilities in cyberattacks (see Social engineering attacks), organisations should provide support to their employees to make them more resilient against these threats. Security awareness campaigns warning people against common threats such as phishing can be used for this purpose, while some employees (e.g. administrators) might require more in-depth security trainings. On a broader scope, awareness campaigns can be furthermore used to prevent mis-/disinformation, educating people on how to evaluate their information sources.

"So we've got huge campaigns about trusted resources, about who you can trust, what sources you should use [..] I learned to follow trusted resources, governmental or official. Often, I would check if a story comes from official sources from our side or from another country." (Ukrainian participant)

Awareness campaigns, however, are not sufficient on their own, unless people also have the capacity to behave in a secure manner. If the technologies in place are too complex to use, human error might be an imminent threat despite user education. Effort should therefore be made to reduce the cognitive load of people who need to use these technologies.

"When introducing new technologies, we try to design them with familiar workflows so users don't face a complete paradigm shift. This reduces the likelihood of security errors during transition periods." (Danish participant)

Further, it's important that all employees know what to do in case of an incident, which is not always the case.

"Some people panic; some don't. Some get very creative, some not. People come in slightly different models. Someone says "OK, what should I do? I can do it everything to help, just say what you want me to do." Others are more in a crisis mode and say "I can work 25 hours a day." And then I was like; people can't work for 25 hours because this is going to take weeks. So, you need to go home and get some sleep, so you don't end up getting unfit for a long period. Anyway, we identified those who was super important in IT, and we worked in two shifts. 12 hours work, 12 hours sleep. In the support services, we had three shifts and already on day one we made a plan for that." (Danish participant)

3.4 CHALLENGES

Our participants reported several challenges they face when trying to secure their digital infrastructure. In the following we group these into those that (a) arise from the complexity of the threat environment and those that (b) stem from the human element as part of cyber defences.

3.4.1 Complexity of cybersecurity

Complex digital infrastructures can lead to complex threat environments with a plethora of different technologies that need to be considered when defending against cyber-attacks. Danish hospitals, for example are known to have a large number of interconnected IT-systems:

"I went to Germany to do some preparatory work. On that trip I visited a university hospital where they had 40 clinical systems, and the staff at the hospitals thought that was a lot. The Danish hospitals have around 1000 IT systems ... So when German hospitals depend on fewer digital solutions than the Danish hospitals, then I would say – and this is on my own personal account – that they are generally more secure." (Danish participant)

3.4.1.1 False positives

False positives can create noise in the detection of cybersecurity incidents. They produce warnings despite the absence of actual threats. Automated defences are particularly susceptible to this and knowing your own infrastructure well is the only way to reduce false positives:

"As we learn the organisation and infrastructure better, we're able to fine-tune our security products to reduce false positives." (Danish participant)

This also means that (generational) changes in an organisations' infrastructure require to re-evaluate all automations and be mindful of changes that might affect automations.

3.4.1.2 Iot devices

The increasing digitisation of organisations poses additional risks. Wherever "dumb" devices are replaced with "smart" and connected ones, new cybersecurity risks emerge.

"Our hospitals are becoming increasingly digitalised, with almost every device—from medical equipment to fridges and even light bulbs—connected to the internet." (Danish participant)

The particularity of IoT devices is that they might operate in remote areas where physical security is not as tightly controlled, opening vectors for attack.

"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." (Danish participant)

3.4.1.3 Need for automation & false positives

Automation can decrease the burden maintaining secure operations even in complex infrastructure scenarios. Participants noted a need for automation in a lot of contexts to be able to manage cybersecurity tasks.

We need automated responses to counter automated attacks. (Danish participant) Especially the advent of wide-spread AI tools is both challenge and opportunity in the context of cybersecurity:

"I anticipate that working with and countering artificial intelligence will dominate our focus in the coming years. We're already integrating AI features into our firewall systems to better detect and mitigate AI-based threats. [...] Artificial intelligence represents one of our biggest security concerns, so we're focusing on understanding what's possible and developing strategies to block, mitigate, or prevent malicious AI applications." (Danish participant)

3.4.1.4 Playing catch up

Participants mirrored a well-known concern from the security field, that those defending systems are always playing catch-up with those trying to compromise them in attacks:

"The challenge with cybersecurity is that we're often playing catch-up. We can build secure infrastructure and prepare as thoroughly as possible, but it's only when skilled hackers or malicious actors find new attack vectors that we learn how to mitigate those specific threats." (Danish participant)

AI tools represent one technology where this challenge has become particularly pronounced.
"However, AI is evolving extremely rapidly, making it challenging for anyone to keep pace." (Danish participant)

3.4.1.5 Dependencies between sectors

Due to cross-dependencies, defences of individual critical infrastructure sectors are of little use (see also Hybrid threats). Often other sectors are needed to keep any other sector up and running.

"It does not help to just look at the individual sector. You have to look across and see where we have the dependency." (Danish participant)

In particular, the energy sector was named as backbone of the digitised infrastructure with everyone else heavily relying on it.

"If the intention is to completely shut down telecommunications in Denmark, then it would probably be the energy network you would target. It would be easier to shut down the energy network than to attack the telecommunication network separately." (Danish participant)

An important aspect also raised by our participants as part of the cross-sector dependence is coordination, or rather the lack thereof.

"I actually think it is the same in the energy sector, then I think that what we need is that the ministries sit at the head of the table to find out first and foremost: Who is coordinating across sectors? [...] That's what I think there is really missing right now and there is a great interest in tele sector to get that running." (Danish participant)

3.4.2 Socio-technical aspects of cybersecurity

The behaviour of those using systems and devices can make or break the security posture of an organisation (see also Considering human/organisational relationships for respective countermeasures).

3.4.2.1 Bad practices of users

When users, especially those with privileged accounts or those with access to sensitive data, show risky behaviour, that can compromise the organisation or cause conflict with legal frameworks.

"Well, our general manager, a doctor, was attacked. She opened a malware link on Facebook." (Ukrainian participant)

However, participants also noted that it is not always that users make foolhardy decisions, but that instead they "can be [...] too busy to remember security details" or that the high stress working environment might take its toll.

"We also need to consider the high-stress work environments in hospitals, like emergency departments. Under pressure, staff might be more susceptible to social engineering attempts that mimic a superior's voice or instructions." (Danish participant)

A lack of awareness by staff was also named as a critical area to improve, not only with aspects to cyber security, but also regarding physical security.

"People simply don't think about security. When we hire new staff, we take them through the hospital to show them how it operates. An adversary wouldn't necessarily need to hack through firewalls—someone with physical access could place a small device to capture data. The delivery areas are particularly vulnerable, with minimal surveillance and potentially interesting shipments secured by simple four-digit codes." (Danish participant)

Interestingly, our participants also reported on practices resembling neutralisation techniques, i.e., techniques used by humans to decrease cognitive dissonance when not following the proper security procedures they know.

"The "ask for forgiveness rather than permission" approach was widespread." (Danish participant)

3.4.2.2 Security vs. other considerations

According to our participants, one of the biggest challenges in maintaining a strong cybersecurity posture is balancing budgets and cybersecurity needs. Especially in crisis situations such constraints can be amplified.

"Broadcom bought VMware and double the cost for the solution. It was really critical for us because doubling the cost during the war or the infrastructure, it's madness." (Ukrainian participant)

Having legacy systems that cannot be easily replaced or cannot be updated to run with newer software poses a severe problem that companies try to mitigate by other practices:

"And in the telecom industry and the telecommunications sector is affected by the fact that you are dealing with really, really very old legacy." (Danish participant)

However, due to the specialised nature of some of the software required to run critical infrastructure and the limited suppliers of these software systems, some systems are incompatible with security measures from the get-go.

"The challenge remains with specialised medical software. For instance, we have a major patient system that doesn't run our antivirus because it operates at such a micro level that the antivirus interferes with its functioning. We lost that particular battle because there are only two suppliers worldwide for this system, and neither would accommodate our antivirus requirements. Sometimes we simply can't win these conflicts when the medical necessity outweighs the security concerns." (Danish participant)

Overall, hardening the system (see Hardening the system via preventive and detective technical measures) can make the system architecture more complex, which can lead to more effort and resources being spent on its maintenance, as well as increase the complexity for its users, e.g. by requiring additional authentication mechanisms.

3.4.2.3 Data storage risks

When physical risks to data mount due to data being held in conflict areas, moving them abroad might be good to retain a high security posture. However, sometimes regulations can prevent such measures:

"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." (Ukrainian participant)

3.4.2.4 Scalability & fallback options

For some essential services like police and emergency services, special communication solutions exist, that are redundant and can be operated even during power outages due to emergency generators (see Redundancy). However, society has changed a lot since the inception of such services and scaling these special communications solutions is not possible. Similarly, other fallback options of the past, like landlines, are not operating anymore, compounding the importance of keeping the telecommunications infrastructure working for all.

"The 70's, there we lived in a world where you can say well if our phones crashed, well, then you would manage that. You had a landline phone at home, and if it didn't work, well, it didn't work. [...] You weren't so dependent on these digital services. [...] Today is just very different [...] We are all completely dependent on being able to communicate with all these devices, and we can't buy anything without. [...] It is fine that the emergency services can communicate with each other. They should be able to, but it's just not enough." (Danish participant)

If then an incident occurs that knocks one or more telecommunications operators offline, the others often cannot scale fast enough to meet the demand of digitised societies.

"We didn't expect that a lot of people would join our network [after an attack on another company in the same sector]. It was really hard to, let's say, provide a service to them, [as well as] to our customers" (Ukrainian participant)

This is aggravated by the fact that ever more parts of society are being digitised. The digitisation of state services can have many benefits for citizens, but also increases the attack surface.

3.4.2.5 Supplier relationships

During conflicts, suppliers might leave certain areas or countries and leave their customers without service. This of course puts a strain on supplier relationships and can pose security risks.

"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." (Ukrainian participant)

Others might increase the costs since under the changed circumstances they need to increase security measures which increases operating costs for those suppliers:

"We didn't understand why, but some of them increase the costs. [...] But most of the suppliers, they are not prepared for it. They will do it, they will increase the cost for the solution or for something else. And it will be doubled. Because to be honest, before the war, suppliers, they didn't pay attention on the cyber security at all. They just wanted to provide the services. That's it. But at the moment they are trying to do something." (Ukrainian participant)

Some vendors also recognised the gravity of the situation and offered services for free while other refused any cooperation.

"For example, when I asked some vendors, they help us really for free. Even we have still that they supporting us and they told us, uh, we will support till the end of the war. It means that they are still supporting us. Yes, that was good. But yeah, some of them didn't even want to have a [...] pilot with us." (Ukrainian participant)

4

RECOMMENDATIONS

In this section we outline our recommendations based on the project findings for organisations as well as for future research.

4 RECOMMENDATIONS

In this section we outline our recommendations based on the project findings for organisations as well as for future research.

4.1 RECOMMENDATIONS FOR ORGANISATIONS

Having plans for emergencies (i.e., business continuity plans, disaster recovery plans, resilience plans, emergency and contingency plans, etc) is crucial for ensuring the resilience of the organisation against cyberattacks. These plans should address the possibility of adverse effect when executing them, such as the lack of coordination, unforeseen cascade effects (i.e. outages of services dependent on the systems being targeted, including effects outside of the organisation), communication issues, hierarchies for decision making, or unforeseen expenses. Once developed, the plans should be continuously maintained through practice, repetition, evaluation, and third-party assessment. It is furthermore of critical importance to understand regulations and to make a conscious gap analysis for compliance, especially for companies that are a part of the critical infrastructure value chain. The countermeasures listed in the report can be a good starting point for preparing emergency plans, as well as for general improvements of the organisation's security posture and cyber resilience. Of particular importance is establishing collaborations, sharing knowledge about incidents and responses with suppliers and customers, as well as with other organisations who might benefit from this knowledge, nationally and internationally.

4.1.1 Concrete recommendations for telecommunications providers

National Roaming for crisis situations.

One of the measures stressed by our Ukrainian participants as crucial for a resilient national mobile communications infrastructure was enabling easy roaming between national providers. This has enabled citizens to stay connected with digitised public services and public or news announcements even in the face of interruptions with one specific provider. This entails being able to service a significantly larger number of customers on short notice, i.e., having available capacity on the mobile network for emergencies. Clear communication surrounding this is also of the essence. If the public is properly informed about the fallback mechanisms national roaming can prevent runs on shops for SIMs of the providers that are still operating and in turn prevent overhead from unnecessary activations of SIM cards that would not be used after the incident.

Prolonged operation capacity during energy outage.

Our Danish participants have identified the energy sector as Achilles heel of the communications infrastructure. Indeed, some argued that attacking the energy sector and exploiting the interconnectedness of the sectors is the easier target. Insights from our Ukrainian participants support this view. In the beginning of the war, Russian attacks on Ukrainian energy infrastructure were able to disable communications infrastructure. Over time the telecommunications providers built up the capacity to operate, e.g., their mobile networks for periods of 12-24 hours even without the power grid operating. We strongly recommend building up such capacity in Denmark as well. With a decline in usage of traditional linear broadcast media, many citizens will rely on online communications to receive public announcements and news.

Protection against hybrid attacks.

Our Danish participants described hybrid attack scenarios often as cyber-attacks preceding and setting the stage for physical attacks, e.g., destabilisation of societies before warfare. However, experiences from Ukraine also show different scenarios. Ukrainian telecommunications providers reported about physical

attacks capturing part of the digital infrastructure with the intent to launch attacks from terminals that are typically trusted parts of the infrastructure. Therefore, Ukrainian mobile providers have started to implement defences against such "insider" attacks.

Shared threat intelligence & Emergency simulations. One of the primary lessons that Ukrainian participants stressed is a change in mindset from seeing what would traditionally be a competitor to seeing an ally. Facilitated by government agencies, the Ukrainian telecommunications providers are now intensively sharing threat intelligence. According to our Danish participants Denmark has a way to go in this regard. Additionally, Danish participants mentioned that other Nordic countries, e.g., Sweden, are already holding emergency simulations across the whole telecommunications sector and including other critical infrastructure sectors. The participants argued that Denmark should try to do similar simulations and could learn from them how to do it.

4.1.2 Concrete recommendations for policy makers

Build support communities. Many Danish organisations are struggling to build up their own cybersecurity competences. An interesting approach that our Ukrainian participants described was building up a nation-wide cybersecurity community to help fill this gap, e.g., by lending expertise during hiring efforts so that companies can find the most suitable candidate for them, even when they currently have little expertise in the cybersecurity field in which they are trying to hire.

Clear responsibilities for the protection of critical infrastructure. Danish participants outlined their frustrations when it comes to responsibilities of protecting critical infrastructure, specifically submarine cables. Our Danish participants explained that neither the telecommunications companies nor the military seem equipped and willing to protect these cables, making them an easy target to disrupt digital infrastructure. They indicated that a gap in legislation leaves these critical pieces of the digital infrastructure unprotected and that government action is called for.

Mandatory compatibility with cybersecurity measures for products aimed at critical infrastructure sectors. Danish participants mentioned that for some products they need to operate critical infrastructure, the very limited number of possible suppliers limits the leverage they have to demand from suppliers to make the products compatible with cybersecurity measures. This could be done by developing national and international regulations to strengthen the compatibility of cybersecurity products used by critical infrastructure sectors.

Mandate cybersecurity supply chain management for government contracts. One aspect stressed by both, Danish and Ukrainian participants, is that a supply chain view needs to be promoted among companies. One way to achieve this would be to mandate cybersecurity supply chain management, ensuring companies are aware of cyber risks from their suppliers and to their customers. NIS2 builds a foundation for this, but according to our participants certifications are just the first step and a true willingness to have a supply chain view is needed among companies.

4.2 RECOMMENDATIONS FOR FUTURE RESEARCH

4.2.1 Dependencies between sectors

This report is a pilot project which realised parts of a larger-scale project that remains relevant. Conducting a standalone sector analysis (telecommunication) can provide valuable socio-technical insights and contribute key technical, operational, and organisational elements to improve cybersecurity emergency response and preparedness. However, focusing on a single sector could also overlook the

interdependencies between sectors and the importance of considering these interdependencies for societal resilience. Examples of such interdependencies in Denmark are manifold. For instance, one exists between the energy and tele-communications sector, as also outlined by our participants. However, many more exist. The centralisation of healthcare services in big hospitals away from regional facilities increases the interdependence of the healthcare sector with the transportation sector. If transportation and consequentially citizen mobility is impaired, this impacts citizens' access to healthcare services.

We believe a comprehensive analysis is a direction for future research of utmost importance that offers Denmark a broader view of the interdependencies between sectors and countries regarding digital infrastructures and in particular the cybersecurity for critical infrastructure. Such research efforts would provide the defence industry, authorities, and other relevant sectors with the essential information needed to make decisions about training, adoption and development of new technologies, implementation of innovative measures, and further investments in and collaborating with private research organisations, academia, and further parts of industry. All these efforts help create a more cyber resilient society.

4.2.2. Alternative communication methods

The need for alternative telecommunication channels has been acknowledged by our participants that either experienced telecommunication outages themselves or saw it as a threat to their organisations or society. Providing such communication channels, however, can be a challenge both on a technical level (e.g., ensuring their general resilience against cyber and hybrid attacks) and on a social level (e.g., ensuring that these channels can be used by wider society, including people with low income and/or low technical literacy, in case of a large-scale cyberattacks). Possible solutions can vary from large-scale infrastructure implemented and maintained by governmental institutions to private solutions such as Starlink or similar alternatives. Correspondingly, the accessibility of these solutions, in terms of their costs, ease of use and trustworthiness can vary. Developing, implementing and testing appropriate solutions requires interdisciplinary research with collaboration with government, industry partners, and general population.

4.2.3 Preparedness guidelines for population

Large-scale cyberattacks can result in outages of critical systems and services, affecting the daily lives of people. While mitigating the impact of these cyberattacks depends on successful emergency response procedures on behalf of government and affected critical infrastructure companies, further support should be provided to the general population. The most effective way of providing support, however, remains an open question. There have been several solutions used by people in Ukraine to protect themselves against communication outages, such as getting a second SIM card from an alternative telecom provider, obtaining radio stations or Starlink terminals, or being ready to switch to paper-based communications. These solutions can be used as a basis for preparedness guidelines communicated to the population in Denmark and other EU countries. However, ways to effectively deliver these guidelines and support the population with their concrete implementation need to be researched.

4.2.4 Attack simulations

On an organisational level, preparedness towards cyberattacks and natural disasters involves developing and maintaining incident response and disaster recovery plans, which are communicated to employees of the organisations. To ensure the effectiveness of these plans, their testing, e.g., as incident simulations, is required. Several approaches for such testing have been proposed, such as adversary simulation and other red team exercises. It is, however, important to ensure that the developed plans and simulation campaigns are both designed to be effective in addressing the specific threats relevant to the organisation and are properly implemented and followed in the organisation. This is not a trivial task.

For example, while phishing simulations are a commonly recommended method to evaluate the organisational vulnerability for phishing campaigns and to raise employee awareness, research shows that in some cases such campaigns can be more complex to implement than often thought (Volkamer, Sasse, & Boehm, 2020; Brunken, Buckmann, Hielscher, & Sasse, 2023) and they can be ineffective in raising the cyber resilience of organisations (Lain, Kostiainen, & Čapkun, 2022; Schöps, Gutfleisch, Wolter, & Sasse, 2024; Schiller, Adamsky, Eichenmüller, Reimert, & Benenson, 2024). Research is therefore needed to understand how to properly design attack simulations so that they address the specific security requirements of the organisation they are used in.

CONCLUSION

Our research shows that the cyber threat, especially from Russian actors, is a significant concern in Ukraine and recognised by many of the Danish stakeholders who are deeply concerned about current and future attacks. The telecommunication sector, together with the energy sector, can be an attractive target to attackers with destructive aims, since the attacks on this sector are not only disruptive by itself, but can have chain reactions towards other sectors, effectively causing great damage to society. While the views among the Danish stakeholders differed on to what extent the Danish telecommunication is vulnerable to cyberattacks, the testimony from the Ukrainian participants shows that telecommunication outages can put people in danger and in worst case cost lives. Ensuring resilience of the telecommunication sector is therefore of utmost importance.

In case of telecommunication outages, the relevant Danish authorities seem to have efficient alternative communication lines in place (SINE etc.) so that they can communicate with each other in case of a successful attack on the telecommunication sector. However, there is no telecommunication alternative for most citizens to communicate with family, colleagues and authorities or to handle the most important digital daily activities, for example online banking, doctors' appointments etc. The Ukrainian participants talked about various mitigation measures they developed as a consequence of the successful attacks on the Ukrainian telecommunication sector, including alternative energy sources, multiple SIM cards and widespread use of satellite connections. Their experience can be used to support the Danish population in being prepared for possible telecommunication outages. Studying the harsh consequences of the attacks in Ukraine, it's an open question to what extent the civil Danish population is protected in their daily lives in case of a major telecommunication outage.

REFERENCES

Brunken, L., Buckmann, A., Hielscher, J., & Sasse, M. A. (2023). "To Do This Properly, You Need More Resources": The Hidden Costs of Introducing Simulated Phishing Campaigns. USENIX Security Symposium (USENIX Security).

Danish Emergency Management Agency. (n.d.). Prepared for crises. Retrieved 11 10, 2025, from https://www.brs.dk/da/forberedt/translations-in-ten-languages/

European Commission. (2022). Digital Economy and Society Index (DESI) 2022. Retrieved 2025, from https://digital-strategy.ec.europa.eu/en/policies/desi

Lain, D., Kostiainen, K., & Čapkun, S. (2022). Phishing in organisations: Findings from a large-scale and long-term study. IEEE Symposium on Security and Privacy (SP).

Ministeriet for Samfundssikkerhed og Beredskab. (2025, 01 29). Organiseringen af Ministeriet for Samfundssikkerhed og Beredskab er på plads. Retrieved 06 02, 2025, from https://samsik.dk/artikler/2025/01/organiseringen-af-ministeriet-for-samfundssikkerhed-og-beredskab-er-paa-plads/

Prakash, T., Schrøder, C., & Moltke, H. (2023, 01 10). Flere danske banker ramt af cyberangreb: Pilen peger på den russiske gruppe Killnet. (DR) Retrieved 09 10, 2025, from https://www.dr.dk/nyheder/penge/flere-danske-banker-ramt-af-cyberangreb-pilen-peger-paa-den-russiske-gruppe-killnet

Schiller, K., Adamsky, F., Eichenmüller, C., Reimert, M., & Benenson, Z. (2024). Employees' Attitudes towards Phishing Simulations:" It's like when a child reaches onto the hot hob". ACM SIGSAC Conference on Computer and Communications Security.

Schöps, M., Gutfleisch, M., Wolter, E., & Sasse, M. A. (2024). Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy. 33rd USENIX Security Symposium (USENIX Security).

SektorCert. (2023). Angrebet mod dansk, kritisk infrastruktur. SektorCert.
Styrelsen for Samfundssikkerhed. (2025, 03). Cybertruslen mod telesektoren. Retrieved from https://samsik.dk/publikationer/telesektoren/

United Nations. (2024). E-Government Survey 2024. Retrieved from https://publicadministration.un.org/egovkb/en-us/#0

Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing simulated phishing campaigns for staff. Workshop on Security, Privacy, Organisations, and Systems Engineering.

RESILIENCE CENTER DENMARK