Digital Infrastructure Resilience and Security
Policy Implications and Mitigation Measures
05 May 2024

White Paper
By
Dr. Georg Serentschy

Table of Contents

1 Executive Summary

This paper addresses policy makers and regulators, companies operating critical infrastructure, as well as wider audiences, to raise their awareness of the necessity of urgent changes in the way the digital ecosystem is governed, against a backdrop of seismic shifts in geopolitics and an ever-changing threat landscape to digital infrastructures and systems.

A need to act now: Our research suggests that policy makers, regulators and other relevant stakeholders should become more aware of the situation and the urgent need to act. We aim to support this with the help of telling examples, covering the ramifications of the dynamic threat landscape. Building on this, recommendations for remedial action and structural improvements to digital governance are described. A detailed list of recommendations can be found in chapter 7 (Recommendations).

Understanding the wider context:

- The **geopolitical context** is key: The issues addressed in this paper are vital to Western countries' security interests. Their interdependencies require the assessment and management of security threats in a geopolitical context. The systematic identification of critical choke points in the supply chain is an important element of this approach. Without this context, security risks cannot be adequately addressed. For more details see chapter 4 (The Geopolitical Dimension).
- **Hybridization:** The current threat landscape can be aptly characterized with this term which describes the type of systemic competition in which any possible instrument is used to achieve the objective of the threat actor in question. For more details see section 3.4.2 (Hybridisation).
- **Complex threat landscape:** Disruptions to digital systems are caused by natural phenomena and man-made activities, such as cyber-physical attacks, sabotage, etc. However, there is a growing new phenomenon, a gray area between natural and man-made causes, triggered by climate change. There have always been "natural" reasons for disruptions such as earthquakes, floods, storms, forest fires, etc., but the increased severity and frequency of most of these disasters is closely linked to climate change. This needs to be differentiated as the causes and prevention are different. For more details see section 3.1 (A Holistic View on Resilience and Security – Role of Regulators).
- **Telecom regulators** can and should play a crucial role in this context and their importance is sometimes underestimated. However, regulatory authorities in most cases do not have a mandate to develop or apply a holistic view and break out of their vertical silos. This is a wakeup call for policy makers to give regulators a new and expanded mandate which would enable them taking up a crucial role in this context.
- Improving the **resilience and security of digital systems** requires a **new form of public-private partnership between governments and the private sector**. Governments cannot tackle these challenges alone, nor can industry. This also has implications for the governance structure for digital affairs. The establishment of a central coordinating body is an important step towards overcoming the usual historically fragmented governance structures. For more details, see chapter 6 (Implications on the Governance Structure – Need to act now).

Relevance for Canada: The war in Ukraine, the escalating conflict in the Middle East and the looming threat of war between China and Taiwan are geographically far away from Canada. However, this is no reason to be complacent and feel safe. Threats to digital systems are ubiquitous and supply chain disruptions have global implications. Specific references for Canada can be found in sections 3.1, 3.7.4, 4.2, 4.4, and 5.7.3.

A full set of **recommendations** can be found in chapter 7 (Recommendations). The following specific points stand out:

- More **transparency** seems to be necessary to **show the public the extent of the vulnerability of our modern society** and to raise the willingness to take appropriate measures, i.e. reorganization of the responsibilities and/or authorities of governance systems internally. We opine that the **highest possible level of transparency**, based on a detailed analysis of disruptive incidents or reverse-engineering of an attack, exposes the attackers and leaves them no choice but to either admit to the attack or use excuses that are so ridiculous and transparent that any observer can easily see the truth (“qui s’excuse, s’accuse”).
- A **security certification for all IoT devices and EVs (electric vehicles)**, regardless of their origin, should be made mandatory by law. The absence of such a security qualification - for whatever reason - can be seen as an attempt to undermine national security.
- **Resilience and security do not come for free**: Telecom operators need incentives to invest in redundant infrastructures to increase resilience and consumers need to be aware that the use of security-certified products comes with higher prices for these products.

Against the backdrop of the dynamically developing and complex threat landscape, we recommend **setting up of a wide-ranging Digital Authority as a central coordinating body and public think tank.** This is more effective than incremental small changes. Suggested **key-functions of a wide-ranging Digital Authority** are:

- Digital strategy development and think-tank for government, combining telecom regulation with innovation policy and industrial policy.
- Information and service for stakeholders.
- Digital research coordination and funding.
- Regulation and market oversight.

The governance setup for digital affairs has grown incrementally in most countries. New national or supranational laws and regulations are often allocated to existing authorities or ministries - less on the basis of an overarching strategy, but more on the basis of day-to-day political opportunities. The **main reason for establishing a Digital Authority as a central coordinating body with far-reaching competences** is obvious: the security and resilience of digital systems, which are essentially the central nervous system of our society, is too important to be left to the status quo, which in most countries is a fragmented governance landscape, with critical gaps and often overlapping competencies resulting in inter-institutional turf-battles and regulatory uncertainty.

2 Introduction

The geopolitical developments of recent years, the war in Ukraine, a dramatic increase in regional conflicts with global implications, the disruption of global supply chains, increasingly dramatic effects of the climate crisis, etc., have contributed to the growing threats to the security of digital infrastructures and hence the need to make them more resilient.[1] Digital infrastructures, in particular those labelled as "Critical Infrastructures" represent the backbone of our society. These **threats are largely global, affecting all countries regardless of how far they are from the epicenters of the crisis. A**ssessing the entire threat landscape therefore requires a holistic geopolitical view.

This document is a snapshot of our research in this area, which we have been pursuing with increasing intensity for some time. It is intended to provide a detailed and illustrative - but not exhaustive - overview of developments in the field of network security and resilience from the outbreak of the COVID-19 pandemic to the present day. Due to the highly dynamic nature of these developments, this is work-in-progress. It is inevitable to amend and revise our analysis and recommendations over time. The aim of this paper is to highlight the most important developments and trends in the areas of security and resilience of digital infrastructure, to outline approaches to tackling these challenges, to characterize institutional and regulatory implications and to derive recommendations for future steps based on this analysis.

This **paper is based** on numerous **interviews with experts** from the regulatory community, the security apparatus, policy, and industry experts and academic security experts. For understandable reasons, most of the interviewees asked not to be identified in this paper. In addition, **extensive secondary research** was carried out. However, it must also be noted that the data base is partly incomplete and partly inconsistent. In this respect, the expert interviews are of particular importance.

The COVID-19 pandemic, combined with escalating geopolitical tensions, led to an 21,4% compound annual growth of incidents from 2003 to 2022 impacting critical infrastructures in the EU (exhibit 5).[2] This development has placed unprecedented pressure on global networks, posing significant risks to the security of digital systems and stressed the need to increase their resilience. The 2017 "NotPetya" ransomware attack (attributed to Russia) severely disrupted global business operations, although its primary target was Ukraine. The attacks on submarine cables between Sweden and Estonia in October 2023 is another incident of vulnerabilities that nations are facing currently. In this "poly-crisis" environment, protecting global network integrity along with its subsets - national networks - is highly demanding and critical.

Due to **spillover effects on and from adjacent sectors**, this paper also covers examples from the energy, industrial automation, and transportation sectors (including navigation), all of which are on the target list of **state (backed) actors** and **non-state extremist groups, aiming**

[1] Security and resilience are not the same and not similar, for details see chapter 3.
[2] Source: EuRepoC quoted by https://www.swp-berlin.org/en/

to attack core functions of our society. As far as **state actors** are concerned, such activities must also be seen as a key element of **hybrid warfare**.

This paper also covers examples of **mitigation measures** and **responses from affected companies and organizations** as well as **implications for the governance structure.**

Among other topics, **this paper deals with important lessons** for policy makers, regulators and industry:

- Every attack on digital infrastructure contains an implicit or explicit message. Deciphering this message is important. Looking at an incident in isolation is not enough and can result in misleading conclusions. A telling quote can be found here.[3]
- Regulators should seek to broaden their remit and obtain a new mandate from policymakers. Embracing the new challenges is key to playing a decisive role in protecting the digital infrastructure.
- Cooperation models between horizontal and vertical authorities are a suitable way of breaking out of the vertical silo and overcoming the new challenges. They are also a useful first step towards a more comprehensive governance reform.

Some high-level comments on the role of the European Cyber Resilience Act (CRA): Many of the points raised in our paper, such as the proposed security certification for IoT products and EVs (electric vehicles), are also addressed in the CRA.

- The CRA will have to be formally adopted by the Council before it becomes law. That will likely be in April or May 2024. The final version of the CRA will then be published in the EU's Official Journal.
- The term “Cyber Resilience Act” is somewhat misleading because it does not seem to say anything significant about resilience, but is limited to cybersecurity issues in a broader sense.
- The problem statement and motivation of the CRA are very broad and comprehensible.
- Although the CRA covers many points that are addressed in our paper (e.g. IoTs and EVs), it is unclear whether there are any regulatory gaps or overlaps in relation to adjacent directives or regulations.
- It is striking that oversight is to be carried out in the traditional way by national authorities and not by a (new) European institution, as is the case with the AI Act with its more modern approach. This raises concerns that this could trigger further regulatory fragmentation.
- It is also striking that **open-source** products are apparently not to be affected by the CRA. Nevertheless, some open-source parties remain critical of the proposed regulation. An interesting voice in this context is the Dutch tech blogger Bert Hubert and his relevant blog post is helpful for a better understanding of these concerns.
- In any case, the Impact Assessment is worth reading for a better understanding of the CRA.

[3] “***As ever with Russia, it’s wise not to look for a single explanation of why they are doing anything. There’s always a combination of things going on.***” (Keir Giles, senior consulting fellow at think-tank Chatham House)

Overview of how the paper is structured:

- **Chapter 2 (Introduction)** sets out the motivation and background for producing this paper,
- **Chapter 3 (Overview)** describes the scope of the topic, the threat landscape and its ramifications, definitions and useful explanations, as well as an overview of related threats,
- **Chapter 4 (Geopolitical dimension)** illustrates the importance of this perspective,
- **Chapter 5 (Illustrative examples and hybridization)** provides selected examples to illustrate the complexity of the threat landscape and the almost endless variations of attack methods, which are amplified by hybridization,
- **Chapter 6 (Governance structure)** describes the impact on the digital governance structure and the urgent need for action.
- The paper concludes with a set of **recommendations (Chapter 7)**, which are also reflected in the Executive Summary (chapter 1).

Cross-references to relevant parts of the paper are indicated by a link to the respective color-coded page number.

3 Overview

3.1 Security and Resilience - key trends in cyber incidents

For decades, network **security and resilience** have been seen as a purely technical matter. However, it should be kept in mind that security and resilience are not the same and not similar. **Security** measures are about **locking up** (firewalls, anti-malware software, access systems, fences, locks, etc.). **Resilience** is about **standing up**. (Digital) resilience never makes the false assumption that security will stop all attacks and breaches; therefore, resilience is about surviving inevitable attacks from inside and outside and about penetrations. Resilience is about continuing to do business even under attack, about discovering breaches and containing them, and about ultimately prevailing despite them. Network redundancy is one way of increasing resilience. There is now a growing awareness that it also has a strong geopolitical dimension that must not be overlooked. More on various aspects of "resilience" can be found here.[4]

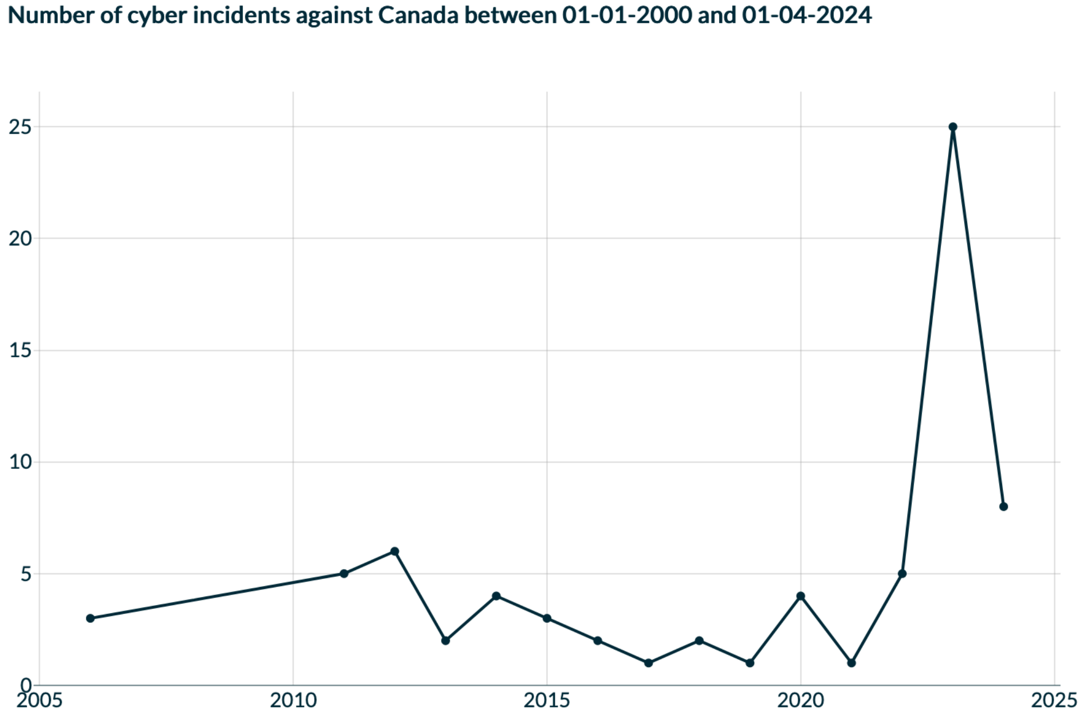
Recommendation 1 – Security and resilience do not come for free: 51

The **European Repository of Cyber Incidents (EuRepoC)** is an independent research consortium dedicated to providing evidence-based scientific analysis of cyber incidents for a better understanding of the current cyber threat environment. Its resources include user-specific, reliable data based on an interdisciplinary perspective. **EuRepoC** provides a **comprehensive**, **inter-disciplinary** and **continuously updated** database of cyber incidents worldwide, covering incidents from the year **2000** to the **present, ~3,000 articles** from **220 sources** scanned and curated daily, each cyber incident is coded across **60 variables** by **EuRepoC's** experts.

The EuRepoC dashboard displays key trends in cyber incidents tracked in its database, and it is updated daily. The following exhibits 1 – 5 extracted from the EuRepoC dashboard provide an overview of cyber incidents against selected countries/regions (Canada, US, Taiwan, South-Korea, EU) between 01-01-2000 and 25-02-2024.

The overall picture shows that **the situation has deteriorated massively** from a global perspective, in particular in the last 4 years

[4] https://www.lse.ac.uk/ideas/Assets/Documents/updates/2022-SU-NATO-HallSandeman.pdf and Stockholm Resilience Centre 2020 https://www.stockholmresilience.org/research/resilience-dictionary.html



Note as of 01/02/2023, the EuRepoC expanded its inclusion criteria. This can explain a spike in incidents from this period onwards.

Exhibit 1: Increasing number of incidents against critical infrastructure in Canada (source: EuRepoC dashboard)

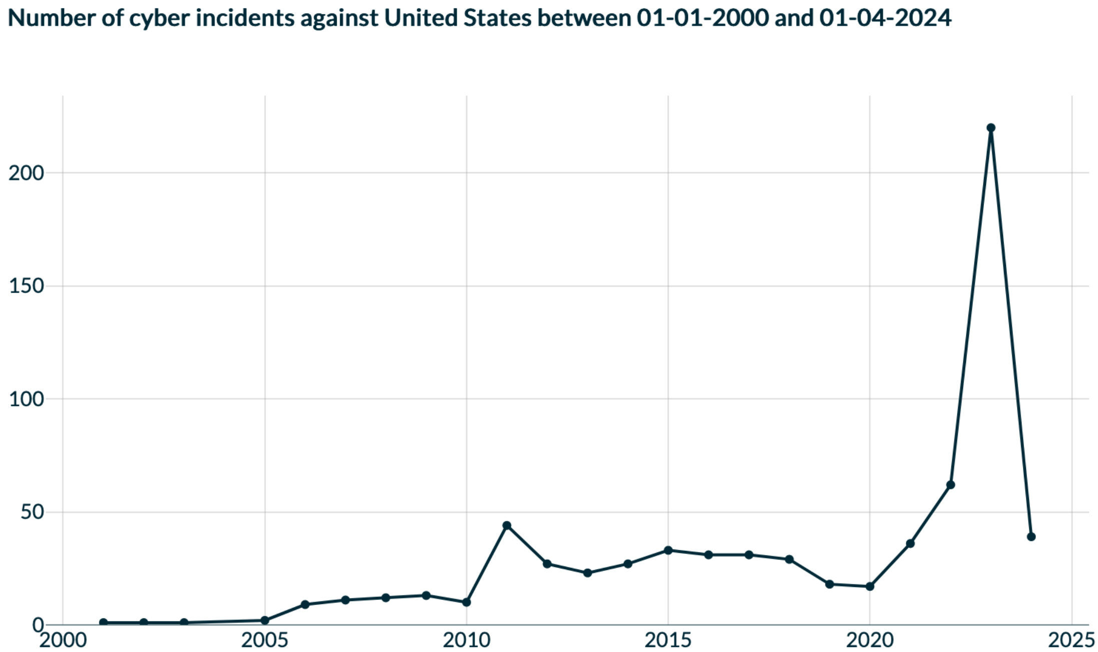


Exhibit 2: Increasing number of incidents against critical infrastructure in the US (source: EuRepoC dashboard)

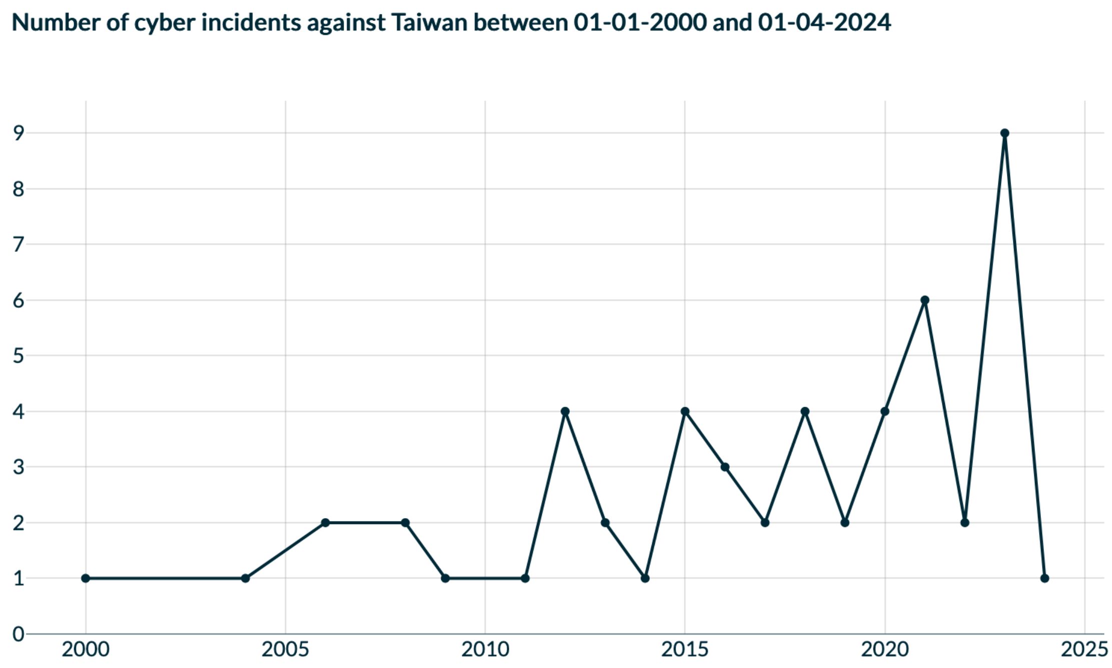


Exhibit 3: Increasing number of incidents against critical infrastructure in Taiwan (source: EuRepoC dashboard)

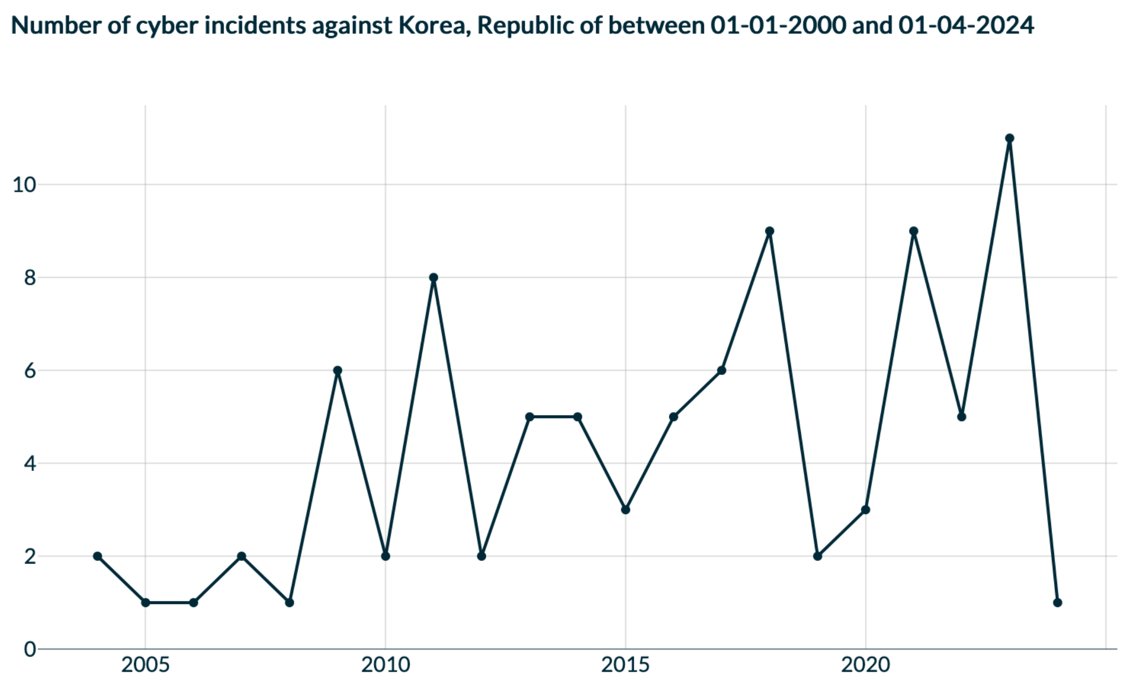


Exhibit 4: Increasing number of incidents against critical infrastructure in the Republic of Korea (source: EuRepoC dashboard)

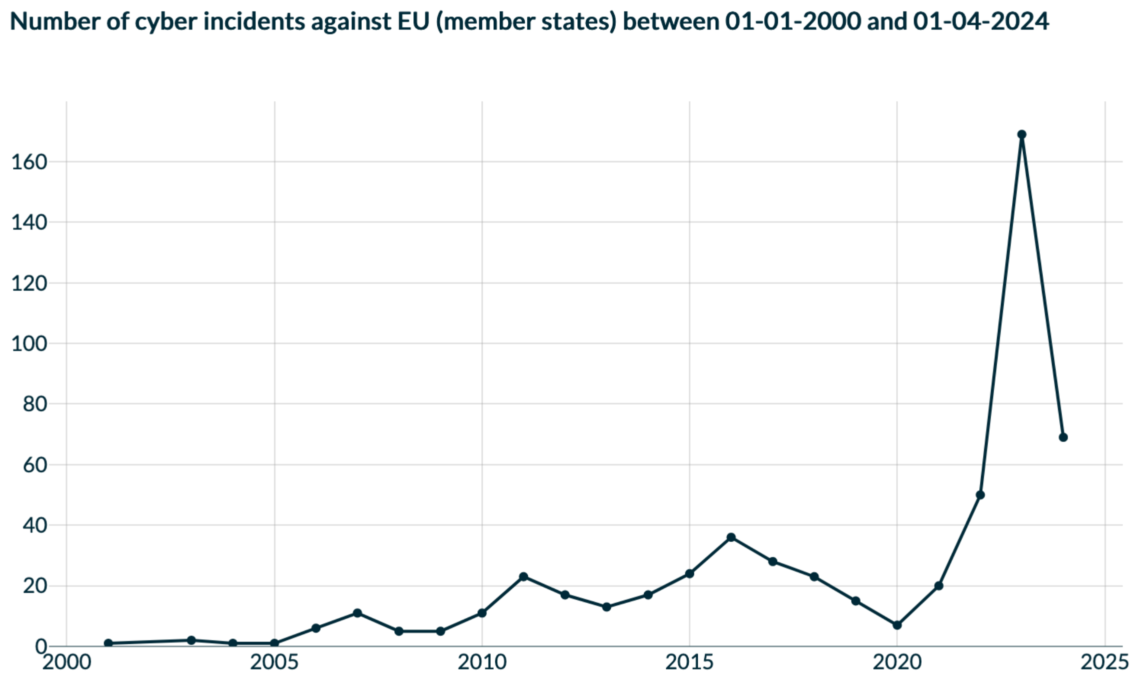


Exhibit 5: Increasing number of incidents against critical infrastructure in the EU (source: EuRepoC dashboard)

3.2 A Holistic View on Resilience and Security – Role of Regulators

We need to develop a Holistic View comprising not only a comprehensive inventory of infrastructure elements, such as cables and switching and routing equipment, but also peering agreements, ownership relations, IXP presence, capacity issues and a look at the relation between physical and logical networks. This in addition to (1) incidents caused by **natural disasters like tornadoes, earthquakes and volcanic activities**[5] and (2) a growing number of man-induced disruptions triggered or amplified by **climate change, such as increased wildfires, floods, landslides, etc.** To complete the picture, there is also (3) the growing category of **disruptions caused by hostile actors**. All three categories of disruptions pose a threat to the functioning and integrity of digital systems calling for a much higher level of resilience. If the actors involved lack the political ambition to develop and apply a holistic approach, the responsible authorities run the risk of making do with small adjustments and getting lost in uncoordinated micromanagement.

[5] The ongoing massive volcanic eruption in Iceland near the town of Grindavik led to the complete destruction of all infrastructure in the surrounding area. Something similar may happen in all active volcano and earthquake regions. There are around 1300 to 1900 active volcanoes worldwide, with 40 to 50 eruptions taking place simultaneously. 800 million people live in volcanic regions https://www.icelandreview.com/nature-travel/eruption-has-begun-north-of-grindavik/

Telecom regulators can and should play a crucial role in this context and their importance is sometimes underestimated. The reasons for this situation are complex. Regulatory authorities often have an overly narrow view focused on economic and legal issues, and they tend to lack understanding of the geopolitical dimension as well as technical, strategic and cybersecurity know-how. Most importantly, regulatory authorities in most cases do not have a mandate to develop or apply a holistic view and break out of their vertical silos. This is a wake up call for policy makers to give regulators an new and expanded mandate.

3.2.1 Category 1: Natural disasters

The **Icelandic regulator** is a notable example of performing a holistic task. It is mandated with improving the resilience of digital infrastructure by, among other things, creating a holistic picture that includes a complete inventory of all types of digital infrastructure and conducting risk analyses. It is executing all relevant regulations, not only the Telecommunications Act, but also the NIS-2 Directive and the CER Directive, as well as other cybersecurity regulations. The authority is thus well positioned to coordinate all the necessary activities. A lack of redundancy is considered as a market failure, allowing the regulator to impose relevant obligations, for example requesting redundant connectivity by installing additional base stations with high autonomy (see below) and redundant back-haul connectivity. With this, the regulator managed to keep connectivity in the Grindavik region[6] up and running despite the massive damages caused by the volcano and its seismic activities. All mobile base stations are battery-backed (4 hrs.), and mobile diesel generators can be quickly brought to places that are cut off from the power grid by connecting them with a plug. This example may sound somewhat exotic or even extreme, but as a small island in the middle of the Atlantic, permanently threatened by massive volcanic activity and fully dependent on submarine connectivity, Iceland gives us a preview of what may happen or has already begun in other regions of the world in terms of extreme events, increasingly induced or intensified by climate change.

3.2.2 Category 2: Natural disasters triggered or amplified by climate change

Man-induced climate change increasingly triggers extreme weather events. The resulting ‘natural’ disasters lead to a strong rise in the destruction of digital and other infrastructure (see exhibit 6). This is an important reason why we need more institutional and regulatory agility.

Furthermore, it can be said that the **Nordic and Baltic countries**, which face a particular serious security threat situation, are all forerunners in this field. They are aware of their threat situation, the issue is high on their agenda and they have the political mandate to act appropriately.

The **lessons learned from the war in Ukraine** in terms of resilience and the modus operandi between authorities and operators during the war are also very relevant to the functioning of networks under extreme stress. Every day, new and often unexpected challenges arise for the

[6] See footnote 4.

people in charge, which do not allow them to always play by the rules. The quantity and quality of personnel required to keep the networks up and running 24/7 requires an agile management attitude and the ability to act under unforeseeable and extreme conditions. Learning and adapting every day and trying to anticipate what may happen is crucial. Operators and authorities in Ukraine are working according to the "3P-Forumula": for people – by people – with people. Base stations' battery power has been extended to 72 hours and diesel generators for supporting critical sites are essential. The logistics of getting portable diesel generators to critical locations on time and maintaining and repairing infrastructure under wartime conditions is another difficult aspect that we can learn from for use in natural disaster situations.

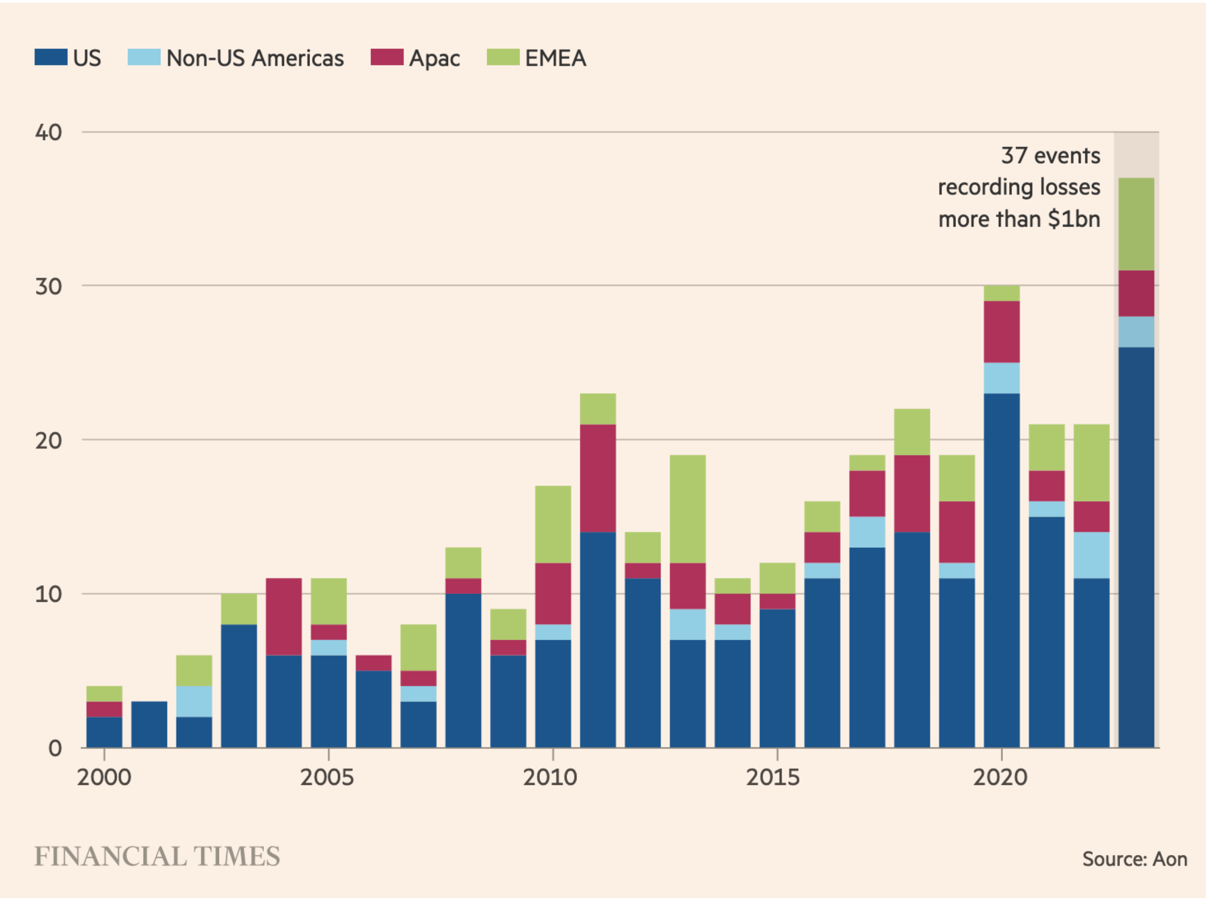


Exhibit 6: Last year (2023) had a record number of billion-dollar insured losses from extreme weather (FT, 22 April 2024)[7]

In this sense, **the practice in the Nordic and Baltic countries,** and the **lessons from Ukraine** can serve as an example for improved institutional and regulatory agility.

[7] https://www.ft.com/content/d935f3ff-4643-47b8-9272-dd0f5715023e?desktop=true&segmentId=d8d3e364-5197-20eb-17cf-2437841d178a#myft:notification:instant-email:content

3.2.3 Category 3: Disruptions caused by hostile actors

The third category, **disruptions by hostile actors**, which manifest themselves in the form of cyber attacks, cyber-physical attacks[8] and acts of sabotage, is described in detail in chapter 5. These are coming from different camps. Besides criminal actors (i.e., copper thieves and similar) we see radical environmentalists, religious fanatics (both fighting against digitalization and society), political extremists, and acts of sabotage from various players in the value chain. This includes hostile states, state-backed actors and criminal groups (with blurred boundaries between them).

3.2.4 Re-shuffling the regulatory agenda

De-siloing telecom regulation and re-shuffling the regulatory agenda: This is a wake-up call for policy makers to reshape and expand the mandate of regulators to make them ready for wider responsibilities, cross-sector cooperation and to re-focus their agenda. Greater redundancy of network elements and the reduction of single points of failure are a prerequisite for greater resilience. However, this is at odds with current regulatory measures such as network sharing and access to the infrastructure of other operators. Considering the geopolitical situation, the growing number of natural- and climate change induced natural disasters, and the complex threat landscape, resilience-reducing regulatory measures like infrastructure sharing and access to infrastructure should be avoided.

3.3 Increasing the Cost for Attackers is crucial for Defense

A **successful defense strategy** requires first and foremost a reduction of threats, i.e. more attention to the red part of the exhibit 7 below (in contrast, reduction of vulnerabilities is represented in the blue part). However, the question remains whether the present tools are comprehensive enough to combat hybrid threats effectively. Military doctrine on defense and offense needs to be adapted for the civilian (dual-use) domain to successfully counter threat actors and increase their costs. Due to hybrid threats, we are currently in a grey area between peace and war globally and need to adapt. We should not militarize civil society, but rather put more resources and thinking into strengthening civil society in the fight against criminal and extremist, ideologically or politically driven actors making use of hybrid instruments.

Versatile Engagement Strategy: The ICC cybersecurity working group advised policymakers to pursue a **"third way" instead of a binary strategy** that is either predominantly **defense or offense**. This involves tackling the rising trend in cyberattacks head on, and reversing this trend by changing the currently far too attractive payoff ratio that motivates attackers. To change the expected cost-benefit calculation of the attackers, **the attackers' costs must be increased as much as possible.** This can be achieved by increasing the likelihood that the attackers will be detected and caught by applying improved attribution strategies and methods. According to the EuRepoC repository, 30% of all attributions are done by IT-security companies (mostly US-based). Only 16% attributions are from receiver states governments.

[8] For the difference between cyber attacks and cyber-physical attacks, see section 3.5.1.

This demonstrates a significant upside potential for improved multi-stakeholder attribution strategies and methods (for comparison, 35% are attacker self-attributions).

Necessity of Global Cooperation: Today's communication networks consist of various layers and highly complex structures, ranging from a single home or cell phone to very sophisticated IoT/Cloud systems with billions of automated devices powered by complex AI systems. The number of devices also gives an unprecedented opportunity to weaponize Distributed Denial of Service (DDoS) attacks, deploy them in geopolitical conflicts.

Fighting against these threats is beyond the capability of a sole service or infrastructure provider and requires cooperation of all global stakeholders, not limited to operators, also regulators, security agencies and IT firms, states and international organizations. Public-private-partnerships models between all stakeholders can help achieving a balanced offensive and defensive strategy.

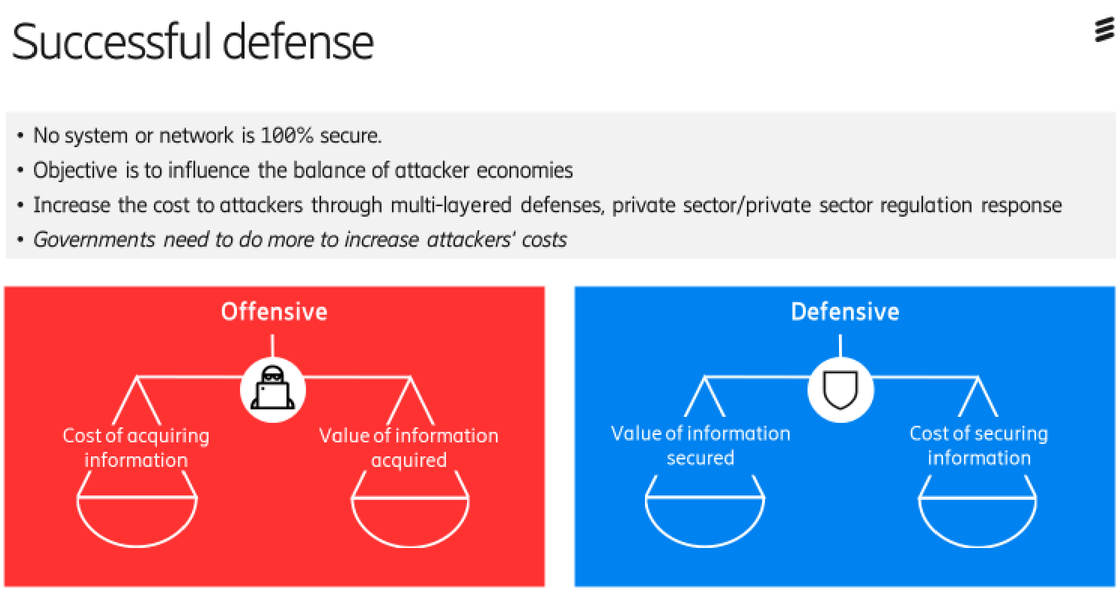


Exhibit 7: Balancing Offensive and Defensive Strategies (source: ERICSSON)

3.4 Network Resilience and Key Developments

Network resilience has several main aspects**:**

- **Architectural**, "resilience by design", the physical and logical layers of the network and their often-underestimated interdependence.
- **Regulatory**, e.g. how to impose obligations on operators to make their networks more resilient.
- **Cybersecurity**, i.e. which attack techniques and surfaces are used by attackers.
- **Technological,** understanding the new risks associated with technological changes (e.g. the widespread deployment of 5G introduced new vulnerabilities in areas like network slicing, IoT/Cloud).

These aspects are at the heart of the relationship between operators, regulators and policy makers.

Key developments with security relevance. The overall risk landscape is very complex, governments often lack information, sometimes not even the operators have complete information.

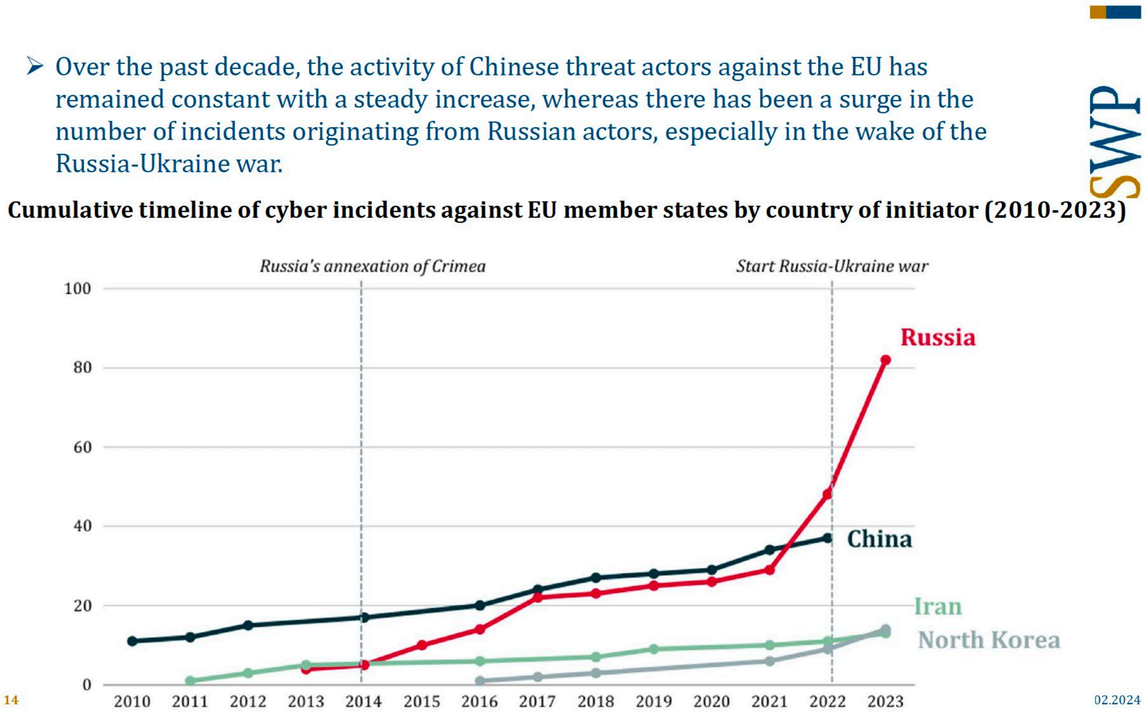


Exhibit 8: Cumulative timeline of cyber incidents against EU member states by country of originator (source: EuRepoC, quoted by SWP)

- **EuRepoC stats** (exhibit 8) **show a global increase in cyber-attacks from 2010 to 2023.**[9] Other attackers, beyond cyber, are coming from different camps, besides criminal actors (copper thieves), radical environmentalists, religious fanatics (both fighting against digitalization and society), political extremists, and acts of sabotage from various players in the value chain. This includes hostile states, state-backed actors and criminal groups (with blurred boundaries between them). They have understood that networks are at the heart of digitalization and our society. **Attacking networks means fighting against the core of society** for political, military, ideological, or religious reasons.
- **Lack of information and lack of transparency**: Digital networks are predominantly in the hands of private companies; they are geographically dispersed and physically difficult to protect. For a long time, governments did not consider digital networks as strategic assets. Governments regarded networks as private assets. But because of their prominent role in a digitized society, networks have become strategic assets.

[9] These number are for EU, but it can be assumed that a similar development can be seen in all countries supporting Ukraine against the Russian aggression.

- After the break-up of the state telecom monopolies, governments lost control of the originally state-owned infrastructures, which were privatized and often ended up outside the view of governments through several rounds of mergers and acquisitions. This is by no means a call for re-nationalization, but rather another example of the **need for a public-private-partnership to secure critical infrastructure**. It is unsurprising that in autocratic systems such as China and Russia, the state exercises a decisive control function over digital (and other critical) infrastructures, but it seems surprising that there is also some control over these infrastructures in democratic systems such as the UK and USA.[10]
    - The UK has partial control via GCHQ.
    - The US has control based on an executive order issued by Donald Trump, which Homeland Security is responsible for implementing.
    - China has done this from the beginning,
    - Russia as well.

- **Public-private-partnerships**: The highly complex and ever-changing threat landscape can only be tackled in cooperation between the private sector and governments and, beyond that, with international cooperation (IT security companies and authorities). Governments will need insight to do their part.

Sub-sea infrastructure: Shallow waters like the Red Sea, Suez Channel and Baltic Sea are highly exposed to underwater sabotage. For more details see section 5.7.

Overall, **the situation has changed significantly since the COVID-19 pandemic;** arson attacks on communication infrastructure (mobile phone masts), which occurred hundreds of times in various countries during the pandemic, are virtually non-existent.[11] Today, however, there are new threats from political extremists, "*Reichsbürger*" and ideologically or religiously motivated activists of various kinds (See also section 5.5.2).

Based on the latest **ENISA report** covering these issues (Telecom Security Incidents 2021), see exhibit 4 below, only 5% of (reported) incidents have been categorized as malicious actions (73 incidents over the course of 11 years).

In the period 2012-2021 nearly two thirds of malicious actions consisted of Denial-of-Service attacks (64%), while the remainder were mainly comprised of lasting damage to physical infrastructure, e.g. arson, cable cuts, etc. Only 4% was attributed to malware and viruses (see exhibit 9, snippet from the ENISA report – 'Figure 23'). This report from 2022 with data up to 2021 shows that physical attacks on the telecommunications infrastructure - although they are very spectacular - recently account for around 10% of all security incidents. Natural events also account for around 10%. This means that attacks and natural disasters together account for around 20% of all network incidents.

[10] Private correspondence, November 2023
[11] During the COVID-19 pandemic, there was a widespread myth - at least in Europe - that 5G "radiation" would transmit the coronavirus. This led to hundreds or more arson attacks against base stations. After the end of the pandemic, this motivation disappeared and with it the arson attacks.

TELECOM SECURITY INCIDENTS 2021
July 2022

Figure 22: Root cause categories - Telecom security incidents in the EU reported over 2012-2021

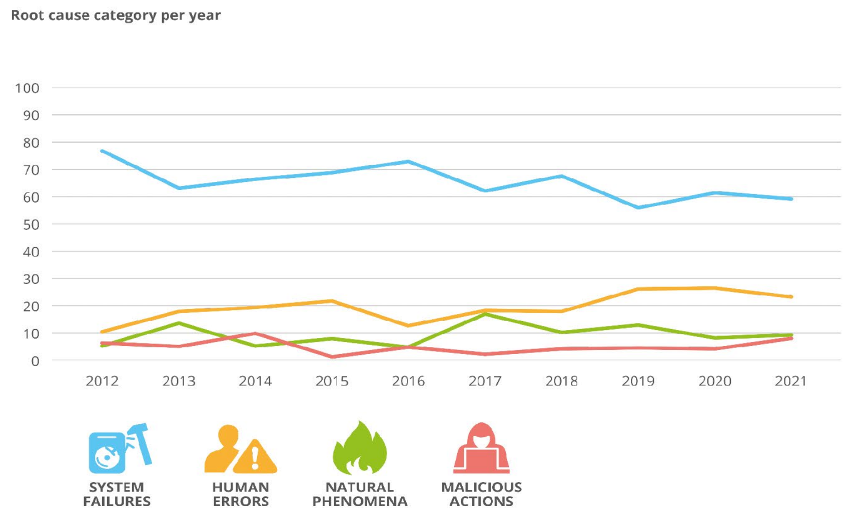


Figure 23: Technical causes for incidents due to malicious actions – Telecom security incidents in the EU reported over 2012-2021

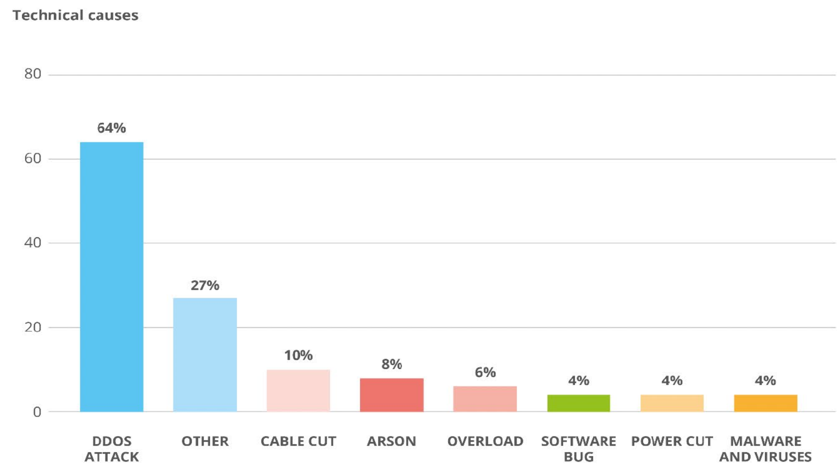


Exhibit 9: Telecom Security Incidents 2021 (source ENISA)

The GSMA Mobile Telecommunications Security Landscape report (chapter 7), 2022 provides significant reporting of both alleged cyber and physical security attacks, directly on critical national infrastructure, including telecommunications providers and on cable and power infrastructure.

Given the lengthy mean-time-to-repair for infrastructure compromises, **resilient network design**, with adequate redundancy and effective pre-emptive physical protection controls, is key to building effective defenses.

According to a European regulator,[12] a significant proportion of "human errors" are hidden system errors, when a faulty system design leads to an overload on the human operator, which in turn leads to errors.

3.5 Useful Definitions and Explainers

3.5.1 Cyber-Attacks and Cyber-Physical attacks

The terms "**cyber-attack**" and "**cyber-physical attack**" refer to different targets and impacts within the domain of cybersecurity. Understanding the distinction between them is crucial for identifying the type of threat and implementing appropriate security measures. Here's a breakdown of the differences:

Cyber Attack:

- **Definition**: A cyber-attack targets computer systems, networks, or devices in the digital realm. The primary objective is to disrupt, disable, steal, or gain unauthorized access to information systems or data.
- **Examples**: Malware infection, ransomware attacks, data breaches, and denial of service (DoS) attacks. These types of attacks aim to compromise the confidentiality, integrity, or availability of data and systems.
- **Impact**: The consequences are typically digital, such as theft of sensitive information (e.g., personal data, intellectual property), disruption of services (e.g., websites going offline), or damage to a company's reputation.

Cyber-Physical Attack:

- **Definition**: A cyber-physical attack specifically targets the computer systems that control physical entities. This type of attack seeks to cause physical harm or disrupt operations of critical infrastructure and physical processes through digital means.
- **Examples**: Compromising the control systems of a power grid to cause outages, manipulating the software of an industrial control system to cause equipment failure, or altering the firmware of medical devices to endanger patient health.
- **Impact**: The consequences extend into the physical world, potentially causing material damage, environmental harm, or endangering human lives. The aim can be to disrupt critical infrastructure (e.g., energy, water, transportation) or to cause physical destruction.

Cyber-physical systems (CPS), such as industrial control systems (ICS), smart grids, and connected medical devices, are particularly vulnerable to cyber-physical attacks due to their critical role in controlling physical processes. Protecting these systems requires a multidisciplinary approach that encompasses both cybersecurity and physical safety measures.

[12] Private correspondence, February 2024.

3.5.2 Hybridisation

"Hybridization" describes a combination of different, temporally and geographically phased attacks that are guided by an overarching strategy in which a broad spectrum of hostile actions at different levels with a high combinatorial effect are deployed to reach the attacker's target. For example, the dragging of an anchor by a ship over almost 200km in an area with sensitive underwater infrastructure, the weaponization of trade, supply chains, raw materials, energy supplies, the manipulation of financial markets and democratic elections through disinformation, the disabling or disruption of vital infrastructure such as navigation systems, satellite communications, etc., are just a few examples. The term also illustrates that the conventional distinction between war and peace as different phases of a political process is outdated and requires new answers.

Recent **examples of Hybridzation** are covered in two articles worth to be mentioned here:

UK's Royal United Services Institute (RUSI) highlighted ("The Threat from Russia's Unconventional Warfare Beyond Ukraine 2022–24") the efforts to which Russia had gone to reconstitute its presence in Europe, often using proxies. Those include members of the Russian diaspora as well as organized crime groups with which the Kremlin has long-standing ties. This report's primary conclusions are that Russia's special services actively seek to expand their capacity in several areas that pose strategic threats to NATO members. **First**, the **GRU is restructuring how it manages the recruitment and training of special forces** troops and is rebuilding the support apparatus to be able to infiltrate **them into European countries. Second**, the **GRU has taken the Wagner Group's functions in house** and is aggressively pursuing the expansion of its partnerships in Africa with the explicit intent to supplant Western partnerships. **Third, the leader of Chechnya, Ramzan Kadyrov, is being used to build a broad network of influence among Chechen and Muslim populations in Europe and the Middle East**, with the aim of contributing to the subversion of Western interests.

An **FT article (5 May 2024) "Russia plotting sabotage across Europe, intelligence agencies warn - Assessments suggest Kremlin agents preparing covert bombings, arson and attacks on infrastructure"** describes a growing number of state-controlled acts of sabotage in Europe. "***As ever with Russia, it's wise not to look for a single explanation of why they are doing anything. There's always a combination of things going on***," said Keir Giles, senior consulting fellow at think-tank Chatham House. "*These pinprick attacks we've seen so far are of course to create disruption, but they can also be used for disinformation. And then there is what Russia learns from these attacks if they want to immobilize Europe for real. They're practice runs*."

3.6 Network Outages

Disruptions to digital systems and network outages are caused by natural and man-made activities, such as cyber-physical attacks, sabotage, etc. However, there is a growing new phenomenon, a gray area between natural and man-made causes, triggered by climate change (as mentioned in 3.2.2). There have always been "natural" reasons for disruptions such as earthquakes, floods, storms, forest fires, etc., but the severity and frequency of most of these disasters is closely linked to climate change. This needs to be differentiated as the causes and prevention are different.

There are many reasons for man-made disruptions, e.g. technical errors in the software or hardware of the network components, or sabotage by criminal or politically/ideologically motivated actors. Natural disasters like earthquakes and volcanic activities can create massive and long-lasting disruptions. In addition, climate change promotes extreme weather conditions and forest fires, landslides and floods, which can damage or destroy infrastructure.

According to a study from the EU Joint Research Center JRC (2017), annual damage to Europe's critical infrastructure could increase ten-fold by the end of the century under business-as-usual scenarios due to climate change alone: from the current EUR 3.4 billion to EUR 34 billion. More recent figures, if available, are expected to be higher.[13] Interestingly, the JRC report is from 2017, and also before that date, no doubt similar estimates existed. But it remains an intriguing phenomenon, that even with events like the flooding in the German Ahrtal Zwei Jahre Ahrtalflut: Schadenregulierung vom Wiederaufbau-Tempo abhängig (gdv.de) little has been done to bring the possible damage of climate-induced risk to a priority level that would make real resilience measures possible. Most of the attention in the debate is devoted to ex-post: repair and reconstruction, and insurance claims. The statistics of the world's largest reinsurers, like Munich Re, Lloyds and Swiss Re speak a very clear language here.

The World Economic Forum (WEF) 2024 risk report uses the Global Risks Perception Survey (GRPS) methodology. It shows the ranking for the shorter term mentions Extreme Weather Events as the #2 risk, where Misinformation is #1. This is clearly linked to social polarization (#3). Cyber is ranked #4 and Interstate conflict #5. But the expectations stretching 10 years, clearly put climate-induced risks on top. In line with the JRC study.

Now why is that? It looks like the 500 people in the GRPS survey and the experts in the WEF panels are well-aware of the facts and the trends sketched in earlier work like the JRC study. But – very human – things/events that are closer and perceived as a direct threat are considered as more urgent (Exhibit 10). Extreme weather events are relevant for both the security and resilience of digital infrastructure.

Seven years have passed since 2017, and in 2024 the can with the greater climate risk will be kicked down the road again. How can this be avoided? One could consider setting up an **International Panel of Experts focused on network resilience** to advise governments based on their own and commissioned research. Major clients and supporters of such a body could include reinsurers like Munich Re, Lloyds and Swiss Re.

[13] More can be found here: https://www.eea.europa.eu/en/topics/in-depth/extreme-weather-floods-droughts-and-heatwaves

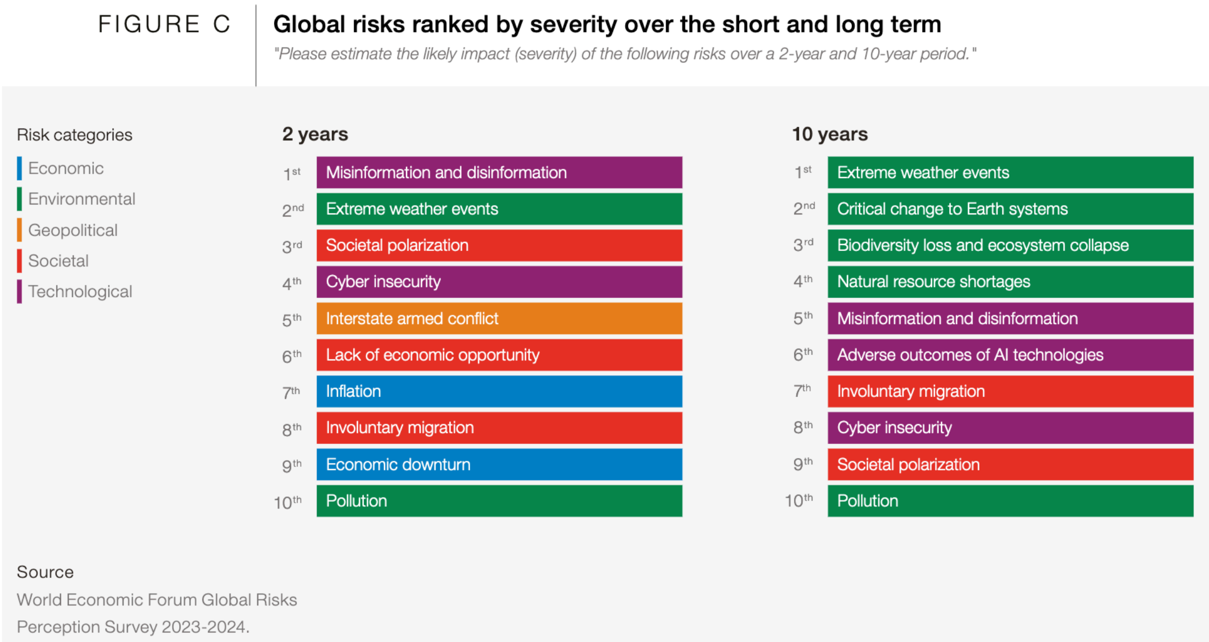


Exhibit 10: Global risks ranked by severity over the short (2 yrs) and long term (10 yrs) (source WEF 2024 Risk Report)

The **reporting obligations of operators in connection with network outages** are gaining more and more attention from regulators and policy makers. For example, "*FCC Requires More Network Outage Reporting After Disasters*" (25 January 2024, Law360).

Recommendation 2 - Setting up an International **Expert panel focused on network resilience: 51**

3.7 Adjacent Threats (Examples)

3.7.1 GPS Sabotage (jamming and spoofing)

Based on reports from several media outlets,[14] a new series of GPS outages in the Baltic Sea region began around Christmas 2023 and continued in 2024. More on these incidents can be found in section 5.6.

3.7.2 Control equipment in electric power grids from "non-like-minded-countries"

Several media outlets[15] reported in December 2023, "*…that UK National Grid has started removing components supplied by a Chinese state-backed company from Britain's electricity*

[14] For example https://cepa.org/article/a-2024-resolution-for-the-west-prepare-for-disaster/ and https://breakingdefense.com/2024/01/as-baltics-see-spike-in-gps-jamming-nato-must-respond/ and https://radionavlab.ae.utexas.edu/wp-content/uploads/clements-direct-geolocation.pdf

[15] For example FT https://on.ft.com/3RMB0h0 and REUTERS https://www.reuters.com/technology/cybersecurity/britains-national-grid-drops-china-based-supplier-over-cyber-security-fears-ft-2023-12-17/

transmission network over cyber security fears, according to two people familiar with the matter. The move by National Grid, which runs the bulk of Britain's electricity grid, came after it sought advice from the National Cyber Security Centre, a branch of signals intelligence agency GCHQ, said one of the people, a Whitehall official. National Grid's decision to terminate its contracts with a UK subsidiary of China's Nari Technology in April 2023 and begin removing components has followed a broader rethink in the west in recent years about Chinese involvement in critical national infrastructure."

A stark warning along the same lines also recently came from the US, as the WSJ reports (31 January 2024): "*Chinese Hacking Against U.S. Infrastructure* [i.e. water, electricity, transportation, etc.] *threatens American Lives*" - U.S. officials say Beijing is preparing to set off potentially damaging cyberattacks in any future conflict, including over Taiwan. Details can be seen in a report from CSIS**,** (Center for Strategic & International Studies, August 11, 2023) "Cyberattack on US Civilian Critical Infrastructures in a Taiwan Scenario."

3.7.3 Threats from IoT devices and Electric Vehicles (EVs)

IoT devices can be found literally "everywhere", in transportation, smart city systems, home and industrial automation, etc. They are often only equipped with rudimentary or dubious security and communicate usually with cloud systems from the country of manufacture, in most cases China. According to an article in The Spectator (May 2023), "*…in January 2023, UK security services took apart a UK government car because data was being transferred via a 'Chinese e-sim' (they meant a cellular module) inside. The government has been tight-lipped about who used the car – or if it ever transported the Prime Minister. But we know from a separate Tesla scandal that it would be perfectly possible for a Chinese engineer to record a private conversation in a car like this with a cellular module.*[16] *Everyone has heard of Huawei and Hikvision, but few know about Quectel, Fibocom or other Chinese producers of cellular IoT modules, even though they represent a far greater threat to free and open countries. No doubt Quectel and others will claim, like Huawei, that they are private companies. But it does not matter: China's security law says that they must hand over data to the organs of state security*."

According to an article in the FT (29 February 2024), the "White House [is] concerned about sensitive data ending up in Beijing's hands as more vehicles hit market - Joe Biden says Chinese smart cars could pose US security threat."

In the **US,** the **Federal Communications Commission (FCC)** in its August 10, 2023, Notice of Proposed Rulemaking (NPRM) on Cybersecurity Labeling for Internet of Things (IoT), seeks input on whether and how the FCC should establish a **cybersecurity certification and labeling program for IoT devices**. According to the NPRM, more than 25 billion connected IoT devices are predicted to be in operation by 2030. The FCC's program is intended to inform consumers about the cybersecurity qualities of the IoT products in the marketplace. In many cases,

[16] Against this background, the decision of the Austrian federal procurement agency BBG to procure Chinese electric vehicles of the BYD brand for members of government, ministries or government-related organizations seems strategically questionable.

devices that do not have a good cybersecurity posture are a threat to their owners and others on the network.

In the EU, the European Cyber Resilience Act (CRA) addresses also the proposed security certification for IoT products and EVs (electric vehicles),[17] however, there are some caveats to this, see chapter 2.

Recommendation 3 - Security certification for IoT devices and EVs (electric vehicles): 51

But **security doesn't come for free**, and we should be prepared to pay a higher price for products with security certification.

3.7.4 Cooperation with research institutions from "not-like-minded-countries"

In the **United States**, several specific regulations govern academic research cooperation in dual-use areas, focusing on the prevention of misuse of research and technology that can be applied for both civilian and military purposes. These regulations are designed to protect national security while fostering innovation and international collaboration. Key regulations include, amongst others (1) Export Administration Regulations (EAR), (2) International Traffic in Arms Regulations (ITAR), (3) Committee on Foreign Investment in the United States (CFIUS), (4) The National Industrial Security Program (NISP) and (5) The Defense Federal Acquisition Regulation Supplement (DFARS). **Summary:** These regulations require researchers and institutions to conduct thorough assessments of their projects and collaborations, obtain necessary licenses, and implement security measures to protect sensitive technologies and information. Compliance is critical, as violations can result in significant penalties, including fines and imprisonment. Institutions often have offices of research compliance or similar bodies to help researchers navigate these requirements and ensure compliance with U.S. laws and regulations regarding dual-use research.

Canada also has a comprehensive framework of regulations and controls for dual-use research and technology, similar in many respects to those in the United States, but with its own specific rules and governing bodies. These regulations aim to prevent the proliferation of weapons of mass destruction (WMD) and the misuse of sensitive technologies, while supporting international trade and academic collaboration. Here's a non-comprehensive overview of the key aspects of Canada's regulatory framework: (1) Export and Import Permits Act (EIPA), (2) Controlled Goods Program (CGP) and (3) Cybersecurity and Information Security.

Canada names 100 Chinese, Russian, Iranian research institutions pose a threat to national security - Canadian researchers partnering with listed institutions won't be eligible for federal funds. Innovation Minister François-Philippe Champagne, Public Safety Minister Dominic LeBlanc and Health Minister Mark Holland said in a joint statement on 16 January

[17] An electric vehicle is often aptly described as a "computer on four wheels".

2024, "*While Canadian-led research is defined by its excellence and collaborative nature, its openness can make it a target for foreign influence, increasing the potential risks for research and development efforts to be misappropriated to the detriment of national security*."

Summary: While the regulatory frameworks in Canada and the U.S. share many similarities, including the goal of preventing the misuse of dual-use technology and supporting international non-proliferation efforts, there are differences in the specific regulations and the administration of these controls. Canadian entities involved in research and development, export, and international collaborations must navigate these regulations to ensure compliance, like their U.S. counterparts. Canada emphasizes a balance between national security, international obligations, and the facilitation of legitimate trade and scientific cooperation.

The geopolitical situation has also led to remarkable changes in the area **of industrial research cooperation**, as the following example show:

According to an article in the Financial Times (10 June 2023), Microsoft is moving some of its best artificial intelligence researchers from China to Canada in a move that threatens to gut an essential training ground for the Asian country's tech talent. The Beijing-based Microsoft Research Asia (MSRA) has begun seeking visas to move top AI experts from China's capital to its institute in Vancouver, said four people with knowledge of he plans. Meanwhile, Experts familiar with the so-called "*Vancouver Plan*" described the move as a reaction to the escalating political tensions between the United States and China. They view it as a defensive move to prevent top talent from being recruited by Chinese tech groups eager for AI researchers who could develop a domestic version of OpenAI's ChatGPT.

There is also growing skepticism in Europe about unrestricted academic cooperation with Chinese research institutions, particularly because all research in the PRC is subordinated to achieving political and military supremacy. Already, early in 2021, the European Commission raised serious concerns "*about intellectual property theft and the authoritarian use of fast-developing technologies, such as AI, by China and other countries*."[18] We must therefore realize that **cooperation with scientists from "non-like-minded-countries"** in the field of basic research in areas with dual-use potential requires a security check according to the applicable criteria. In this context it is helpful, that the European Commission published recently a White Paper to launch a public consultation on the funding of research and development (R&D) at EU level for dual-use technologies.

Basic research with a dual-use potential[19] in **security-critical areas** such as for example **AI and quantum technologies** come increasingly under scrutiny by the European Commission and member states' policy makers and the security apparatus. The reason for this is that (quoting the Think Tank of the European Parliament)[20] "*China's party-led political system does not*

[18] See also https://www.politico.eu/article/commission-to-favor-rd-tie-ups-with-non-like-minded-countries/

[19] On January 24, 2024, the European Commission published a White Paper to launch a public consultation on the funding of research and development (R&D) at EU level for dual-use technologies https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf

[20] https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2023)702592

allow clear distinctions between commercial, political and military interests, often viewing Chinese state and private companies' international activities as instruments helping the Chinese Communist Party (CCP) expand its influence in foreign countries and undermine geopolitical rivals. The CCP's military-civil fusion (MCF) strategy incentivizes civilian actors to contribute to the modernization of the People Liberation Army (PLA) through technology transfer." This is another example that shows that even basic research (at least in certain critical dual-use areas) must be seen in a geopolitical context. For more details see for example the article in the magazine DATUM (published October 2023 in German language), "*China deliberately siphons off knowledge from Austrian universities*". This article takes a critical look at the practice of cooperation with China and Chinese universities and PhD students by Nobel Prize winner Anton Zeilinger.

Swiss universities have developed a more critical attitude. Swiss newspaper NZZ reported (December 2022, in German language) that the prestigious ETH University in Zurich rejects researchers from China due to the risk of espionage. According to Swiss online news portal swissinfo.com (December 2022), Swiss universities are on guard against Chinese espionage. "*The suspicion that Chinese researchers pass on information from the Western scientific world to Beijing has led some Swiss universities to strengthen their cooperation with Switzerland's Federal Intelligence Service, according to the Swiss weekly. Others have scrapped research collaboration efforts. The Chinese law on intelligence clearly states that all citizens must cooperate with the national intelligence service, the newspaper noted. And the researchers most loyal to Beijing typically benefit from grants for stays abroad*."

The **German Academic Exchange Service (DAAD)** has published guidelines for academic cooperation with China in a recommendation paper on 15 January 2024. The DAAD favors a *realpolitik approach*, which also forms the basis of the German government's China strategy.[21] In summary, it can be said that "de-risking" is increasingly becoming the overarching leitmotif for governments and policy makers.

Recommendation 4 - Admission of scientists from non-like-minded countries: 51

3.7.5 Vulnerabilities in medical devices and hospital cybersecurity in the US

A joint research project conducted by Health-ISAC (7 August 2023), Finite State, and Securin unveiled a significant increase in vulnerabilities within medical products and devices, highlighting the urgent need for robust cybersecurity measures in the healthcare sector. The study identified 993 vulnerabilities across 966 medical products, marking a 59% year-over-year increase from 2022. Notably, 160 of these vulnerabilities are weaponized, with 101 trending in the wild, and some are associated with ransomware or being exploited by Advanced Persistent Threat Groups. The rise in firmware vulnerabilities within connected medical products emphasizes the critical need for enhanced software supply chain security to protect patient safety and healthcare operations.

[21] See also https://www.ft.com/content/2e83bd08-90c4-467a-86a4-4db2e31d60de

The FDA has also been proactive in addressing **cybersecurity risks associated with medical devices**. For example, it issued an alert about a cybersecurity risk for the Medtronic MiniMed 600 Series Insulin Pump System, which could potentially be compromised to deliver incorrect insulin doses. Other alerts include vulnerabilities in software like the Illumina NextSeq 550Dx, which could affect patient results and networks, and the PTC Axeda agent and Axeda Desktop Server, used in numerous medical devices with potential for unauthorized access and control.
These **examples underscore the complexity and seriousness of cybersecurity threats in the medical device sector**. Healthcare organizations are advised to prioritize cybersecurity, employ robust practices, conduct regular risk assessments, and stay updated on security threats and technologies to mitigate risks effectively.

Recommendation 5 - Healthcare organizations: 51

4 The Geopolitical Dimension

4.1 The importance of the geopolitical context

The **geopolitical context** is key: These issues are vital to Western countries' security interests and the interdependencies across the newly emerging alliances (see exhibit 11 below) require the assessment and management of security threats in a geopolitical context. Without this context, security risks cannot be adequately addressed.

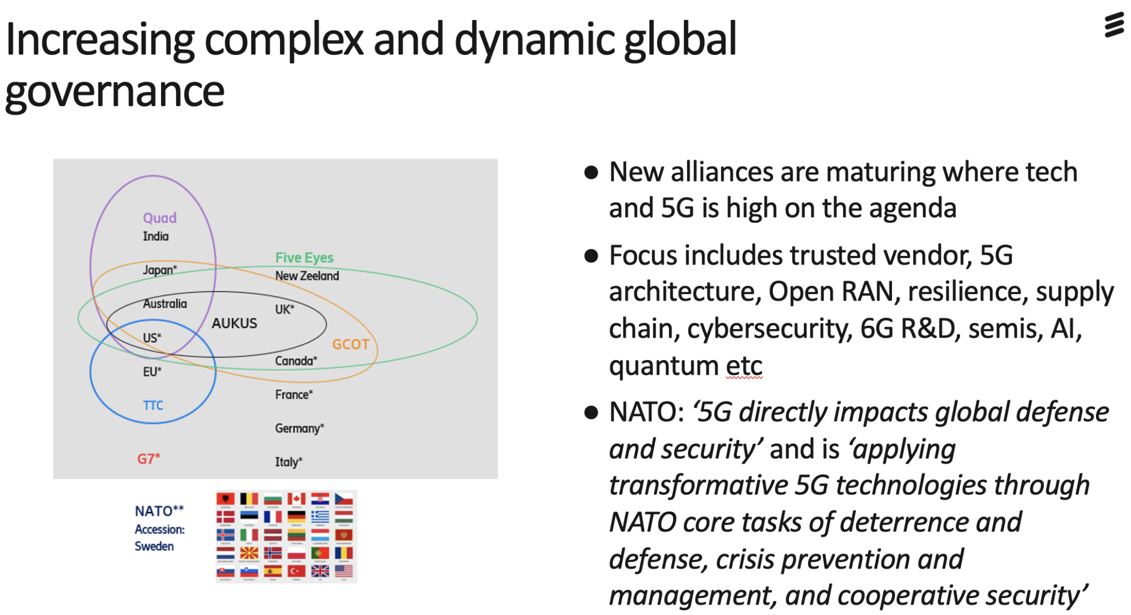


Exhibit 11: Emerging Global Governance Bodies (Source: Ericsson)

The **importance of the geopolitical context** is aptly described by **Paul Tucker**, former central banker and author of the book "Global Discord", in an opinion piece published in the FT on April 25, 2024. Tucker points out that "*Western policymakers ignore changing global power relations at their peril*." And Tucker continues, "*The west's bedrock objective should be to hold on to the distinctive way of life that characterises constitutional democracy. Apart from living by our fundamental norms and so healing our domestic politics, that entails **ensuring the***

resilience of the core systems upon which we rely*; avoiding costly unforced policy errors; and maintaining alliances and friendships around the world*."

There is no better way to express the importance of the geopolitical dimension.

4.2 Emerging Global Governance Bodies

In 2021, the 5G Security Conference was held in Prague, where a strategic paper on vendor diversity was adopted. In September 2023, it became public that an informal group called "Global Coalition on Telecommunications (GCOT)" was founded. USA, UK, Australia, Canada, and – interestingly – Japan are members of this group. GCOT is a new informal multilateral alliance which endeavors to promote international consensus, foster global dialogue, and drive innovation within telecommunications. This statement sets out the GCOT's purpose and the areas of collaboration that the coalition will focus on. It is noteworthy that no EU country is currently a member, although the Prague Declaration is one of the cornerstones of this initiative. According to people familiar with this issue, GCOT is still in an evolving phase.

However, the UK announcement and Japan's participation (with key providers for openRAN like Hitachi and Toshiba), clearly point to a political effort to give openRAN a strategic push. openRAN can well be seen as a driver for vendor diversity.

4.3 Network Security

As the MERICS report (November 2023) shows, hacking has become a standard repertoire with increasingly sophisticated methods and is part of a long-term Chinese strategy to achieve economic, military and political supremacy.

Network security, but also the security of adjacent services based on digital networks, industrial automation, digital health, smart energy, smart agriculture, and smart home with a high proportion of IoT devices at critical points must be managed from this perspective. It should be clear that without a security qualification for such devices, national security can be seriously compromised.

The **Think-Tank of the European Parliament** published in June 2023 a wake-up call on the "Security implications of China-owned critical infrastructure in the European Union". This research demonstrates that traditional approaches to infrastructure protection based on direct ownership are insufficient, since China's party-state can obtain access to critical infrastructure through indirect, equally effective channels. As these cases show, infrastructure protection mechanisms, whose codification and implementation remains incomplete, must be extended to be able to scrutinize the risks that China's leverage over non-science investors and Chinese state-linked contractors pose to the EU's critical infrastructure.

4.4 Critical Minerals

Critical minerals: Even if the issue seems to be somehow off-topic in the context of this paper at first glance, the supply of critical minerals is a very important aspect for the global dimension of the security and resilience of digital systems as they are at the heart of the semiconductor industry. The "de-risking" of the Western digital ecosystem, "decoupling from China" and “friend-shoring” (i.e., the shifting of production to politically friendly countries) are becoming new buzzwords in this debate. China has increasingly weaponized critical global mineral supplies, as part of its hybridization strategy, opening up new opportunities for the Canadian mining industry. In a post by the **China Institute of the University of Alberta**, “Critical Minerals Securitization and Canada’s China Dilemma” the institute points out, that “*Security concerns surrounding China and critical minerals create a dilemma for the Canadian mining sector… To realize these long-term benefits, however, Canada is incentivized to lessen its own dependence on China as a source of capital and expertise, which will create major short- to medium-term challenges for Canadian miners… Demand for Canadian critical minerals is at an unprecedented high, however, to supply those minerals, Canadian mining companies will need access to significant quantities of up-front investment, expertise, and personnel. In the past, Canadian companies have looked to China, which is well positioned to fulfil those needs, however, given energy security considerations, this proposition is made increasingly difficult*.”

4.5 An increasingly critical attitude towards China

There is a huge amount of literature on this subject, which will not be discussed in detail here. The ban on Chinese network equipment (especially Huawei and ZTE) in the US and other members of the "Five-Eyes-Alliance", the increasingly massive restrictions on chip exports to China and the export restrictions on machinery (e.g. ASML) for chip production are one aspect of this development. A report by the EC on China's systematic trade distortions, particularly vis-à-vis Europe, in various key areas is also worthy of note. This report can be seen as the basis for justifying the introduction of tariffs on Chinese imports of Electric Vehicles (EVs) and products related to renewable energy production (solar, wind, storage systems) some of which have given rise to security concerns.

The EC’s Directorate General released on 10 April 2024 a 700-page report on the economic distortions created by the Chinese government. This report has been prepared by the Commission Services for the purpose of the application of the 1994 GATT Anti Dumping Agreement, addressing in particular the so-called *normal value* of goods, to determine (whether there is) dumping, as provided for in EU Regulation (EU) 2016/1036 of 8 June 2016 on protection against dumped imports from countries not members of the EU. This sober report, which updates the 2017 analysis, contains more than 3,500 authoritative references citing official Chinese documents and information from the IMF (International Monetary Fund), OECD (Organization for Economic Cooperation and Development), WTO (World Trade Organization) and other agencies. The report examines China's economic distortions on three specific lines:

- The role of central planning by the CCP and state ownership of enterprises and resources.
- The governance of the production factors land, labor and capital, and
- The control of the industrial sectors of chips, telecommunications, railroads, steel, aluminum, chemicals, ceramics, renewable energies and electric vehicles (EVs).

5 Illustrative Examples and 'Hybridisation'

5.1 South-East Asia

Media outlet ZD-NET reported, that **Singapore reviews ways to boost digital infrastructures after big outage** - Following recent incidents including an hours-long data center outage, Singapore is working on a new bill as part of measures to beef up its digital infrastructures (4 March 2024).

CSIS, the Center for Strategic & International Studies, has published a very revealing report (August 11, 2023) that clearly shows that in order to achieve a specific goal in a region (Taiwan), a wide range of cyber-physical attacks are used against Taiwan's most important supporter (USA) 13,000 km away. (See also info box on "hybridization")**: Cyberattack on US Civilian Critical Infrastructures in a Taiwan Scenario**: "*The primary targets, particularly those that would support U.S. forces in any engagement over Taiwan, are located in the United States.* ***China is engaged in a major cyber reconnaissance effort against them****. If China is willing to accept the risk of broadening a conflict over Taiwan, it may decide that cyber actions against civilian infrastructure in the United States could usefully disrupt communications and the flow of material needed for military operations. The broad calculus for China's decision-making will likely involve weighing the relative military advantage gained from cyberattacks on critical infrastructure against the probability that such attacks would provoke a harsh U.S. response or expand the conflict*." The intent is to disrupt, paralyze, or destroy an opponent's operational capabilities. This makes it likely that China has considered attacks on critical U.S. civilian infrastructure. **The most probable targets fall into three categories**: The **first** would be **electrical power facilities**. The **second** would be the **pipelines and railroads** in the continental United States that connect to these locations. The **third** would be the **logistics and communications networks**, including those that support supply chains for manufacturing precision-guided munitions and military aircraft. Primary targets would include telecommunications systems in cities and regions where naval and air bases are located, such as California, Hawaii, and Washington State.

How digital threats from East Asia are increasing in breadth and effectiveness (Microsoft Security, Oct 05, 2023) The East Asian threat landscape is evolving rapidly, and emerging trends from affiliated threat groups have the potential to impact public and private entities across the globe. **Chinese nation-state groups** are conducting widespread cyber and influence operations (IO), with a particular focus on the South China Sea region. China also continues to target the US defense sector and probe US infrastructure signals in an attempt to gain competitive advantages for its foreign relations and strategic military aims. Lastly, Microsoft has seen China becoming more effective at using IO to engage social media users with content on US elections. **North Korean threat actors** are also stepping up their efforts, demonstrating increased sophistication in their attack capabilities. While North Korea lacks the same level of influence capabilities as China, they have shown a continued interest in intelligence collection and growing tactical abilities to leverage cascading supply chain attacks and cryptocurrency theft. All of these changes have serious geopolitical and financial implications for the global landscape at large.

The Asia-Pacific region was the most targeted for cyber-physical attacks in 2022, accounting for 31% of incidents responded to by IBM's X-Force IR team. The manufacturing sector was particularly affected, being the focus in 58% of incidents, largely due to vulnerabilities in older systems and a low tolerance for operational downtime. Spear phishing was the leading initial access vector, followed by exploitation of public-facing applications. The region also saw a significant impact from extortion and ransomware, emphasizing the critical need for improved cybersecurity defenses.

Newspaper "South China Morning Post" reported (29 April 2023), ahead of the **G7 meeting in 2023, Japan saw an increase in cyberattacks**, including DDoS attacks aimed at disrupting online traffic by overwhelming servers with data. The targets included companies and government offices, highlighting concerns over digital infrastructure security as Japan hosted the summit. Notable targets of these attacks were West Japan Railway and Tokyo Electric Power Company Holding. The **connection with the G7 summit** is another revealing example of **hybridization**.

According to the Cybersecurity Threatscape of Asia Report 2022-2023, government systems in Asia are prime targets due to the valuable information they contain, like citizens' personal data and national importance information. For example, in 2022, a cybercriminal stole a database containing information on 105 million Indonesian citizens from the Indonesian General Election Commission and offered it for sale on the dark web. Furthermore, in July 2023, it was reported that data from over 300 million Indonesian residents were leaked, presumed to come from the *Dukcapil system*, a department responsible for citizens' data management in Indonesia.

5.2 United States

China's cyber army is invading critical U.S. services - A utility in Hawaii, a West Coast port and a pipeline are among the victims in the past year, officials say, according to a report in The Washington Post, December 11, 2023: "*Hackers affiliated with China's People's Liberation Army have burrowed into the computer systems of about two dozen critical entities over the past year, these experts said. The intrusions are part of a broader effort to develop ways to sow panic and chaos or snarl logistics in the event of a U.S.-China conflict in the Pacific, they said. Among the victims are a water utility in Hawaii, a major West Coast port and at least one oil and gas pipeline. The hackers also attempted to break into the operator of Texas's power grid, which operates independently from electrical systems in the rest of the country. Several entities outside the United States, including electric utilities, also have been victimized by the hackers*."

This article is a strong wakeup call for CISOs: **Critical infrastructure attacks aren't all the same: Why it matters to CISOs** (CSO, Feb 22, 2024): "*On the other hand, China's infiltration of Western critical infrastructure is a* ***long-term effort that has involved reconnaissance, gradual intrusion, and cross-infrastructure access compromise over years****. Reporting on Wray* [Christopher Wray, FBI Director] *and Easterly's* [Jen Easterly, the director of the US Cybersecurity and Infrastructure Security Agency (CISA)] *comments to Congress suggest that ongoing PRC-linked intrusions of concern stretch back at least five years. Recent warnings* *don't reflect sudden concern; they are more an assessment of foreign capacity for disruption built on a more holistic compromise of American infrastructures than has previously been seen*."

Chinese Cyber Operation Volt Typhoon Attacks US Critical Infrastructure (SecOps Solutions, 21 March 2024): Of late, Volt Typhoon has been unleashing havoc on different US infrastructure domains and has been causing severe damage and fraught with fear among the digital world players. It has carefully devised a continuous series of cyber-attacks to cripple critical systems such as energy grids, communication networks, and transport. While their techniques are clever and their scope encompassing, they only demonstrate the vulnerability of cyber defenses and the importance of strengthening them. One of the most peculiar stunts Volt Typhoon does is to break in and direct the technical networks governing essential infrastructure spheres, such as control systems of electricity suppliers, mainly based in the US. While their initial focus has been zeroing-in mainly on IT networks, the prospect now is for them to penetrate the physical ICSes, which manage the services that are vital to the world population. Through penetrating these, Volt Typhoon could cut off supply of electricity that is jointly provided by several power utility services providers. This may result in a power outage and citywide chaos.

The well known **Colonial Pipeline hack** in May 2021 is well investigated example for a cyber-physical incident with wide-ranging consequences. More can be found in a recent article published by the Georgetown Environmental Law Review (7 March 2023).

The **SolarWinds hack** was a major cybersecurity event in 2020, not because a single company was breached, but because it triggered a much larger supply chain incident that affected thousands of organizations, including the U.S. government. An article, published by TechTarget on 3 November 2023, explains what happened: SolarWinds is a major software company based in Tulsa, Okla., which provides system management tools for network and infrastructure monitoring, and other technical services to hundreds of thousands of organizations around the world. Among the company's products is an IT performance monitoring system called Orion. As an IT monitoring system, SolarWinds Orion has privileged access to IT systems to obtain log and system performance data. It is that privileged position and its wide deployment that made SolarWinds a lucrative and attractive target.

Recommendation 6 - Analyze incidents through the lens of hybridization: 52

5.3 Czech Republic

The FT reports (5. April 2024), that Russia is trying to sabotage European railways, warns the Czech secret service. Russia has made "thousands" of attempts to interfere with European rail networks in a campaign to destabilize the EU and sabotage critical infrastructure, the Czech Republic's transport minister Martin Kupka has said. He told the Financial Times, Moscow was suspected of having made "thousands of attempts to weaken our systems" since Russian President Vladimir Putin ordered the full-scale invasion of Ukraine in February 2022. The hacking campaign included attacks on signaling systems and on the networks of the Czech national railway operator České dráhy, Kupka said. Past attacks have put ticketing systems out of service and raised concerns about successful interference with signals causing serious accidents.

Keeping in mind, that this is another example of Russia's hybridization to undermine European support for Ukraine, the question arises what can be done against such activities. We argue that outside communication should be **as transparent as possible**, resulting from a detailed analysis of the incident or reverse-engineering of the attack. This helps to reveal the attacker and leaves them no choice but to either admit to the attack or use excuses that are so ridiculous and transparent that any observer can easily see the truth (*"qui s'excuse, s'accuse"*).

Recommendation 7 - Transparent outside communication is crucial: 52

5.4 France

String of attacks on French telecom infrastructure preceded April 2022 attack on fiber optic cables. (CYBERSCOOP, Suzanne Smalley, June 10, 2022). https://cyberscoop.com/attacks-french-telecom-infrastructure-fiber-optic-cables/ (Exhibit 12).

French authorities believe the **fiber optic cable cuts** that disrupted Internet service across large swaths of France in April 2022 were likely the work of **radical ecologists** who oppose the digitalization of society, according to Kave Salamatian, a French academic who specializes in Internet resilience and who said he has been briefed on the investigation by colleagues at the National Cybersecurity Agency of France (ANSSI).

A **new trend is coming from France and Belgium**. **Thieves are stealing emergency power equipment (batteries and solar cells)** from mobile phone base stations from containers that are not adequately protected. This has two consequences: firstly, the loss of expensive equipment and secondly, the non-functioning of the emergency power supply in the event of a power outage. It is important to know that the mobile phone shelters in Belgium and France are usually not secured by an alarm system with a connection to the control center. Stolen batteries and solar cells are usually shipped to Africa.[22]

5.5 Germany

5.5.1 Overview

Extreme climate activists, including some aggressive groups that do not shy away from violence and so-called "*Reichsbürger*", who do not recognize the legitimacy of the German state, attack institutions, facilities, buildings and digital infrastructure in order to draw attention to their concerns. In Germany, a **Center of Excellence** has been set up for this purpose, in which experts from network operators and security authorities are represented. In general, it can be observed that the willingness to use violence is increasing among all groups. In Germany, this has culminated for years in arson attacks on May 1 and throughout the year in certain neighborhoods in Berlin.

[22] Private correspondence, November 2023.

Exhibit 12: Fiber optic cables cut in several locations in France prompting an criminal investigation (Source: CYBERSCOOP)

5.5.2 Examples

But arson attacks on adjacent targets are coming back (exhibit 13). Almost a billion in damage caused by an **arson attack on the power supply of the TESLA factory in Brandenburg/Germany**. The US electric car manufacturer is struggling to restart production (Handelsblatt, 6 March 2024). According to an article (6 March 2024) in the newspaper SPIEGEL, the attacks attributed to the group since 2011 have mostly targeted cable ducts on railroad lines. In some cases, the left-wing extremists also attacked radio masts or data lines, and sometimes even company vehicles. According to the 2019 report by the Berlin Office for the Protection of the Constitution, the "**Vulkan Group**" is said to ***"expose the vulnerability of urban mobility and communication infrastructure, disrupt public order and cause considerable damage to property"*** through acts of sabotage.

October 2022, sabotage against Deutsche Bahn's (railway) fiber optic lines in northern Germany caused a failure of the GSM-R network, a dedicated mobile network based on the GSM standard, maintained specifically for voice, signaling and security communication with trains (not for passengers). Previously unknown perpetrators had cut fiber optic cables at two separate locations in Germany. Investigators stated that these attacks were sufficient to take the GSM-R network infrastructure and backup system offline. The fact that rail communications can be disrupted so quickly raised questions that go far beyond rail transportation: Are critical infrastructure and data networks well enough protected against sabotage? Did Deutsche Bahn make mistakes here? And were the perpetrators possibly rail insiders or foreign intelligence services? (heise online, 8 October 2022 – German language).
https://www.heise.de/news/Sabotage-bei-der-Bahn-Viele-vertrauliche-Infos-sind-offen-zugaenglich-7307277.html

Exhibit 13: Arson attack on the power supply of the TESLA factory in Brandenburg/Germany (source: Handelsblatt, 6 March 2024)

September 2022 Nord Stream pipeline sabotage. On 26 September 2022, a series of clandestine bombings and subsequent underwater gas leaks occurred on the Nord Stream 1 and Nord Stream 2 natural gas pipelines. Both pipelines were built to transport natural gas from Russia to Germany through the Baltic Sea, and are majority owned by the Russian majority state-owned gas company, Gazprom. Three separate investigations were conducted by Denmark, Germany and Sweden.
https://en.wikipedia.org/wiki/2022_Nord_Stream_pipeline_sabotage

Copper theft: **Deutsche Bahn (German Railway)** is currently experiencing major problems with **copper theft** due to the current high price of copper. **Copper theft** plays only a **minor role at Deutsche Telekom,** but a **very significant role at Deutsche Bahn. Copper theft costs millions of dollars every year** for rail network operators across the globe. According to a report from the International Union of Railways (UIC), which is from November 2013, in Germany the state railway (Deutsche Bahn) is using **artificial DNA to mark its infrastructure** to make recovered goods easier to trace. Also, **Deutsche Bahn joined up with leading telecommunications and energy companies** to establish an **association of German metal traders** so that scrap could be more closely monitored. More details can be found here: https://uic.org/security/metal-theft

5.5.3 Reactions and Countermeasures in Germany

A **working group** has been set up at **EUROPOL**, which also includes representatives from Deutsche Bahn and Deutsche Telekom. There is intensive cooperation within the Deutsche Telekom Group and informal exchange with other network operators.

Deutsche Telekom is not protecting its physical infrastructure with special measures because a cost/benefit analysis has shown that the massive hardening of facilities scattered throughout the country would cost considerably more than replacing damaged equipment. Copper theft plays only a minor role at Deutsche Telekom, but a very significant role at Deutsche Bahn.

Media campaigns, especially on social media, have proved very effective as measures against copper thieves. When copper thieves are caught, this is exploited in traditional media and social media with messages such as “we’ve caught you” and has a noticeable preventative effect due to the severe penalties.

Increasing Resilience of Telecommunication Networks in Germany. In 2022, the Federal Network Agency BNetzA published the strategy paper “*Resilience of telecommunications networks*” in collaboration with stakeholders. The positive response to this paper has once again underlined the enormous importance of the topic of resilience in politics as well as in the telecommunications industry. The BNetzA currently prepares a **resilience guide** for small and medium-sized enterprises (SMEs) in particular. The summary of a draft version can be provided on request. It is aimed at a wide range of companies in the telecommunications sector, from large market leaders to small local providers. The guide focuses on the **development of a holistic resilience strategy**. It considers different areas such as infrastructure, technology and human factors, not only to cope with disruptions, but also to enable preventive measures to minimize risk and respond quickly to disruptions. The aim is to support SMEs, city carriers, municipal utilities, TV cable providers and local fiber network operators without critical infrastructure. This guide is intended to offer flexible approaches to identify and implement individual potential for improving resilience.

5.6 GPS Sabotage and how to achieve more resilient Positioning – Navigation – Timing (PNT)

5.6.1 Evidence for GPS sabotage (jamming and spoofing)

Several media outlets[23] reported that an attack against the GPS navigation system in the Baltic area caused massive outages in Sweden and neighboring countries. On 25 and 26 December 2023, parts of the satellite navigation for air traffic and shipping in southern Sweden were knocked out. In addition to Sweden, parts of Finland, Denmark, Germany, Poland and the Baltic countries have been affected. These incidents began around Christmas 2023 and continued in 2024. Russian Foreign Ministry says that its Baltic Fleet's electronic warfare unit trained successfully with 100 soldiers and about 20 military units in Kaliningrad in the days before Christmas. The goal has been to suppress what is called "*enemy navigation and radio communications*".[24] Both civilian and military targets are said to have been included in the exercise.

There is empirical evidence for an increase of GPS (GNSS) spamming and spoofing since 2022 “*Since February 2022, there has been an increase in jamming and or spoofing of global navigation satellite systems (GNSS)*,” the bulletin said.

[23] For example https://www.tellerreport.com/news/2024-01-03-sweden-hit-in-largest-gps-sabotage-in-the-baltic-sea.Hy-qLeI7Oa.html and https://cepa.org/article/a-2024-resolution-for-the-west-prepare-for-disaster/ and https://breakingdefense.com/2024/01/as-baltics-see-spike-in-gps-jamming-nato-must-respond/ and https://radionavlab.ae.utexas.edu/wp-content/uploads/clements-direct-geolocation.pdf

[24] https://nordicreporter.com/2024/01/russia-blamed-for-biggest-gps-sabotage-in-baltic-sea/

According to an article in THE ECONOMIST (November 2023), in which various experts are quoted, the Ukrainian battlefield is showing on a large scale that such incidents are not an isolated phenomenon. Ukraine discovered in March 2023 that its Excalibur GPS-guided shells suddenly started going off-target, thanks to Russian GPS jamming. Something similar started happening to the JDAM-ER guided bombs that America had supplied to the Ukrainian air force, while Ukraine's HIMARS-launched GMLRS long-range rockets also started missing their targets. Little noticed by international observers, the Russian superiority in the field of electronic warfare (EW), an area in which Ukraine is apparently on its own because its Western supporters are unable or unwilling to provide anything comparable, is becoming increasingly apparent. In a LinkedIn blogpost (18 April 2023) "GPS jamming defeating US weapons in Ukraine - Leaked documents", the author of this blogpost highlights, that "*The US Congress has long questioned DoD about its over-reliance on GPS*" whereas "*Russia and China have terrestrial PNT systems that are very difficult to disrupt and do not rely at all on space*."

The website GPSJAM provides a global overview of GPS disruptions daily. As the website indicates, the problem areas for GPS jamming and spoofing are currently around the Baltic Sea, the Black Sea, Arctic region and Middle East. According to this website, currently no GPS jamming activities are observed in North America. See also European Union Aviation safety Agency (EASA) website.

A report from CISCO Talos (4 December 2023), shows another interesting example for the vital role of GPS-timing and time synchronization. As Russia's invasion of Ukraine entered its first winter in late 2022, nearly half of Ukraine's energy infrastructure had been destroyed, leaving millions without power. The resulting energy deficit has exacerbated something that hasn't had much media attention: The effects of electronic GPS jammers affecting vital electrical equipment. Ukraine's high-voltage electricity substations rely on GPS for time synchronization. So, when the GPS is jammed, the stations can't accurately report to power dispatchers on the state of the grid. This complicates efforts to balance loads between different parts of the system, which is necessary to avoid outages and failure — especially during peak demand and surge times. Until recently, there was no solution to this problem.

A recent article in THE ECONOMIST (30 April 2024) on this topic reports on increased incidents in the Baltic region, but with a different explanation of the background: "*European officials familiar with the matter say the jamming is not intended to disrupt civil aviation but likely to protect Russian forces from Ukrainian drone strikes, which are becoming more frequent and ambitious*." However, this explanation ignores the fact that it does pose a threat to civil aviation. It also reinforces our recommendation not to rely solely on GNSS/GPS and to consider other PNT methods.

5.6.2 Methods to increase PNT resilience (examples)

An update from Booz Allen Hamilton on "Assuring Resilient Positioning, Navigation and Timing (PNT)" describes the importance of emerging PNT technologies and methods for **achieving a more resilient PNT**. Nascent space-based and ground-based technologies offer new options to reduce the dependency on PNT information coming solely from GPS, while simultaneously making it more difficult for adversaries to jam or disrupt GPS signals or disable the satellites themselves. A fully integrated PNT system includes for example the extended use of LEO satellites, enhanced Long Range Navigation (eLORAN) to provide a backup to GPS timing, Ring Laser Gyros, quantum-based clocks and combining quantum clocks with inertial sensors.

GPSdome2 is the industry's first high-end anti-jamming and fully retrofit solution tailored for defending manned and unmanned Ground Vehicles, drones and small-med UAVs from jamming attacks. Fully retrofit, it is compatible with almost any GNSS off the shelf receiver. Using up to four off-the-shelf active antennas, with dual-band protection (GPS L1+L2 or GPS L1+Glonass G1) it protects from up to three jamming directions simultaneously in each band. With optional mil-spec compliance, it is the only anti-jamming solution relevant for smaller and lighter platforms. https://infinidome.com/gps-dome-2/

Quantum sensors will start a revolution — if we deploy them right (nature, 24 May 2023) A new way to enhance PNT applications without GPS and similar. Let's not forget that it took 20 years for GPS receivers to go from specialized devices for the military, tech-savvy outdoor people and ship owners to navigation devices for smartphones and cars. Now the quantum community needs to follow similar paths to realize the benefits of suitable quantum sensors.

The **US PNT Advisory Board** recently made three recommendations (1) Quickly prototype a GNSS interference detection and reporting system, (2) Implement an internet-based High Accuracy and Robustness Service (HARS) for GPS, and (3) Relax export controls that currently restrict use of adaptive anti-jam antennas.

These are just a few illustrative examples of alternative methods and not a complete collection of all possibilities to avoid over-reliance on GNSS/GPS as a PNT service.

Recommendation 8 – Avoid over-reliance on GNSS/GPS and deal with emerging PNT technologies: 52

5.7 Challenges for Subsea Infrastructure

5.7.1 Examples of increasing threats to underwater infrastructure

The paper (27 June 2023) The Escalating Global Risk Environment for Submarine Cables is a rich source for outlining the growing and complex threat situation in the underwater sector landscape. The following paragraph provides some telling examples:

Over the last decade, Chinese state-owned or -affiliated enterprises have sought a greater stake in the global submarine cable network, almost certainly increasing China's ability to manipulate, surveil, and interfere with worldwide data flows. "*State actors seeking an espionage edge will almost certainly target the entire submarine cable ecosystem for intelligence collection: landing station infrastructure, the submarine cables themselves, third-party providers, and the hardware and software that knits it all together. Separately, Russia will almost certainly increase its overt and covert mapping of submarine cables, and likely engage in targeted sabotage on land and underwater, to inconvenience western countries, as* *well as determine utility for hybrid warfare applications. China will also very likely continue to probe and disrupt the cables Taiwan relies upon*."[25]

- February 2023: A member of the United Kingdom's Royal United Services Institute claimed Russia is likely developing special-purpose submarines to target submarine cables and other infrastructure.
- February 2023: A joint Dutch Military Intelligence and Security Service-General Intelligence and Security Service report stated Russia is undertaking preparations for sabotaging offshore infrastructure in the North Sea, such as submarine cables, gas pipes, and windmill farms.
- September 2022: A Danish patrol boat identified a Russian naval vessel, which carries a small submersible designed for underwater operations, in the vicinity of the Nord Stream gas pipelines several days before they were destroyed.
- January 2022: The head of the UK's Armed Forces stated, "Russia has grown the capability to put at threat those undersea cables" that represent the "world's real information system".
- January 2022: Norway's government reported that a submarine cable connecting its mainland to the Svalbard archipelago was severed, which law enforcement investigators determined to be the result of "human impact".

5.7.2 International cooperation to better secure subsea infrastructure

Protecting offshore and subsea critical infrastructure requires international cooperation (16 April 2024): The plans come after Belgium, Germany, the UK, the Netherlands, Denmark and Norway signed a declaration beginning of April to share more information about protecting critical assets. Defending that infrastructure had become "*a geopolitical, security and also an economic imperative*", said Tinne van der Straeten, the Belgian energy minister. The plan is for developers of wind farms, subsea cables and gas pipelines to share more data — including video footage and information collected by sensors — with military agencies. The key issues are: establishing what the major threats to energy infrastructure are, what can be done about it and how sensitive data can be shared in real time. It is about establishing a data-sharing network, along with efforts to develop artificial intelligence technology that would evaluate satellite data as well as input from drones and electronic sensors. Belgium could become the first country to formalize this, based on proposals for the auctions of contracts for its new **North Sea energy hub, an artificial island** nicknamed Princess Elizabeth. "*Close co-operation is absolutely needed*." See also https://www.teamjustitie.be/fr/2024/04/09/08-04-pacte-de-securite-pour-la-mer-du-nord-la-belgique-se-joint-a-cinq-pays-riverains-pour-securiser-les-infrastructures-critiques-sous-marines/

The **SWP study** (28 February 2024) Critical infrastructure in the crosshairs: Scope for countermeasures under international law takes a closer look at the **framework conditions under international law** as to which defensive measures are permitted to counter espionage and sabotage off Europe's coasts (in German).

[25] Ibid: https://go.recordedfuture.com/hubfs/reports/ta-2023-0627.pdf

5.7.3 More examples of increasing threats to underwater infrastructure

On 6 February 2024, the **German Institute for International and Security Affairs (SWP)** published a study (in German language) on "Maritime critical infrastructures - strategic importance and suitable protective measures." The authors of the study emphasize, that "*the maritime space is home to a multitude of infrastructures that are of central importance for global energy relations, the network of global trade in food and fertilizers and, finally, the exchange of data on the internet. At the same time, maritime infrastructures will become even more important in the future; it will be necessary to observe which new infrastructures emerge through new uses of maritime space, such as deep-sea mining or carbon storage. Some maritime infrastructures are so important to society that they should be regarded as critical infrastructures and given special protection. The high degree of international networking means that infrastructures on the coast of one country can be of particular importance for the whole of Europe. However, due to global networking, maritime infrastructures in more distant regions are also of critical importance for Europe. To protect maritime infrastructures, the focus should be on resilience and diversification in addition to approaches that target the specific characteristics of individual facilities or sectors. Where this is not possible and the threat from state actors is high, additional military protection measures are required*."

Recommendation 9 – How to protect underwater infrastructure Recommendation 9

Recommendations from SWP and others aim to strengthen the security and resilience of maritime infrastructures to effectively address the diverse and complex threats. Another important finding is that due to the **global nature of maritime infrastructures**, even **countries such as Canada that are geographically far away from the epicenter of a conflict** can be **affected by a disruption of this infrastructure**.

Subsea cables vulnerabilities: According to a report from CSIS ("Invisible and Vital: Undersea Cables and Transatlantic Security") undersea cables have two types of vulnerabilities: physical and digital. However, it should be noted that the most common threat today—responsible for roughly 150 to 200 subsea cable faults every year—is accidental physical damage from commercial fishing and shipping, or even from underwater earthquakes. Industry actors have the prime responsibility for accounting for and mitigating these incidents. Of greater concern are more malicious threats. Regarding physical challenges, the two primary concerns are that the cables might be destroyed or tapped—by either a non-state actor, as per some recent isolated incidents of piracy, or, more likely, by a state adversary like Russia.

There are several conceivable objectives severing a cable might achieve: cutting off military or government communications in the early stages of a conflict, eliminating internet access for a targeted population, sabotaging an economic competitor, or causing economic disruption for geopolitical purposes. Actors could also pursue several or all these objectives simultaneously.

More difficult and subtle than destroying the cables is tapping them to record, copy, and steal data, which would be later collected and analyzed for espionage. It is believed this could be done in one of three ways: inserting backdoors during the cable manufacturing process, targeting onshore landing stations and facilities linking cables to networks on land, or tapping the cables at sea.

The final type of threat is cyber or **network attacks**. By **hacking into the cable network management systems** that private companies use to manage data traffic passing through the cables, malicious actors could disrupt data flows. A "**nightmare scenario**" would involve a hacker gaining control, or administrative rights, of a network management system. At that point, they could discover physical vulnerabilities, disrupt or divert data traffic, or even execute a "kill click" deleting the wavelengths used to transmit data. The potential for sabotage or espionage is quite clear—and according to Lawfare, the security of many of the network management systems is not up to date.

It is positive to note that **awareness of the issue of submarine cable resilience and safety is increasing**. In a "Reflection Paper on Submarine Communication Cables" published on February 1, 2024, ETNO highlights that the European Union's dependence on submarine infrastructure has become a significant problem for Europe's security, resilience and sovereignty, a vulnerability that was underscored by the well-known incidents in Northern Europe in 2022 and 2023. ETNO is tackling the issue of resilience in two directions: **(1) Resilience through funding**: EU funding under the Connecting Europe Facility (CEF) could be extended to support initiatives in this area and mitigate the rising costs that operators are repeatedly confronted with, e.g. in relation to ensuring effective repair and maintenance strategies. **(2) Resilience through governance**: Increased cooperation between public authorities and private entities is essential to ensure the resilience and safety of submarine cables. Cooperation between civil and military actors is also essential. Member States should be encouraged to establish a clear and structured dialog between the private and public sectors to jointly ensure the resilience of submarine cables.

CYBER DEFENSE ACROSS THE OCEAN FLOOR – The Geopolitics of Submarine Cable Security
(Atlantic Council scholar Justin Sherman, 30 September 2022)
https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf

The author of the article emphasizes, that "*Authoritarian regimes, particularly in Beijing and Moscow, will continue funding submarine cable development projects globally, gradually reshaping the Internet's physical topology to encourage Internet traffic to move through their own borders and through other midpoints their security agencies can intercept. And should cables be damaged or disrupted, delayed repairs will undermine Internet traffic delivery because the US government hasn't invested sufficiently, in cooperation with US industry and allies and partners globally, in quickly fixing that infrastructure and restoring the flow of Internet traffic.*"

Submarine Cables and the Risks to Digital Sovereignty (posted 25 January 2024, Luciano Floridi et al.)

The authors addressing the huge importance of submarine infrastructure for Digital Sovereignty: "*The international network of submarine cables plays a crucial role in facilitating global telecommunications connectivity, carrying over 99% of all internet traffic. However, submarine cables raise challenges to digital sovereignty due to their ownership structure, cross-jurisdictional nature, and vulnerabilities to malicious actors. In this article, we assess these challenges, current policy initiatives designed to mitigate them, and the limitations of these initiatives. The nature of submarine cables curtails a state's ability to regulate the infrastructure on which it relies, reduces its data security, and threatens its ability to provide telecommunication services. States currently address these challenges through a combination of regulatory controls over submarine cables and associated companies, investing in the development of additional cable infrastructure, and implementing physical protection measures for the cables themselves. Despite these efforts, the effectiveness of current mechanisms is hindered by significant obstacles arising from technical limitations and a lack of international coordination on regulation. We conclude by noting how these obstacles lead to gaps in states' policies and point towards how they could be improved to create a proactive approach to submarine cable governance that defends states' digital sovereignty*."

5.7.4 Examples: United Kingdom – Spain – United States (quoted from the SWP study)

UK: The study from the SWP on "Maritime Critical Infrastructures" (in German language), describes the UK's approach to protecting maritime critical infrastructure. Ports, ships, marine energy infrastructure such as oil and gas pipelines and submarine cables are considered critical infrastructure in the UK. The National Protective Security Authority (NPSA) (the former Centre for the Protection of National Infrastructure) plays a central role in their protection, carrying out risk assessments and advising both government and industry. In recent years, the government has placed a particular focus on maritime security. The UK National Strategy for Maritime Security 2022 emphasizes improving the protection of maritime infrastructure as a result of the Network and Information Systems Regulations 2018 and provides for a review of regulation to protect submarine cables. In October 2023, Proteus, the Navy's first Multi-Role Ocean Surveillance Ship (MROSS) of the navy was put into service. Another ship is being planned.

Spain's National Security Strategy refers to the relevance of maritime critical infrastructure such as submarine cables, pipelines and ports. Spanish Government, National Security Strategy 2021: A Shared Project, Madrid 2021.
https://www.dsn.gob.es/es/file/7272/download?token=miLM79u6

The **USA** has numerous regulations and measures in place to protect maritime critical infrastructure, including around cybersecurity. See US Department of Homeland Security, The Maritime Infrastructure Recovery Plan, Washington, D.C., April 2006.
https://www.dhs.gov/sites/default/files/publications/HSPD_MIRPPlan_0.pdf
United States White House Office, National Maritime Cybersecurity Plan to the National

Strategy for Maritime Security, Washington, D.C., December 2020, https://www.hsdl.org/c/abstract/?docid=848704

5.8 Nordic Countries and Submarine Infrastructure

Finland's National Risk Assessment 2023 classified submarine cables and maritime transport infrastructure, among other things, as critical to national security of supply. Finland's Ministry of the Interior, National Risk Assessment 2023, Helsinki 2023. https://julkaisut.valtioneuvosto.fi/handle/10024/164629

Several articles dealing with the unprecedented incident in the Baltic Sea on October 8, 2023.

- **Sweden says undersea telecoms link to Estonia damaged** (The Guardian, 17 October 2023). Incident is thought to have coincided with damage to a gas pipeline and a telecom cable connecting Estonia and Finland. https://www.theguardian.com/world/2023/oct/17/telecoms-cable-between-sweden-and-estonia-damaged-sweden-says

- **Estonia believes that damage to a telecommunications cable in the Baltic Sea between Sweden and Estonia is related to damage to a pipeline and cable between Estonia and Finland**, Sweden's government said on Oct 23, according to REUTERS. On Oct. 8 a subsea gas pipeline and telecommunications cable connecting Finland and Estonia were damaged, in what Finnish investigators believe may have been deliberate sabotage. Helsinki is investigating the pipeline incident, while Tallinn is looking into the cable incident. https://www.reuters.com/world/europe/swedish-govt-says-estonia-has-linked-baltic-cable-pipeline-damages-2023-10-23/

- **Damage to gas pipeline, telecom cable connecting Finland and Estonia caused by 'external activity'** (AP News, 10 October 2023). https://apnews.com/article/finland-estonia-pipeline-24d6623cf2778464fdb4ef1d85c70d91

- **Damage on undersea infrastructure connecting Sweden, Finland, and Estonia –** published by https://www.zareepartners.com/ (07 October 2023).

  The incident involving the Chinese cargo ship "NewNew Polarbear", which dragged its anchor along the seabed for 185 kilometers over a crucial area of undersea infrastructure connecting Sweden, Finland, and Estonia, gains further complexity when thinking about the background and owners of the ship.

  Considering the strategic implications of the ship's path over data cables and gas pipelines vital to Nordic countries (see exhibit 14 below), some authorities might view this as more than a mere coincidence, potentially raising suspicions of deliberate sabotage. The ship's ability to maintain speed despite the drag of an anchor could indicate a calculated effort to disrupt undersea infrastructure, a concern that would likely draw the attention of international maritime and security agencies.

Given the strategic nature of the affected infrastructure and the geopolitical context, it's essential for authorities to thoroughly investigate the incident, considering both the ship's origins and ownership structure. This comprehensive approach would help ascertain whether this was a regrettable accident or a calculated act of sabotage, a distinction with significant international ramifications.

Driven for example by these incidents and the overall geopolitical situation, **Nordic and Baltic regulators established a coordination/cooperation platform on network security and resilience**, based on the NATO Seven Baseline Requirements (Chapter 6 of the NATO document, resilient civil communications systems).

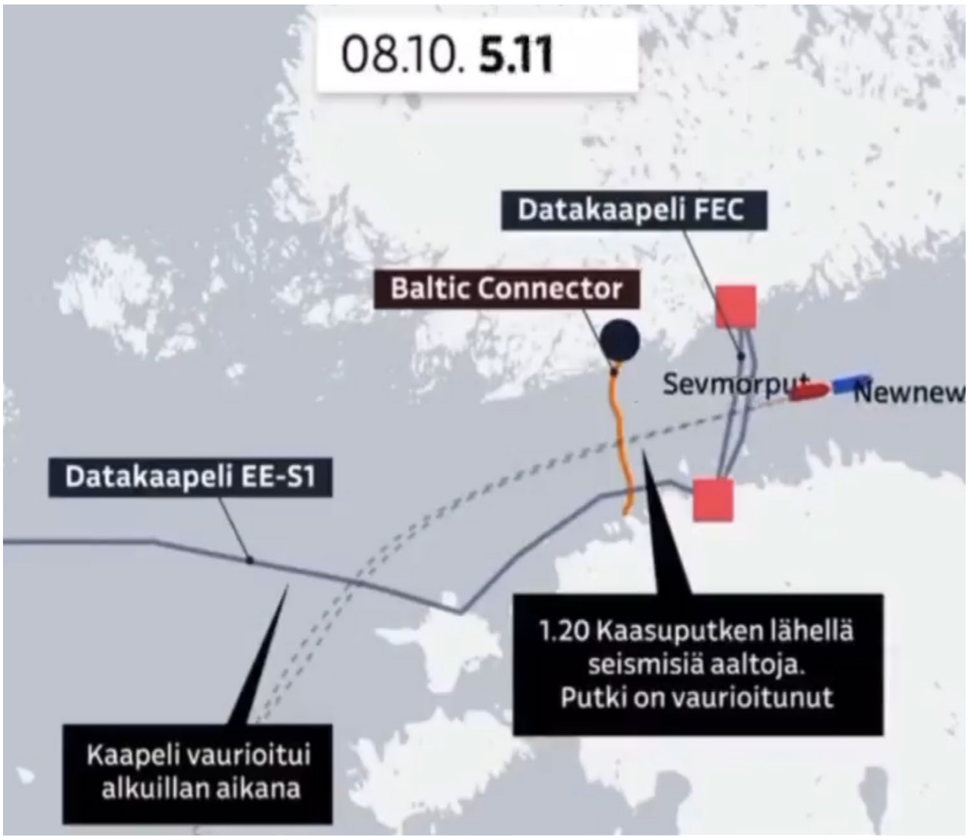


Exhibit 14: Route of the Chinese cargo ship "NewNew Polarbear" over a crucial area of undersea infrastructure connecting Sweden, Finland, and Estonia (Source: Zareepartners[26])

6 Implications on the Governance Structure – Need to act now

6.1 The Challenge

States and international organizations should enhance the security and resilience of the digital infrastructure they rely on to guarantee the security of citizens and the functioning of the society and the economy. They should have both the **ability to act offensively as well as defensively**. In the light of the fact that an increasingly broad range of instruments is deployed to gain the upper hand in conflicts and competition, **new concepts must be developed to deal with the "hybridization" many of the above-mentioned examples illustrate**.

Thinking and policy-making about defense and security should not only cover the traditional military means – i.e. supporting al the 'classical' land, sea, air, space, electronic and cyber capabilities – but increasingly focus on how to make civilian infrastructure more robust. How soon will a modern economy grind to a halt if electronic payments and cash-machines are disrupted? This type of thinking requires a paradigm-shift in the making of security policy that goes beyond increasing the control governments have over critical infrastructure. When the

[26] https://www.linkedin.com/posts/moses-zaree_shippingindustry-geopolitics-scandinavia-ugcPost-7134002841777491968-y8M5/?utm_source=share&utm_medium=member_ios

instruments of conflict and competition permeate the entirety of societal life, in particular as a result of the digitization, society as a whole has to become more able to deal with them.

6.2 The status quo of digital governance appears inadequate

In contrast, the **current regulatory and administrative situation regarding the resilience and security of digital systems and networks** in many countries appears **inadequate** in view of the increasingly complex threat landscape and geopolitical developments. We are not talking here about theoretical dangers, about things that could happen, but about incidents such as those described in the examplesaove , which we encounter constantly and with increasing frequency. We must ask ourselves critically *what would happen if* – as was the case in 2014 with Russia's annexation of Crimea against international law – we did not react sufficiently to the changed and intensified threat landscape.

6.3 New response patterns and governance approaches are emerging to overcome the challenges

As can be seen from the example of the **Dutch government's response**[27] **to recent cybersecurity incident (COATHANGER FortiGate RAT)**, there is obviously a new way in public responses away from "behind closed door" discussions towards a very high degree of transparency and publicizing of incidents, whereby – as can be seen from the latest example from the Netherlands – there is no shying away from a clear attribution of the incidents with an unprecedented great deal of technical detail as evidence for the attribution.[28]
We also consider the **highest possible degree of transparency to be necessary to show the public the extent of the vulnerability of modern society and to raise the willingness to take appropriate measures.** This means the reorganization of the responsibilities and/or authorities internally, the imposition of sanctions externally and to demonstrate their legitimacy. Transparency will also help to strengthen the willingness to cooperate among the authorities, including the willingness of political decision-makers to give the cooperating authorities a stronger mandate.

We do not currently see any dedicated regulatory cooperation models that deal specifically with the issue of resilience and security of digital infrastructure. However, there are some **cooperation models with different levels of maturity or depth of cooperation and different degrees of organization between regulators and other competent authorities** for similar horizontal regulatory problems, some of which are already well developed (in particular the UK model) and can be used as blueprint *mutatis mutandis*:

[27] https://www.reuters.com/technology/cybersecurity/china-cyber-spies-hacked-computers-dutch-defence-ministry-report-2024-02-06/
[28] FortiGate devices were hacked via a vulnerability and parts of the ministry's network were infiltrated. The Dutch government traced the hack in all its technical details, published all the details and thus made it possible to clearly identify the attacker (China). This high level of transparency was a turning point, as the previous policy of discretion was abandoned and everyone could see what had happened.
https://www.theregister.com/2024/02/06/dutch_defense_china_cyberattack/

- **UK**: The Digital Regulation Cooperation Forum (DRCF) brings together four UK regulators to deliver a coherent approach to digital regulation for the benefit of people and businesses online. On 6 February 2024, the DRCF announced, that they are preparing to launch the **DRCF AI and Digital Hub** pilot in the spring 2024. This new Government-funded service will support AI and digital innovators with queries that span regulatory remits. The overall aim of the Hub is to increase innovators' confidence in bringing new AI and digital products safely to market, by helping them understand and navigate regulatory requirements. The DRCF AI and Digital Hub addresses innovators developing a new AI or digital products. Details about the AI and Digital Hub can be found here.
- **GERMANY'S CLUSTER BONN**: Six German regulatory authorities dealing with new digital markets developments created a new cooperation network, called the Digital Cluster Bonn to compare notes on the Digital Markets Act, the Digital Services Act, the Data Act and the AI Act, the regulators said in a joint statement on 15 January 2024. **Six authorities, one common approach:** The network will unite staffers from the Federal Financial Supervisory Authority, the Federal Office of Justice, the Federal Office for Information Security, the Federal Commissioner for Data Protection and Freedom of Information, the Federal Cartel Office and the Federal Network Agency, which regulates telecommunication infrastructures. The regulators signed a memorandum of understanding to commit to exchanging information, setting up working groups, hosting joint events and publishing common position papers.
- **AUSTRALIA**: The Digital Platform Regulators Forum (DP-REG) is an information-sharing and collaboration initiative between Australian independent regulators with a shared goal of ensuring Australia's digital economy is a safe, trusted, fair, innovative and competitive space.

6.4 Establishment of a digital authority with central coordination competence

Various organizational models are conceivable, from loose informal cooperation to a formalized joint platform based on statutory regulations. Jointly organized exercises, joint external communication and jointly supported internal and external transparency lay the foundation for a stronger political mandate. From the developments and perspectives described here, it is becoming increasingly clear that the **setting up of a wide-ranging Digital Authority as a central coordinating body and public think tank** is more effective than incremental small changes here and there.

Exhibit 15 shows a schematic representation of the proposed **key functions of a far-reaching Digital Authority** and how this authority is embedded in the federal government and authority structure:

- Digital strategy development and think-tank for government, combining telecom regulation with innovation policy and industrial policy[29]

[29] We published the concept of combining telecom regulation with innovation policy and industrial policy in detail in the book **"The Changing World of Mobile Communication"** (Chapter 9: "**Toward Anticipatory**

- Information and service for stakeholders
- Digital research coordination and funding
- Regulation and market oversight.

As a starting point for **planning of a governance reform**, we suggest **mapping security and resilience-relevant topics to the existing authority landscape** and developing more in-depth cooperation models and integration models from this (Table 1).

The entire governance setup for digital affairs has grown incrementally in most countries, and new national or supranational laws and regulations are often allocated to existing authorities or ministries, less on the basis of an overarching strategy but more on the basis of day-to-day political opportunities.

The **main reason for establishing a far-reaching Digital Authority as a central coordinating body** is obvious: the security and resilience of digital systems, which are essentially the central nervous system of our society, is too important to be left to the status quo, which in most countries is a fragmented governance landscape, with critical gaps and often overlapping competencies resulting in turf-battles and regulatory uncertainty.

Resilience Tasks/Elements	Institutional Landscape
Digital infrastructure mapping and inventory (overall picture)	Telecom ministry, authorities and regulator
Risk landscape and assessments	All relevant governmental bodies
Redundancy (incentives and obligations)	Telecom ministry, authorities and regulator
Civil protection preparedness	Civil protection ministry/organization/agency
Grid stability and redundancy	Energy ministry, authorities and regulator
Enhancing the role of regulators for inventory and risk assessment	Telecom ministry, authorities and regulator
Climate change induced natural disasters (floods, landslides, wildfires, etc.)	Geo Sphere research and forecasting (geology, geophysics, volcanology, climatology and meteorology)
Natural disasters (earthquakes, volcanic activities, etc.)	Geo Sphere research and forecasting (geology, geophysics, volcanology, climatology and meteorology)
Impact of redundancy on competition	Competition authority
Regulation as a toolset for mitigating risks	Telecom ministry, authorities and regulator
Cyberattacks	Cybersecurity ministry & authorities

Table 1: Illustrative mapping of security and resilient relevant topics to the existing authority landscape.

Regulation and Beyond") in fall 2023. The book is open access and can be downloaded here https://link.springer.com/book/10.1007/978-3-031-33191-6.

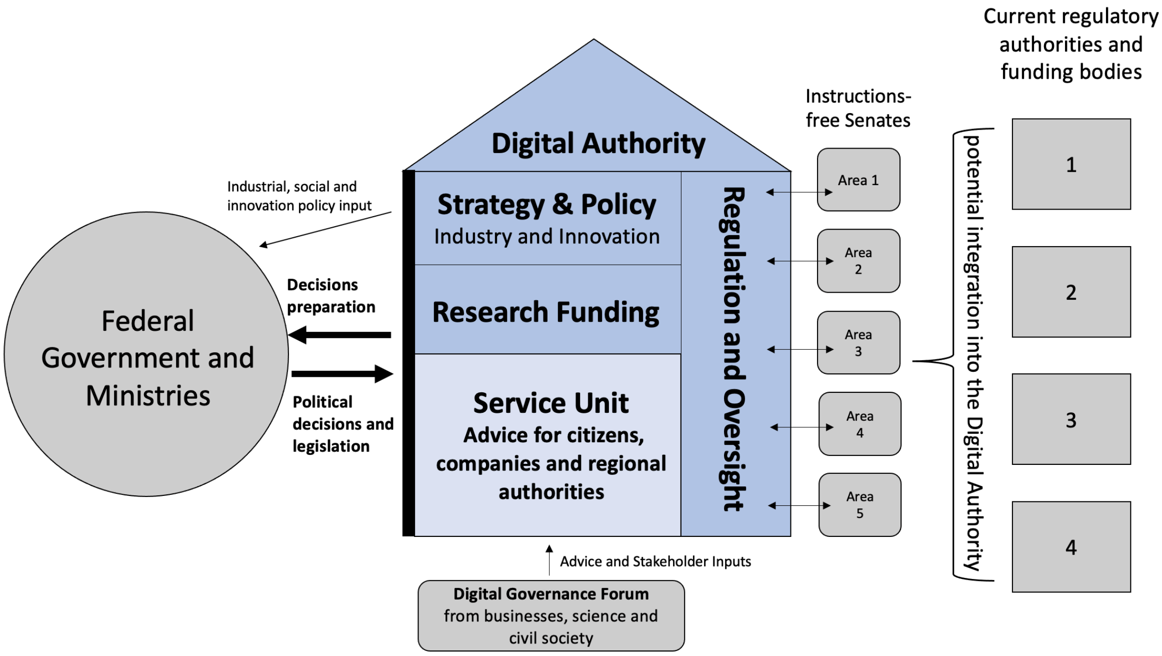


Exhibit 15: Schematic representation of the proposed far-reaching digital authority (Source: own research[30])

Recommendation 10 – Digital Authority - Recommendation 10

From a European perspective, the Strategic Technologies for Europe Platform (STEP) might be used to support the necessary steps towards a more appropriate governance. STEP is the European response to the need to boost investments in critical technologies in Europe. STEP seeks to reinforce, leverage and steer EU funds – existing and new – to investments in deep and digital, clean and bio technologies in the EU, and in people who can implement those technologies into the economy. STEP also introduces the Sovereignty seal – the EU quality label for sovereignty projects. To find all information about existing funding opportunities for STEP investments and relevant contact details of national authorities, visit the dedicated Sovereignty portal.

7 Recommendations

From a **governance perspective and in the organization of authorities**, several measures can be undertaken to increase the resilience of digital infrastructure. Most of them are already implemented in many countries. These measures involve a combination of policy, regulation, coordination, and strategic planning: (1) Fostering a Culture of Cybersecurity Awareness, (2) Establishing Dedicated Cybersecurity Agencies and Formulating Clear Cybersecurity Policies and Legislation, (3) Enhancing International Cooperation, (4) Public-Private Partnerships (PPP), (5) Crisis Management and Response Teams, (6) Legal Framework for Cross-Border Data Flow and Privacy. **States and international organizations should enhance the resilience of**

[30] https://www.serentschy.com/reflections-on-a-digital-policy-and-regulation-under-one-roof/

the digital infrastructure they rely on to guarantee the security of citizens and the functioning of the society and the economy. They should have both the **ability to act offensively as well as defensively**.

A set of **ten key policy recommendations** can be derived from our analysis:

7.1 Recommendation 1

Resilience and security do not come for free: Telecom operators need incentives to invest in redundant infrastructures to increase resilience and consumers need to be aware that the use of security-certified products comes with higher prices for these products. For the credibility of a determined policy, the political level must offer concrete and binding incentives and/or relief for companies and consumers. BACK - Overview

7.2 Recommendation 2

Setting up an E**xpert Panel focused on network resilience** to advise the government based on their own and commissioned research. Major clients and supporters of such a body could include insurers Munich Re, Lloyds and Swiss Re. However, we recommend not waiting for international initiatives, but taking action at national level as quickly as possible. BACK-Network Outages

7.3 Recommendation 3

A **security certification for all IoT devices and EVs (electric vehicles)**, regardless of their origin, should be made mandatory by law. The absence of such a security certification - for whatever reason - can be seen as an attempt to undermine national security. BACK-Threats from IoT devices and Electric Vehicles (EVs)

7.4 Recommendation 4

The **admission of students or scientists from non-like-minded countries** without security clearance in areas with dual-use potential is strongly discouraged. Furthermore, it is recommended to find a careful balance between the demands of national security, international obligations and the facilitation of legitimate trade and scientific cooperation. BACK-Cooperation with research institutions from “not-like-minded-countries”

7.5 Recommendation 5

Healthcare organizations are advised to prioritize cybersecurity, employ robust practices, conduct regular risk assessments, and stay updated on security threats and technologies to mitigate risks effectively. BACK-Vulnerabilities in medical devices and hospital cybersecurity in the US

7.6 Recommendation 6

Looking at an incident in isolation obscures the bigger picture and the effect of hybridization. It is recommended to **analyze incidents for possible further correlations through the lens of hybridization** in order to take effective measures. BACK-United States

7.7 Recommendation 7

More **transparency** seems to be necessary to **show the public the extent of the vulnerability of modern society** and to raise the willingness to take appropriate measures, i.e., reorganization of the responsibilities and/or authorities internally. We opine that the **highest possible level of transparency** resulting from a detailed analysis of the incident or reverse-engineering of the attack exposes the attacker and leaves them no choice but to either admit to the attack or use excuses that are so ridiculous and transparent that any observer can easily see the truth. BACK-Czech Republic

7.8 Recommendation 8

Governments globally (even if currently not affected) should **avoid an over-reliance on GPS and deal with emerging PNT technologies** and methods for achieving a more resilient PNT**.**
BACK-Evidence for GPS sabotage (jamming and spoofing)

7.9 Recommendation 9

Main **recommendations taken from the** [SWP report] on the security and resilience of maritime critical infrastructure include amongst others:

- **Promoting infrastructure diversity** (i.e. higher redundancy) as the most effective means of countering threats and making critical infrastructure less vulnerable.
- **Complementary military protection** against targeted attacks when diversification and resilience alone are not sufficient, in particular through improved intelligence and deterrence. Focus on locations where several critical infrastructures (i.e. multiple cable landing station) come together.
- **International cooperation** to secure maritime critical infrastructures also outside European waters that are important for Europe, for example through strategic dialogs, increased information exchange or joint military measures and exercises.

BACK-More examples of increasing threats to underwater infrastructure

7.10 Recommendation 10

Institutional reform – Digital Authority: Improving the **resilience and security of digital systems** requires a **new form of public-private partnership between governments and the private sector**. Governments cannot tackle these challenges alone, nor can industry. This also has implications for the governance structure for digital affairs. The establishment of a **central coordinating body** is an important step towards overcoming the usual historically fragmented governance structures. To effectively manage the complex new challenges, **we recommend** setting up a **wide-ranging digital authority** as a central coordinating, advisory and decision-making body, while reassessing regulatory priorities, including competition policy aspects where necessary. BACK-Implications on the Governance Structure – Need to act now

8 Acknowledgements

We thank our interviewees from the regulatory community, the security apparatus, policy experts and relevant individuals from industry and academic security experts for their inspiring and insightful insights. Special thanks go to Rene Summer and Gabriel Solomon (both ERICSSON) for useful discussions, our colleagues from the Brown Bag Lunch Group (BBL) for assisting us with sounding-board discussions and Derk Oldenburg and Paul Timmers, who played a key role with many valuable discussions, critical feedback and important contributions.

=== End of Document ===