Digital Infrastructure Resilience and Security
Policy Implications and Mitigation Measures
14 February 2024

Abridged Version

EXPERT REPORT

Dr. Georg Serentschy

Table of Contents

1. Executive Summary and 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, to name only a few impactful factors, have contributed to the growing threats to the security and resilience of digital infrastructures, which represent the central nervous system of our modern societies. These **threats are largely global, affecting all countries regardless of how far they are from the epicenters of the crisis**, and assessing the entire threat landscape requires a holistic geopolitical view.

This document summarizes 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, we reserve the right to amend and revise our analysis and recommendations over time. The aim of this report is to highlight the most important developments and trends in the areas of security and resilience of digital infrastructure, outline approaches to tackling these challenges, characterize institutional and regulatory implications and derive recommendations for future steps based on this analysis.

The **report is based** on numerous **interviews with experts** from the regulatory community, the security apparatus, policy experts and relevant people from industry and academic security experts. For understandable reasons, most of the interviewees asked not to be identified in this report. In addition, **extensive secondary research** was carried out and all information was carefully analyzed by us.

The COVID-19 pandemic, compounded by escalating geopolitical tensions, has placed unprecedented pressure on global networks, posing significant risks to digital infrastructure, cybersecurity, data privacy and the resilience of network systems. 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 subtle 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 report also covers illustrative examples from the energy, industrial automation, and transportation sectors (including navigation), all of which are on the target list of **state (backed) actors** and **extremist groups, aiming to attack core functions and symbols of our society**. As far as **state actors** are concerned, such activities must also be seen as a key element of **hybrid warfare**.

This report also covers examples of **mitigation measures,** illustrative examples of **responses from affected companies and organizations** and **implications for the governance structure.**

An insightful **quote** from one of the interviewees provides a **useful framing**: "*The underlying message conveyed by attacks against infrastructure is the most important thing. Looking at an incident in isolation is not enough and can result in misleading conclusions.*"

2. Overview

The **geopolitical context** is key: The issues addressed in this paper are vital to Western countries' security interests and the interdependencies across the alliances require the assessment and management of security threats in a geopolitical context. Without this context, security risks cannot be adequately addressed.

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 penetrations, 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.[1]

2.1. A Holistic View on Resilience and Security – Role of Regulators

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. In addition to network attacks by threat actors, events caused or amplified by **climate change such as increased wildfires, floods, landslides, etc.** and **natural disasters like tornedoes, earthquakes and volcanic activities**[2] pose an additional threat to the functioning and integrity of the networks. If there is no political ambition to develop and apply a holistic approach, the authorities responsible run the risk of doing nothing more than making small fixes here and there and getting lost in uncoordinated micromanagement.

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, they tend to lack understanding in the geopolitical dimension as well as technical, strategic and cybersecurity

[1] 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

[2] 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/

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.

In contrast, 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. With this, the regulator managed to keep connectivity in the Grindavik region[3] 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, Iceland gives us a preview of what may happen or has already begun in other regions of the world in terms of extreme events induced or intensified by climate change.

Furthermore, it can be said that the **Nordic and Baltic countries**, which face a particular serious threat situation, are all forerunners in this field.

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 the functioning of networks under extreme stress. Every day, new and often unexpected challenges arise for the people in charge, which do not allow them to play always by the rules. The quantity and quality of personnel required to keep the networks up and running 24/7 requires 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 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.

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

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

[3] See footnote 2.

such as network sharing and access to the infrastructure of other operators. Considering the geopolitical situation and the complex threat landscape, regulatory priorities should be reconsidered. We recommend to considering setting up a wide-ranging digital authority a a central coordination and advisory body. To effectively manage the complex new challenges, **we recommend** considering the **establishment of a wide-ranging digital authority** as a central coordinating, advisory and decision-making body, while reassessing regulatory priorities.

2.2. 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 1 below. However, the question remains whether our tools are comprehensive enough to combat the threats effectively. Military doctrine on defense and offense needs to be adapted for the civilian domain to successfully disrupt threat actors and increase their costs. Due to hybrid threats, we are currently in a gray 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.

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 and must bear the consequences of their illegal actions.

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.

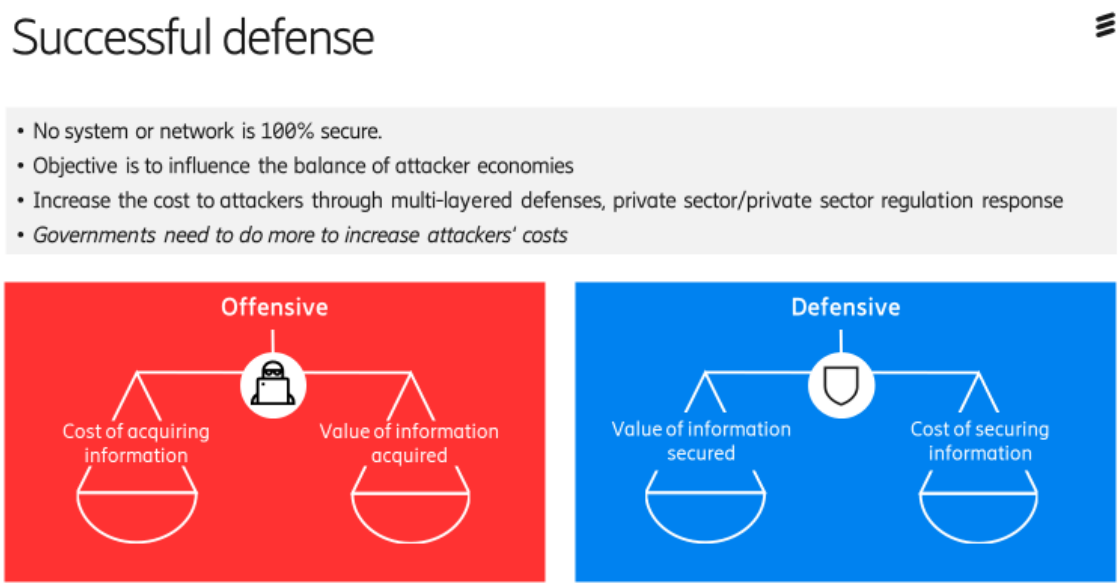

Exhibit 1: Balancing Offensive and Defensive Strategies (source: ERICSSON)

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, states and international organizations.

2.3. 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.

- **A global increase in attacks** (not all of which are reflected in the statistics for various reasons). Attacker 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. Now, governments need to develop a new perspective and find ways to gain control over infrastructure by restoring state oversight.
- In the past, **infrastructures have grown uncontrolled by governments**, which is why it is difficult to regain control over something that governments never had control over (except for former state monopolies?). In most European countries, governments have no control over infrastructures, and sometimes even the operators themselves are only partially aware because assets are transferred after mergers etc.
    - The UK has partial control via GCHQ.
    - The US has control based on an executive order issued by Trump, which Homeland Security is responsible for implementing.
    - China has done this from the beginning,
    - Russia as well.

Sub-sea infrastructure: Shallow waters like the Red Sea, Suez Channel and Baltic Sea are highly exposed to underwater sabotage.
Overall, **the situation has changed significantly since the CV-19 pandemic;** arson attacks on mobile phone masts, which occurred hundreds of times in various countries during the pandemic, are virtually non-existent. Today, however, there are new threats from political extremists, "*Reichsbürger*" and ideologically or religiously motivated activists of various kinds. Based on the latest **ENISA report** covering these issues (Telecom Security Incidents 2021), see exhibit 2 below, only 5% of (reported) incidents have been categorized as malicious actions (73 incidents over the course of 11 years).

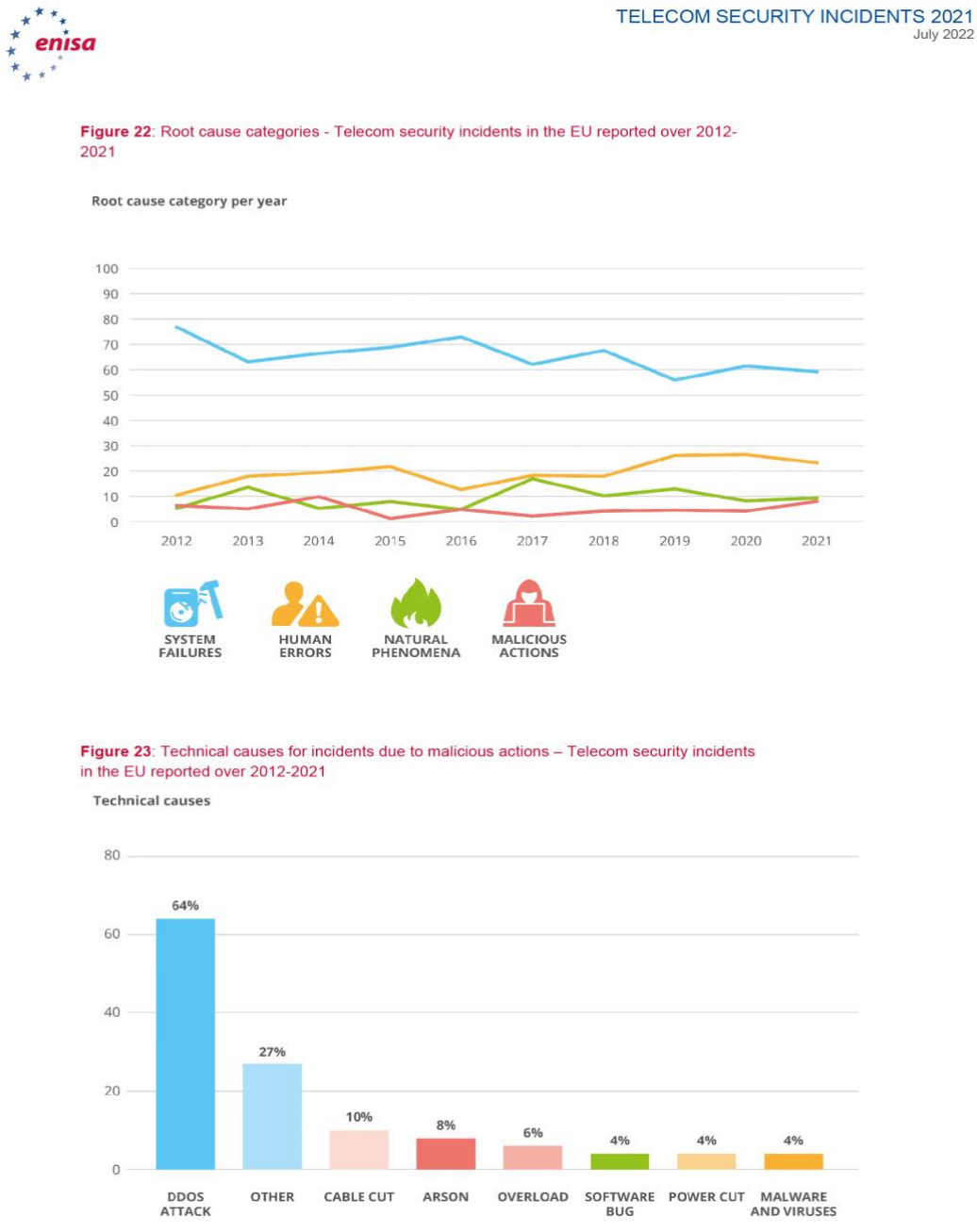

Exhibit 2: Telecom Security Incidents 2021 (source ENISA)

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 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.

According the GSMA Mobile Telecommunications Security Landscape report (chapter 7), 2022 has seen 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,[4] 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.

2.4. Network Outages

More or less massive failures of digital infrastructure occur regularly. There are many reasons for this, e.g. technical errors in the software or hardware of the network components, or sabotage by criminal or politically/ideologically motivated actors. In addition, climate change promotes extreme weather conditions and forest fires, which in turn can damage or destroy infrastructure. Natural disasters like earthquakes and volcanic activities can create massive and long-lasting disruptions. We are observing a steady increase in acts of sabotage and environmental network disruptions. These incidents are relevant for both the security and resilience of digital infrastructure.

The reporting obligations of operators in connection with grid 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).

2.5. Adjacent Threats (Examples)

2.5.1. GPS Sabotage (jamming and spoofing)

Based on reports from several media outlets,[5] a new series of GPS failures in the Baltic Sea region began around Christmas 2023 and continued in January 2024. More on these incidents can be found in Chapter 4.

2.5.2. Removal of Chinese equipment in electric power grids

[4] Private correspondence, February 2024.
[5] 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

Several media outlets[6] reported in December 2023, "*…that UK National Grid has started removing components supplied by a Chinese state-backed company from Britain's electricity 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.

2.5.3. Threats from IoT devices and 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.[7] 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*."

Recommendation: From a European perspective, a **security qualification for all IoT devices and EVs (electric vehicles)**[8], regardless of their origin, should be made mandatory by (European) law. The absence of such a security qualification - for whatever reason - can be seen as an attempt to undermine national security. But security doesn't come for free, and we should be prepared to pay a higher price for products with security qualification.

[6] 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/

[7] 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-affiliated organizations appears to be questionable.

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

2.5.4. Cooperation with Chinese research institutions

Basic research with a dual-use potential[9] in **security-critical areas** such as for example **AI and quantum technologies** come also increasingly under scrutiny by the European Commission and member states' policy makers and the security apparatus because (quoting the Think Tank of the European Parliament) [10] "*China's party-led political system does not 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.[11] In summary, it can be said that "de-risking" is increasingly becoming the overarching leitmotif for governments and policy makers.

Recommendation: 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*." 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

[9] 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
[10] https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2023)702592
[11] See also https://www.ft.com/content/2e83bd08-90c4-467a-86a4-4db2e31d60de

consultation on the funding of research and development (R&D) at EU level for dual-use technologies.

3. The Geopolitical Dimension

The **geopolitical context** is key: These issues are vital to Western countries' security interests and the interdependencies across the newly emerging alliances (see exhibit 3 below) require the assessment and management of security threats in a geopolitical context. Without this context, security risks cannot be adequately addressed.

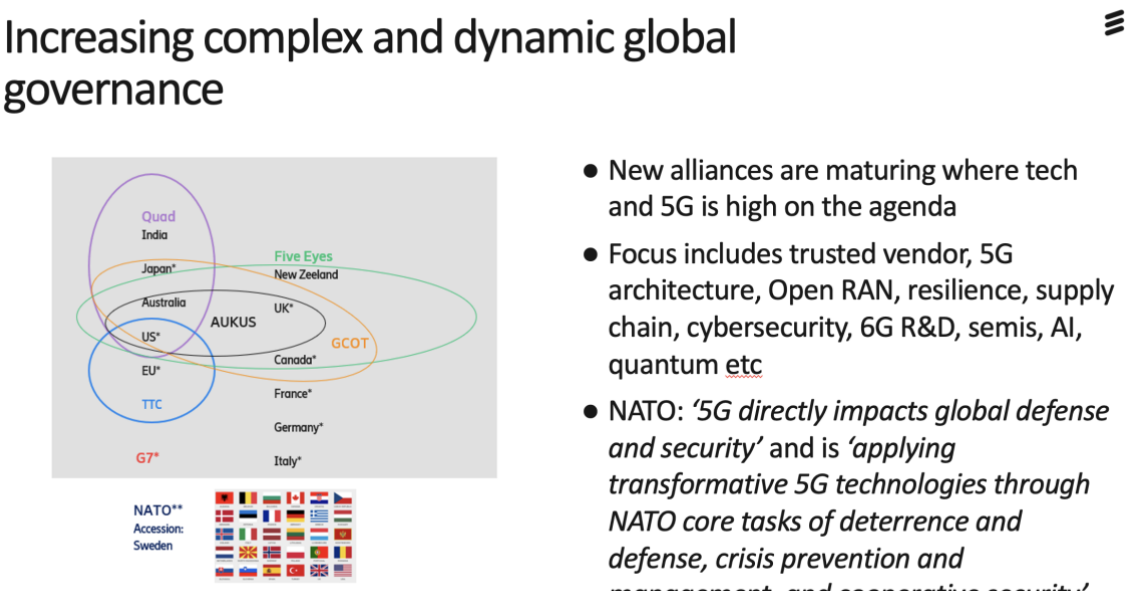

Exhibit 3: Emerging Global Governance Bodies (Source: Ericsson)

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 – surprisingly – Japan are members of this group. Interestingly, currently no EU country is 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 companies 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.

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. Illustrative Examples (February 2024)

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

This part is not included in this abridged version - further details can be made available on request.

4.2. France

This part is not included in this abridged version - further details can be made available on request.

4.3. Challenges for Subsea Infrastructure

4.3.1. Literature Examples

This part is not included in this abridged version - further details can be made available on request.

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

This part is not included in this abridged version - further details can be made available on request.

4.4. Nordic Countries and Submarine Infrastructure

This part is not included in this abridged version - further details can be made available on request.

4.5. Germany

4.5.1. Overview

This part is not included in this abridged version - further details can be made available on request.

4.5.2. Examples

This part is not included in this abridged version - further details can be made available on request.

4.5.3. Reactions and Countermeasures in Germany

This part is not included in this abridged version - further details can be made available on request.

5. Implications on the Governance Structure – Need to act now

States and international organizations should enhance the 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 instruments of conflict and competition perspire 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.

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. This is not about theoretical threats, but about clear evidence. We must ask ourselves critically what would happen if – as was the case in 2014 with Russia's unlawful annexation of Crimea – we did not react sufficiently to the changed and intensified threat landscape.

As can be seen from the example of the **Dutch government's response** [12] **to recent cybersecurity incident (COATHANGER FortiGate RAT)**, there is obviously a new trend 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

[12] https://www.reuters.com/technology/cybersecurity/china-cyber-spies-hacked-computers-dutch-defence-ministry-report-2024-02-06/

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.[13]

We also consider the **highest possible degree of transparency to be necessary to show the public the extent of our vulnerability and to raise the willingness to take appropriate measures**, i.e., reorganization of the responsibilities and/or authorities internally and 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 to give the cooperating authorities a stronger political 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*:

- **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 (groan), 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.

[13] https://www.theregister.com/2024/02/06/dutch_defense_china_cyberattack/

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.

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).

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.

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.

6. 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) Establishing Dedicated Cybersecurity Agencies and Formulating Clear Cybersecurity Policies and Legislation, (2) Enhancing International Cooperation, (3) Public-Private Partnerships (PPP), (4) Fostering a Culture of Cybersecurity Awareness, (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 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 **seven key policy recommendations** can be extracted from our analysis:

1. The **geopolitical context** is key: The issues addressed in this paper are vital to Western countries' security interests and the interdependencies across the alliances 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. **Geopolitical thinking** for all actors involved should serve as a guiding principle for strategy development and execution.

2. **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 mainstream measures such as network sharing and access to the infrastructure of other operators. Considering the geopolitical situation and the complex threat landscape, regulatory priorities should be reconsidered.

3. **Institutional reform – Digital Authority**: 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.

4. More **transparency** seems to be necessary to **show the public the extent of our vulnerability** and to raise the willingness to take appropriate measures, i.e., reorganization of the responsibilities and/or authorities internally and 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 to give the cooperating authorities a stronger political mandate.

5. A **security qualification 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.

6. **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.

7. **Cooperation with scientists from "non-like-minded-countries"** in particular in the field of basic research in areas with dual-use potential like AI and quantum requires a mandatory security check according to the applicable criteria.

7. 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 my colleagues from the Brown Bag Lunch Group (BBL) Derk Oldenburg and Paul Timmers, who played a key role with many valuable discussions and contributions.

=== End of Document ===