EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors

Follow up to the Council Conclusions on the EU's Cyber Posture of 23 May 2022 and Council Conclusions on the EU Policy on Cyber Defence of 22 May 2023

NIS COOPERATION GROUP

Executive summary

The Council, in its May 2022 Conclusions on the EU's cyber posture, requested the Commission, the High Representative, and the NIS Cooperation Group (NIS CG) to carry out a risk evaluation and develop risk scenarios from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries. It was decided to focus this report on two sectors: telecommunications (mobile networks, fixed networks, satellite, and core internet infrastructure) and electricity (including gas to the extent it supports the generation of electricity).

Dependencies on critical components from third countries and supply chain-related vulnerabilities are a particular risk for both sectors. Many specific components have limited suppliers based outside the EU which may be considered high-risk due to susceptibility to government interference without adequate legal or judicial constraints. Moreover, the increasing importance of renewable energy sources, such as wind and solar power, introduces many new - and often less secure - digital technologies into energy networks critical to society. The EU's cyber posture would greatly benefit from further research on potential security measures.

For the telecommunications sector, the top risks identified are risks to mobile and fixed telecommunications networks, risks to the internet's core infrastructure and risks to the satellite communications. The enormous databases of sensitive information held by the mobile subsector are a major target for ransomware. The unavailability of communication sector services caused by ransomware and destructive malware carries large potential for spillover harm into other sectors. Moreover, the risk of disruption is heightened in areas where a telecommunications operator is the sole provider for critical entities or in a particular region. The risk of espionage resulting from infiltration of malicious insiders, or from hostile third countries exercising pressure on 5G suppliers to facilitate cyberattacks scores equally likely, though its impact is much harder to assess. Vulnerabilities in roaming infrastructure can be exploited to geolocate users, intercept calls and SMS messages, while smishing (using deceptive text messages) and vishing (using voice and telephone technologies) attacks can be used to harvest credentials and gain access to critical systems. Unpatched devices used to connect to the Internet are susceptible to compromise and can be used as part of botnets controlled by malicious actors. For core Internet infrastructure, including the around 200 undersea cables around the world, physical sabotage is the most salient risk. The highest risk concerning satellite networks is signals jamming, due to its low cost and the ease with which it can be orchestrated.

For the electricity sector, the highest identified risks concern entities directly connected to the electricity grid (including gas infrastructure). The most salient threats are insiders who either work for hostile actors and infiltrate organisations, or are manipulated via social engineering, along with cyberattacks from the outside, where ransomware and malware are used to gain control over, or otherwise disrupt, operational technology relied on by gas producers and electricity generators. Additionally, espionage is an important risk for the energy sector, for two reasons: first, there are large amounts of sensitive intellectual property in the sector and, second, the sector attracts considerable pre-positioning activity by advanced threat actors with the aim of later executing destructive attacks.

Ten risk scenarios have been developed for use in both EU and national risk preparedness exercises on the basis of the results. The scenarios reflect the most salient risks across a wide range of subsectors and are designed to stress test current preparedness measures.

The conclusions include 17 suggestions over four areas of improvement for the civilian electricity and telecommunications sectors' overall cybersecurity posture and resilience, collective intelligence, cross-sectoral crisis management and follow-up risk assessments. They take into account recent policy and legislative developments: notably, the adoption of the Cyber Resilience Act will create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle.

Member States and cyber networks are recommended to take this report into account when organising their future risk preparedness exercises. This includes any national and EU-level risk assessments, as well as organisational readiness exercises and stress testing of critical infrastructures in the electricity and/or telecommunications sectors.

Table of contents

1. Introduction

This report presents a risk evaluation and risk scenarios from a cybersecurity perspective with reference to the telecommunications and electricity sectors. It has been prepared at the request of the Council by services of the European Commission and the NIS Cooperation Group, with regular consultations of the European External Action Service, and includes input from relevant bodies, agencies and networks.

1.1 Request for this report from Council

The Council, in its Conclusions on the development of the European Union's cyber posture of 23 May 2022 'invite[d] the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe[1], to conduct a risk evaluation and build risk scenarios from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries and present them to the relevant Council bodies.' Subsequently, in its 23 May 2023 Conclusions on the EU Policy on Cyber Defence, the Council 'invite[d] [the Member States and EU institutions, bodies and agencies] to ensure that risk evaluations, scenarios and subsequent recommendations are taken into account when defining and prioritising measures and support, at EU and where appropriate national level'. The Council furthermore calls for 'the risk scenarios to be considered by all relevant actors in risk assessment processes, as well as in the development of cyber exercises'.

1.2 Scope

At the request of the NIS Cooperation Group, it was agreed to put the initial focus for this exercise on the civilian sectors with a high degree of interdependency and criticality for society and the economy, namely:

- telecommunications (mobile networks, fixed networks, satellite and core internet infrastructure); and
- electricity, including gas to the extent it supports the production of electricity.

Further sectors will be addressed in future iterations of this exercise.

[1] The European cyber crisis liaison organisation network established under the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

1.3 Relationship to related exercises

Risk assessments and evaluations are important factors for shared situational awareness, preparedness and ensuring resilience of critical infrastructure. A list of related exercises is found in Annex 1.

This report takes into account and complements several similar but parallel exercises with different scopes and objectives. It incorporates and summarises relevant existing material and supplements it with further input gathered from the Member States and entities in accordance with the Council conclusions. With respect to the telecommunications evaluation, much information contained in this report had been already supplied by Member States as part of the 'Nevers call' risk assessment requested by EU Telecoms Ministers in March 2022[2] and which was published by the NIS Cooperation Group in February 2024[3]. With respect to the electricity sector, some analysis has been incorporated from the national risk preparedness plans in the electricity sector by national competent authorities, which had been mandated by the 2019 Regulation on risk-preparedness in the electricity sector[4].

This report aims to provide for an EU-level overview of the cybersecurity risks for the telecommunications and electricity sectors and their interdependencies with each other and with other sectors. The scope of this evaluation is broader and at a higher level than the Nevers exercise, incorporating the comparative risks of signals jamming, physical sabotage and elaborating upon spillover effects between the telecommunications and electricity sectors. While the Nevers exercise addresses a larger number of detailed scenarios and recommendations for risk mitigation in the telecommunications sector, this report takes a wider approach regarding the types of risks included and draws strategic conclusions on how better to prepare for those scenarios. In addition, this report aims to lay the foundation for a standardised approach to EU cybersecurity risk assessments and scenario-building to align any similar future assessments, and to guide the formulation of the target risk scenarios.

An overview comparing what is contained in the various risk assessment exercises is provided in the table below.

[2] Informal Meeting of the Telecommunications Ministers (2022) *Nevers Call to Reinforce the EU's Cybersecurity Capabilities*. https://presse.economie.gouv.fr/download?id=92155&pn=2131%20-%20Joint%20call%20to%20reinforce%20the%20EUs%20cybersecurity%20capabilities-pdf

[3] NIS Cooperation Group (2024) *Cybersecurity and resiliency of Europe's communications infrastructures and networks.* https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

[4] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (Text with EEA relevance.)

	Requested by	Contributors to exercise	In Scope	Out of scope	Risk scenarios	Recommendations
Cyber posture (telecoms and electricity)	Council	Commission, EUIBAs[5], NIS CG, relevant civilian and military bodies and networks including CyCLoNe	Cybersecurity risk of attacks on Member State or partner country.	Non-intentional damage	Strategic risk scenarios based on sector-neutral methodology	Overall areas for improvement in the EU's cyber posture
Nevers (telecommunications)	Informal Council meeting of Telecommunications Ministers	Commission, NIS CG, BEREC[6], ENISA[7]	Risk of cyber-attacks on EU's communications networks and infrastructures by a hostile third country, organised crime and pro-state hacktivists.	Accidental damage Non-man-made threats Purely financially motivated attacks	Detailed risk scenarios	Strategic and technical recommendations to mitigate the specific risks in telecoms sector
National electricity risk preparedness plans	Required under Regulation (EU) 2019/941	Competent national electricity authorities	National electricity crisis scenarios including caused by cyberattacks	Detailed cyber risk assessment	National risk scenarios of a successful attack on the electricity sector	None at EU level

1.4 Methodology

This report is based on the results analysis of inputs received from Member States' representatives in the NIS Cooperation Group, and relevant EU institutions, bodies and agencies. It was conducted by Directorate-General for Communications Networks, Content and Technology (DG Connect) and the NIS Cooperation Group, with the assistance of ENISA. The evaluation

[5] EU institutions, bodies and agencies.
[6] The Body of European Regulators for Electronic Communications.
[7] The European Union Agency for Cybersecurity.

identifies the main cybersecurity risks for the EU's telecommunications and electricity sector and interdependencies between those two sectors and between them and other sectors, in particular those of a cross-border nature. The telecommunications sector evaluation builds on the Nevers risk assessment and incorporates information collected as part of this assessment.

Commission services, Member States and ENISA analysed the evaluation results during a workshop and follow-up discussions. Ten risk scenarios were developed for use in both EU and national risk preparedness exercises. The scenarios are based on the highest-ranking risks identified in the evaluation, including the most plausible elements in terms of threat actors, threats, vulnerabilities, assets, and types of (spillover) harms. In doing so, less likely, or less impactful scenarios were excluded. In the final stage, Member States discussed and agreed on a common set of recommendations.

This report aims to represent the current state of sectorial risks at the EU level. In addition, Member State contexts and priorities may differ from the aggregated perspectives indicated in the report.

1.5 Structure of this report

Section 2 provides an overview of the overall threat landscape as well as of the sector-specific threat landscapes and considerations for the electricity and telecommunications sectors, providing the background against which this risk assessment has been conducted.

Section 3 presents the risk evaluation, ranking risks based on both the quantitative and qualitative data derived from the input received.

Section 4 presents risk scenarios for use in future risk preparedness exercises. The scenarios reflect the risk evaluation in section 3 and are formed of building blocks (threat actors, threats, assets, vulnerabilities and harms) described in Annex 2.

Section 5 contains conclusions for areas of improvement regarding the scenarios in section 4.

2. Context of the risk evaluation

2.1 Threat landscape

This section gives a broader overview of threat landscapes underlying the risk evaluation, including information on factors, key drivers or trends, based on the latest analyses.

The cybersecurity threat landscape increasingly mirrors global geopolitical tensions[8]. In addition to traditional and long-established cyber-espionage campaigns by nation-states, attempts to disrupt and even destroy targets in a wide area of government and private activities are increasingly observed. Russia's ongoing war of aggression against Ukraine has been

[8] For further information on this section, see: ENISA (2023) *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

accompanied by malicious activities against Ukraine's critical infrastructure, whereas the conflict in the Middle East since the attack on Israel by Hamas in October 2023 has been accompanied by cyberattacks by pro-Hamas hacktivist groups on Israeli targets, mostly in the form of distributed denial of service (DDoS) attacks and website defacements. Moreover, cyberattacks by state-sponsored actors are often accompanied by disinformation campaigns.[9] While spillover from the Middle East conflict has been limited, a great variety of entities across various sectors in the EU have been targeted on a regular basis by pro-Russian actors in retaliation for the provision of material support to Ukraine.

Threat actors are increasing their capabilities, dedicating more resources to researching and discovering new vulnerabilities and developing new exploits. Of particular interest are zero-day vulnerabilities, that is, vulnerabilities that have been disclosed, but not yet patched, and which have increased considerably since 2020.[10] Additionally, black market sellers are making such new vulnerabilities and exploits more widely accessible and the 'hacker-as-a-service' business model is gaining further traction and continues to lower the skill levels required to execute cyber-attacks.

Supply chain risks are particularly pertinent to cybersecurity in the electricity and telecommunications sectors due to the intricate and interconnected nature of these industries. Both sectors heavily rely on a complex network of suppliers, vendors, and service providers to ensure the smooth functioning of their critical infrastructure. Any compromise in the supply chain, whether intentional or unintentional, can have profound implications for the security of the entire system. Cyberattacks targeting the supply chain can result in the introduction of malicious hardware, firmware, or software components, posing significant threats to the integrity, confidentiality and availability of sensitive data and critical operations. How essential electricity and telecommunications are to society, including emergency services, healthcare and national security, the potential consequences of a supply chain-related cybersecurity breach are far-reaching and could impact not only economic stability but also public safety. Threat groups have shown an increased interest in, and exhibit increased capabilities for, supply chain attacks.

Ransomware remains a persistent threat with global damages at a record high, estimated at over 1 billion euros in 2023. Advances in sophistication of (spear-)phishing - e-mails seemingly sent from trusted senders which remains the most common initial vector - as well as user fatigue, have contributed to this rise. Extortion techniques are further evolving, with numerous new techniques being used to extend the classic ransomware operation modus operandi, such as through the popular use of leak sites hosted over the public internet where exposed victim data can be indexed, cached, searched and identified faster. Meanwhile, through continuous 'retirements' and rebranding, ransomware groups aim to avoid law enforcement and sanctions.

[9] Microsoft (2022) *Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[10] Mandiant (2023) *Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace*, https://www.mandiant.com/resources/blog/zero-days-exploited-2022

Finally, novel, hybrid, and emerging threats are feature in the threat landscape with high impact. Consent phishing is used by attackers to send users links that, if clicked, will grant the attacker access and permissions to applications and services. Machine Learning models are at the core of modern distributed systems and are increasingly becoming the target of attacks, while AI will increasingly be used for the purposes of phishing, disinformation and creation of deepfakes.

2.2 Sectoral threat landscape: telecommunications

Entities in the telecommunications sector including telecommunications operators, satellite companies and internet services are crucial facilitators for critical infrastructure and its development in virtually every sector. The EU's 2030 Digital Decade Policy Programme aims for 100% coverage of gigabit and 5G connectivity in each Member State by 2030. With 5G deployment and the growing number of IoT devices, the sector is rapidly expanding to markets of new technologies. However, these new markets and innovations stretch the surface of the networks, consequently increasing their vulnerability.

Over the past few years, the telecommunications sector has been a victim of espionage activities, physical sabotage, as well as data theft and exploitation. The overall trend is an increase in cyberattacks on telecommunications organisations and networks, including threats from both state-sponsored and criminal actors. Constant innovations in the sector increase the complexity of European telecommunication supply chains, making it increasingly difficult to ensure a high level of cybersecurity and resilience. Moreover, the increase in devices connected to the internet, referred to as the Internet of Things (IoT), has resulted in many IoT and critical infrastructure projects experiencing security-related issues.

Mobile and fixed telecommunication entities tend to control large databases including large quantities of sensitive data, which are targets for potentially lucrative ransomware attacks. Double-extortion techniques, involving threats both to leak the sensitive stolen data and to render them unusable through encryption, have emerged, which increase the pressure on victims to pay the ransom. The number of cases of data leakages increased globally by 17%, from 1 108 to 1 291 between 2020 and 2021[11].

Furthermore, 5G is relying more and more on virtual infrastructures for the operation of its core network, resulting in a multiplication of the number of access points to be secured. The EU coordinated risk assessment on the cybersecurity of 5G networks accordingly identified a number of risks and risk scenarios associated with 5G networks, such as the risk of dependency on single

[11] Identify Theft Resource Center (2021) *Number of data breaches in 2021 surpasses all of 2020.* https://www.idtheftcenter.org/post/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/

suppliers or the risk of state interference through the 5G supply chain, which remain relevant for the present risk evaluation[12].

Finally, Russia's ongoing military aggression against Ukraine has also significantly altered the sector's threat landscape. Two of the most sophisticated attacks targeted the satellite KA-SAT network, owned by Viasat, on the eve of the full-scale invasion in February 2022, and Kyivstar, Ukraine's largest telecommunications operator, in December 2023. In addition, Internet service providers and digital infrastructure providers have been regularly targeted by pro-Russian hacktivists with DDoS attacks.

2.3 Sectoral threat landscape: electricity

The EU's ambitions to reduce carbon emissions and its dependency on fossil fuels are contributing to an increasing demand for renewable electricity technologies. To address this in a more efficient and effective manner, the EU's aim is to better distribute and trade electricity throughout its internal energy market.

Europe's cross-border electricity networks are operated according to rules that help govern the work of operators and determine how access to electricity is given to users across the EU. As electricity networks are increasingly interconnected between countries, the EU-wide rules effectively manage these electricity flows in the internal energy market, and a network of System Operation Regions (SORs) was established.[13] SORs include transmission system operators (TSOs) that have been designated or assigned with responsibilities which are relevant for system operation. These responsibilities include calculation of capacity, assessment of needed remedial actions to ensure security of the whole system, coordination of all the outages to ensure security and efficiency, adequacy assessment and tasks related to the provision of system balancing. There are five SORs in total: the Baltic-, Nordic-, Central European-, Southeast European- and Southwest European SORs.

The electricity sector is further characterised by high levels of integration of, and reliance on, different operational technologies (OT). OT is defined as hardware and software that detects or causes a change through the direct monitoring and/or control of industrial equipment, assets, processes, and events. OT systems are, therefore, at the heart of managing the electricity grid. They help monitor the status of power generation sources, transmission lines, and distribution networks in real-time. This enables grid operators to balance supply and demand, prevent overloads, and respond to emergencies quickly. Moreover, as renewable energy sources like solar and wind power become increasingly prevalent, OT is vital for managing the intermittent nature of these sources. However, the increasing interconnectedness of these devices, such as smart

[12] NIS Cooperation Group (2019) *EU coordinated risk assessment of the cybersecurity of 5G networks*. https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[13] The SOR networks are established in accordance with Article 36 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity, and defined in the ACER Decision on SOR: Annex I (https://www.acer.europa.eu/Individual%20Decisions_annex/ACER%20Decision%2005-2022%20-%20Annex%20I%20-%20Definition%20of%20SORs_0.pdf)

meters, has increased the attack surface. On top of that, many OT devices are used over longer periods of time and patched less frequently than the average IT component, making them more vulnerable to attacks. Protecting both IT and OT systems from cyber threats is, therefore, essential to safeguard the integrity and reliability of the electric grid.

The electricity sectors continue to attract cyberattacks. Although the majority of attacks are relatively unsophisticated, the criticality of the electricity sector to society and the economy makes it a prime target for those with the intent of causing wide-ranging societal disruption, as well as for cybercriminals looking for sensitive targets. A real-world example of societal disruption through the electricity sector can be found in the series of cyberattacks against the Ukrainian energy sector, which were closely followed by waves of missile attacks, in the autumn and winter of 2022.[14]

3. Risk evaluation

This section presents the risk evaluation for the EU. The first section focuses on the telecommunications sector and the second section on the electricity sector (including gas to the extent that it contributes to the generation of electricity). The third section then addresses the issues of spill-over risks and critical interdependencies across both sectors.

3.1 Risk evaluation for the EU's telecommunications sector

The top risks identified are, in this order: risks to mobile and fixed telecommunications networks, risks to the internet's core infrastructure and risks to the satellite communications. The risk analyses for mobile and fixed telecommunications networks are largely similar in terms of likelihood and impact. The results for the core internet infrastructure showed similar types of risks as those for the telecommunications networks, though there was a stronger emphasis on physical damage. For satellite infrastructure, the main risks pertained to jamming and to its role as a back-up network. The risks identified across the telecommunications sector can be divided into two categories: threats that could lead to the unavailability of critical services with a direct impact on society, and those involving espionage by corporations or nation-states where the potential impact is harder to assess.

With regard to **mobile and fixed telecommunications**, **the unavailability of critical services caused by financially motivated ransomware groups is a major concern**. Other types of disruption, such as those caused by **destructive malware (e.g. data wipers[15]) deployed by a state-sponsored actor are as likely to occur as ransomware incidents but with a slightly**

[14] Economic and Security Council of Ukraine (2022) *Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions*. https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-17-Ukraine-ESCU-Cyber-Artiller-Propaganda-Comprehensive-Analysis-of-Russian-Warfare-Dimensions-ESCU.pdf

[15] Data wipers are a type of malicious software designed to irreversibly erase or destroy data on a computer or storage device, often used as a destructive component in cyberattacks.

lower impact. Coordinated large-scale **DDoS attacks** can have severely disruptive effects and serve as cover for more serious attacks such as ransomware or data wiper attacks. The impact of any of the risks involving disruption is strongly amplified where the telecommunications operator is the sole provider for critical infrastructure entities or where regional connectivity is covered by one single operator.

Vulnerable end-user devices are a particular risk to the fixed and mobile networks subsectors**.** A single operator may provide Internet access to millions of customers with smart devices. If these end-user devices are vulnerable, for example as a result of unpatched home routers, vulnerable IoT devices, or legacy personal computers, they can be used by attackers to create large botnets, that is, groups of devices that are under the control of a malicious actor, for other types of attacks. Large botnets of compromised end-user devices have been used to create large-scale DDoS attacks which are hard to mitigate because the attack traffic comes from many different networks, allowing the attackers to hide the source of the activity.

Espionage risks are considered equally likely in both the mobile and fixed telecommunications subsectors, though their impact is much harder to assess than for other types of attacks. A successful intrusion can provide the basis for significant future attacks, for instance through logic bombs, where code is intentionally inserted into a software system that will set off a malicious function when specified conditions are met, or through the exfiltration of sensitive data such as login credentials.

Supply chain attacks are a growing concern. The complexity and diversity of the supply chains in mobile and fixed telecommunications make it difficult for buyers to conduct due diligence on all bought services, software and hardware components. The degree of exposure to this risk is strongly influenced by the extent to which the supplier has access to the network, in particular its most sensitive assets, and by the risk profile of the individual supplier. Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) are potential vectors for an attacker to gain access to telecommunications operators while evading the operator's security measures.

Furthermore, **dependencies on suppliers in third countries** are identified as a potentially prominent threat. The EU coordinated risk assessment on the cybersecurity of 5G networks showed the risks related to the 5G supply chain, notably the risk stemming from suppliers. Hostile third countries may exercise pressure on 5G suppliers in order to facilitate cyberattacks serving their national interests. These dynamics are also relevant to the rest of the telecommunications sector.

Two particular types of espionage threats for mobile telecommunications are identified. The first is **SS7 attacks**, which exploit vulnerabilities in the roaming infrastructure and can be used for geolocating subscribers, intercepting calls, and SMS messages, etc. The second is **weaknesses in legacy telephony and SMS services**. Smishing and vishing attacks, which exploit the lack of authentication and encryption in voice and SMS traffic can be used to attack two-factor authentication systems to access critical systems in other sectors and can be used in general to spread disinformation.

Within the core Internet infrastructure subsector, the risks are similar to those of the telecommunications networks though with some notable differences. The risk of ransomware was assessed considerably lower compared to the same risk for the mobile and fixed telecommunications subsectors. The risk of **physical sabotage of submarine cables is of particular concern**[16] in this subsector. Currently 95% of international internet traffic is transmitted by the roughly 200 cables around the world. These cables lie on the ocean floor, while nearer to the shore they are buried under the seabed for additional protection. Unintended cable damage by commercial marine activity accounts for more than 70% of the yearly incidents. This large share can be explained by unintentional incidents rooted in unfamiliarity with legal rules and protection zones or negligent behaviour and deliberate risk-taking when operating near cable installations. However, these incidents also show the relative ease with which intentional physical damage might be enacted. Intentional, physical destruction of cables can take place either using improvised cutting devices such as anchors and dredging devices, through undersea explosives or by using divers, submersible boats, craft or military-grade drones and submarines. Information on the cable routes can be easily obtained and potential attackers can use their own resources to obtain precise maps of the sea floor and the location of cables. The Revised EU Maritime and Security Strategy and its Action Plan[17] and the Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures[18] already drew attention to the vulnerability of maritime critical infrastructure, including cable infrastructures, and suggests increasing preparedness exercises and surveillance of critical infrastructure.

Some of the most critical issues for submarine cables revolve around recovery operations. The duration of an incident's impact is highly dependent on the distance from a spare cable storage and cable ship availability. Additionally, there is a lack of pre-existing coordination mechanisms between states and cable owners. The private sector is currently responsible for the planning, production, operation, and maintenance of repair operations, which is done with privately owned repair vessels. Although requiring significant time and resources to plan and execute, a large-scale coordinated attack on submarine cables that would result in damage to several cables at once could both be difficult to mitigate and have long-lasting impact, especially considering the relatively low number of repair vessels.

Landing stations, where the undersea cable connects to the land infrastructure, are vulnerable sites. Every submarine cable must have at least two landing points. From there, its fibre-optic signals are transmitted over land. Landing stations play a key part in the operation of submarine cables. They can perform many functions, including terminating international cables, supplying power to cables and acting as a point of domestic and/or international connection. In these landing stations, there are systems needed for the functioning of the cable network – such as heating, ventilation, and air-conditioning systems. Landing stations are usually equipped with battery

[16] See also: ENISA (2023) *Undersea cables: what is at stake?* https://www.enisa.europa.eu/publications/undersea-cables?v2=1
[17] See also: Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan
[18] European Commission (2024) Commission Recommendation of 26.2.2024 on Secure and Resilient Submarine Cable Infrastructures. https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures

groups and power generator groups that operate in case of power supply failure from the public grid (normally with two independent points of access). However, such battery and generator sets can only ensure power supply for a few hours, not entire days, unless a continuous supply of fuel is ensured – and generator groups are also vulnerable to attack. Furthermore, containers are installed in well-known locations, and hence could be susceptible to unauthorised access.

Additionally, there are numerous ways in which **cyberattacks can be carried out against the submarine cable network**.[19] One of the most significant cyber threats is linked to the reliance on remote network management systems. As network management systems are often connected to the internet and rely on HTTP and TCP/IP protocols and non-proprietary software, they become susceptible to a range of cyber threats. Hacking into network management systems can provide attackers control of multiple cable management systems, visibility of networks and data flows, knowledge of physical cable vulnerabilities, and the ability to monitor, disrupt, and divert traffic. Network Operation Centres, remote access portals, and other systems needed for the functioning of the cable network – such as electrical power, routers, heating, ventilation, and air-conditioning – are also potential cyberattack vectors.

Finally, **the risks for satellite networks were perceived to be overall lower** than those in the other sectors, though by no means negligible. Within this subsector, **espionage and jamming are the most critical risks**. Jamming in particular is an easy and cost-efficient way to interrupt a satellite's up- and downlink. All other risks are on a much lower level of impact compared to similar risks in other subsectors. However, significant spillover risks from satellite infrastructure were illustrated by the Russian attack on Viasat's KA-SAT network. The attack resulted in partial interruption of KA-SAT's consumer-oriented satellite broadband service, impacting several thousand customers located in Ukraine and tens of thousands fixed broadband customers across Europe which included German windfarms.[20]

3.2 Risk evaluation for the EU's electricity sector

Overall, the electricity sector's digital transformation, the deeper integration of IT and OT networks/systems and the increasing number of small energy providers are considered to significantly widen the potential attack surface[21]. The market expansion of renewable energy sources introduces additional risks for the electricity sector, for example, where equipment and external maintenance providers have access to the operator's resources and networks. Moreover, the rapid expansion of IT components and the fact that OT components are often relatively old

[19] See also: Bueger, Liebetrau and Franken (2022) in-depth analysis: security threats to undersea communications cables and infrastructure – consequences for the EU

[20] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[21] This section builds on national risk preparedness plans https://energy.ec.europa.eu/topics/energy-security/security-electricity-supply/risk-preparedness-plans-electricity-sector-national-competent-authorities-and-commissions-opinions_en

and receive fewer patches creates a larger potential for new zero-day vulnerabilities to be discovered and exploited.

The risk assessments across the different System Operation Regions were largely consistent. In general, two distinct categories of risk were identified. The first category consists of **risks to entities directly connected to the electricity grid** (including gas infrastructure), and the second category of **risks to market participants not physically linked to the grid.** Where entities directly connected to the grid are attacked there are potentially high levels of societal disruption, compared to attacks against non-connected electricity market participants. For each of these categories, several unique risks were identified as most salient across all of the System Operation Regions.

Within the category of threats to connected entities, the worst-case outcome is a blackout, that is, the total loss of power to a wide area for a long duration, resulting either from malicious cyber activity coming from within the network or from the outside. Of these two vectors, **insider threats are considered by Member States to be the most impactful**. This threat can typically materialise either through social engineering (psychological manipulation of victims and impersonation as techniques to access sensitive information), or direct infiltration by foreign agents with malicious intent hired as technical staff. A malicious insider with a sufficient level of clearance can scan the network for vulnerabilities for long periods of time while going virtually unnoticed. This provides the opportunity to set up complex attacks that might both be hard to detect and difficult to mitigate. Two factors were found to exacerbate the likelihood of an insider threat materialising. First, maintenance services and other third-party services are frequently performed remotely, which greatly increases the risk of false authentication of malicious actors. Second, some Member States flagged the market pressure stemming from domestic skilled labour shortages and difficulties to attract talent due to budgetary constraints, providing an opportunity for malicious agents with adequate skills to position themselves for hire. Thorough vetting is essential but relies on having accurate and relevant background information on potential candidates. The degree to which governments provide support in this process currently varies across the EU.

For malicious activity from the outside, the top risk is **ransomware attacks**. The energy sector is the third most targeted sector for ransomware attacks in the EU, following heavy industry and finance. Although the likelihood of such a ransomware attack is considerably lower than that of a DDoS attack, the impact is much higher and is generally harder to mitigate. **Destructive malware** injected into SCADA systems of the transmission system operators (TSOs) or distribution system operators (DSOs) could have a significant societal impact, and could disable the distributed control systems (DCSs) of major gas producers or electricity generators. Various waves of such incidents in Ukraine's energy sector occurred both before and after Russia's full-scale invasion in February 2022.

Cyber espionage in the electricity sector is closely related to the aforementioned risks, as espionage operations can both be aimed at data exfiltration for economic or political gain and at pre-positioning for destructive attacks at a later time. This approach is clearly illustrated by Russia's operations against the Ukrainian grid in 2015 and 2016, where initial access was obtained through online social engineering. In this way, cyber espionage becomes a springboard

for destructive attacks later on. Countering espionage in the energy sector relies on timely and accurate information available to the electricity sector entities. The degree to which such information is available currently differs per Member State, which comes with a clear risk of missing cross-border operations by Advanced Persistent Threat actors (APTs).

Supply chain compromises were identified as a major catalyst for outside malicious activity. This includes compromising the security of a target by exploiting weaknesses in the network of organisations and processes involved in the production and distribution of a product or service. There are three main types of supply chain compromises.

(1) **software supply chain attacks**, where attackers inject malicious code into software components or during their development or distribution phase or compromise the development tools themselves. This allows attackers to compromise software to be used by the electricity sector before it even reaches the sector's infrastructure and before it has been properly secured. This gives attackers a future backdoor into the software once deployed or to allows them plant logic-bomb types of malwares to cause systems to malfunction at given time or under pre-determined circumstances.
(2) **hardware supply chain attacks**, where malicious actors can introduce counterfeit or malicious hardware components into the supply chain either during the manufacturing or the transportation phase. Pre-compromised hardware can be used by an attacker in a similar way as pre-compromised software, i.e., as a backdoor into a system or as a logic-bomb style of disruptor. However, unlike with software supply chain attacks, mitigation implies replacing physical components which could be much more costly, as well as time- and labour intensive.
(3) **third-party service attacks**, where an external (security) service provider or a cloud-based security service is compromised which gives the attacker direct access to the downstream energy infrastructure.

A closely related issue and potentially enabling factor for supply chain attacks is the growing material **dependencies on third country suppliers**, as many suppliers of the often highly specific software and hardware in the electricity sector are not EU-based and may be judged high risk. The number of dependencies for the electricity sector is rising sharply, driven by the increasing digitalisation of existing electricity infrastructures and the rapid growth of renewable energy plants. This requires novel and increasingly complex constellations of technologies developed and/or manufactured outside of the EU, making security controls difficult. Such suppliers may be susceptible to interference by the government of a non-EU country without adequate legal or judicial constraints. This includes states that may be able to exert enough influence over their private sector to force them into implementing backdoors or malicious components or code into their products at a large scale. Following similar dynamics, critical electricity infrastructures dependencies on foreign cloud-hosted services can be exploited by countries hosting those cloud infrastructures.

A sector identified as particularly vulnerable to risks from third country dependencies is **wind farming**. This subsector is expected to grow drastically under the EU's current plans for expanding the share of renewable energy and it relies on relatively new types of technology, which provide ample opportunities to introduce large numbers of potentially compromised components onto the

European market. While EU-manufactured components are generally considered safer and of higher social and environmental standards, inadequate and uncertain demand, slow and complex permitting, high inflation and commodity prices, inadequate rewards for high environmental and social standards and rising competition from non-EU vendors have already led to an increased uptake of non-EU alternatives. This greatly increases the risk of major vulnerabilities in an increasingly vital subsector.

DDoS attacks, though highly common, have had very limited operational impacts in the electricity sector. However, they can be used to exacerbate other attacks. For example, Russia's cyberattack on the Ukrainian grid in 2015 and 2016 coincided with a DDoS attack on the power companies' websites and call centres in addition to their malware attacks, making it difficult for customers to report outages or access information about the blackouts.

Threats of attacks on non-connected electricity market participants involve market entities that are not physically connected to the electrical grid but nonetheless play an important role in the functioning of the electricity markets. Examples of such participants include electricity traders that buy and sell electricity contracts on the wholesale market and electricity storage providers. This risk associated with these entities is generally less impactful but there is a concern with the higher exposure of corporate networks of these actors. **Ransomware is identified as the top threat contributing to this risk, as the unavailability of market participants' services may have operational spill-over effects for electricity operators**. Finally, DDoS attacks against non-connected entities are also common, but they have had negligible impact so far.

3.3 Spill-over risks and interdependencies across sectors, Member States and with third countries

Telecommunications and electricity are highly critical and interdependent sectors. As a result, there are significant risks of an incident in one sector spilling over into the other. All other critical sectors under the scope of the NIS2 Directive are, to a large extent, dependent on the well-functioning of the telecommunications and electricity sectors.

Spillover effects from the telecommunications to the electricity sector include **the loss of availability, integrity or confidentiality of communication.** This includes day-to-day emergency operations of electricity sector operators such as telemetry services (e.g. the monitoring of supplies, consumption surges and peaks) and related alarm systems. It can also involve the loss of availability of communication resulting in a break-down of coordination among electricity market entities.

In terms of **spillover from the telecommunications sector to other sectors**, all critical sectors are highly dependent on the availability of telecommunications. In particular, access to emergency services and public warning systems would be disrupted where they rely on the public mobile networks. Digital payments would be disrupted, affecting in turn public transport and retail services online and offline. A significant incident could also disrupt the ability of Member States to coordinate their crisis response. The health sector is also highly dependent on telecommunications for scheduling hospital appointments.

Spillover effects from the electricity to the telecommunications sector are threefold. First, **power outages to data centres** may lead to widespread economic and societal disruption. Second, **power outages to fixed or mobile core network sites** can result in a widespread electronic communications disruption. Third, **power outages to fixed network regional exchanges or mobile network base stations** may result in regional electronic communications outages.

Regarding **spillover effects from the energy sector to the other sectors**, the energy sector underlies virtually every other critical sector. Without adequate energy flows, critical infrastructures are dependent upon their own back-up energy supplies.

In addition to cross-sectoral spillover effects, four critical interdependencies between Member States were identified that might facilitate cross-border spillover effects. First, the EU **network of electricity transmission systems** is highly interlinked allowing for a fast spread of incidents. It is to be noted that a high level of interconnection brings more stability to the everyday operation of the overall system. However, there is a broad reliance on the same ICT/OT products, services and providers or manufacturers which could rapidly escalate any incidents involving these products, services of providers to an EU level. Second, **the gas infrastructure network is highly interconnected**. This means that a successful cyberattack on one of these companies could have significant spillover effects, as gas distribution can be halted which greatly increases the pressure on the EU energy systems. Third, **shared telecommunications networks for EU-level crisis coordination** are essential to managing cross-border crises. Any compromise of these systems would severely worsen any ongoing crisis. Fourth, **crucial top-level domain name servers, Internet Exchange Points (IXPs) and large cloud data centres** are identified as posing considerable spill-over risks in case of compromise or disruption. Some of these servers, IXPs and data centres are not located in the EU, which may further complicate any attempts at mitigating any harmful consequences.

4. Risk scenarios

This section outlines ten risk scenarios, four for the telecommunications sector and six for the electricity sector. The telecommunications sector scenarios build on the 10 scenarios identified in the Nevers risk assessment. The methodology for the selection of the scenarios is described in section 1.4.

4.1 Telecommunications sector scenarios

Risk Scenario 1

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
SUPPLY CHAIN ATTACK TO GAIN ACCESS TO THE INFRASTRUCTURE OF OPERATORS	State-sponsored actors Hackers-for-hire	Backdoor Zero-Day Persuasion	Security services Intellectual property	CVE Zero-day Dependencies on suppliers and managed service providers	Economic Social/societal

Context

A hackers-for-hire group is employed by a state-sponsored actor from a hostile third country to execute a supply chain attack on the telecommunications sector. Their target is an MSP in the supply chain of multiple operators in the sector who supplies a small but critical piece of software to them and has a weak security posture.

Technical

In the first stage of the attack, the hackers-for-hire group that has managed to compromise the MSP via social engineering, forces the installation of ‘update’ to the MSPs software used by the operators. The ‘update’ introduces a vulnerability in the software allowing for backdoor access to it and thus the IT environments of operators using it. This access is sold by the organised crime group to a state-sponsored threat actor.

On a second stage of the attack, the state-sponsored actor leverages the backdoor access to gain foothold to the IT environments of several telecommunications operators including cloud-based services. Once the goal is achieved, the actor stealthily gathers information for espionage purposes, namely with regard to leading technology on green energy (clean hydrogen production).

Impact

After several months the supply chain attack is detected, because one operator realises there is an unknown vulnerability in the software of the MSP. As with many espionage attacks, the impact of the attack is not immediately felt, but immediate concerns over national security and the security

interests of the Member States as well as of the Union as a whole are raised, as the targeted ongoing hydrogen research conducted by companies operating in strategically important industries. Such loss of intellectual property undermines the ability to maintain the domestic energy sector's competitive edge and innovation.

In addition, the knock-on effect of a supply-chain attack may impact more organisations which are dependent on the compromised supplier. Finally, restarting some industrial operations would require hours and potentially days if some services require important repairs and their supply chains are disrupted significantly.

Risk Scenario 2

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
DDOS ATTACK TO CAUSE A LARGE-SCALE NETWORK OUTAGE	State-sponsored actors Hacktivists	DDoS attack	Network devices Servers Internet Exchange Points (IXP) Backbone internet provider Server/data-centre provider		Unavailability of the Internet Economic Social/societal

Description

Context

A State actor threat agent supported by a hacktivist group, engages in large-scale DDoS attacks on the communication networks and infrastructures of several EU countries, with the aim of causing social unrest and disrupting economic activities, including, for example, the disruption of digital and online payments, other digital services and logistical processes.

Technical

The attackers use Domain Name System (DNS) amplification and a pre-prepared botnet of infected home routers and other end-user devices. Some operators are able to stem the flow by using AI-enabled cyber defence measures that are able to re-route, filter and block malicious traffic. Other operators across the EU do not manage to deal with the attack.

Impact

Network outages on the affected operators last for several hours. While the attack is not fully mitigated and access restored to some of the most critical customers, cascading effects take place with significant impact. The economic impacts are initially local, as shops and industries would be able to provide very few services without communications. Industries and businesses beyond the geographical coverage of the current scenario could be affected shortly after. Damage can escalate if the financial sector is hit. The messaging network for financial transactions, for instance, suffers persistent disruptions over a substantial period (e.g., transactions processing, digital banking services, etc.), further limiting the overall economic activity and trade.

Risk Scenario 3

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
AI POWERED DISINFORMATION	State-sponsored actors Hacktivists	Disinformation Smishing/Vishing (spear)phishing / Whaling Deepfakes AI text generator Spoofing Jamming	Applications End users	CVE	Reputational Social/societal

Description

Context

In the midst of high geopolitical tensions, a state-sponsored threat actor unleashes a disinformation campaign aimed at influencing election outcomes of a rival nation. Hacktivists aligned with the state's objectives support the creation and spreading of similar disinformation narratives. In addition, the threat actor attempts to generate fear by interfering with telecommunications capacities.

Technical

The campaign initially exploits widespread smishing and email spoofing campaigns sent to rival nation citizens, disseminating a mix of falsehoods masked as truth in relation to the government in function. Many of these emails were specifically addressed to the recipients themselves, suggesting the attackers may have stolen databases (for instance, voter registration systems) during an earlier espionage-related cyberattack. Links in the SMSs and emails redirect readers to websites resembling those of reputable news outlets. The threat actors also make use of AI-

leveraged bots to manipulate opinions through posts on comment sections, create deepfakes, and disseminate fabricated narratives around pressing economic or societal issues.

At the same time, the threat actor jams communication satellite signals and cuts several communications cables in various regions.

Impact

These carefully constructed tales, paired with the intermittent unavailability of telecommunications across the EU, exact a psychological toll, spread uncertainty, and erode trust among the population. The impact on society is significant, as trust in traditional media collapses and confusion and scepticism permeate public discourse.

Risk Scenario 4

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
ESPIONAGE	State-sponsored actors Cybercriminals Malicious insiders	Spyware SQL injection Persuasion	Applications End users	CVE	Reputational

Context

An organised crime group operating as an initial access broker has managed to penetrate the infrastructure of several EU telecommunications operators in different EU countries. The group achieved this by bribing disgruntled employees working at the targeted critical infrastructures. The crime group then proceeds to advertise their stolen access on dark web forums aspiring to sell it to other actors (including state-sponsored actors), who could leverage it to further their objectives.

Technical

The initial foothold attack is done by injecting malicious SQL code into web application fields of an API used to communicate and interact with the underlying telecommunications infrastructure (e.g., send SMS, perform number verification, or access other services). The implanted code enables the state sponsored actor to operate as an APT that can obtain and exfiltrate sensitive information on an ongoing basis for instance eavesdropping on critical communications and the geolocation of specific subscribers, or to cause disruptions.

Impact

The impact of this network intrusion is not immediately known, because it is used as a preparation for future attacks, and it took place in an inconspicuous manner. It takes several months for the affected operators to detect the intrusion. An example of a follow-up attack can be found in TRS1.

4.2 Electricity sector scenarios

Risk Scenario 1

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
MALICIOUS ACTIVITIES BY INSIDER THREATS	State-sponsored actors Cybercriminals Malicious Insiders	Trojan horse Persuasion	Servers Applications End users	CVE	Outage Economic Reputational Social/societal

Description

Context

An employee of an EU-based transmission system operator with high levels of access turns rogue and intentionally engages in malicious activities in support of a state sponsored cybercriminal group that targets the entity.

Technical

Leveraging their privileged access to several central locations with access to multiple switching stations, a group of rogue employees deploy a remote access trojan (RAT) in a shared folder of a network-attached storage server (NAS) via USB at different regional locations. The threat actors leverage their remote access to map corporate and operational networks and deploy malware designed to detonate only when a specific model of programmable logic controller (PLC) is identified. The malware works by altering the programming of those PLCs causing them to “stealthily” operate incorrectly until their disruptive effect can take place.

Impact

The successful attack makes it impossible for the organisation to sustain critical on-going operations as it degrades system performance and disrupts business operations. There are interruptions to energy supply and/or downtime. Given the severity of the attack, the state-sponsored cybercriminal group and/or other copycat groups, continue exploiting it to cause further immediate damage leading to a full disruption. Direct effects on other critical infrastructure take

place in the shape of potential difficulties in gas and oil distribution and in water supply and wastewater treatment. With the lack of power, a decrease of the quality of communications may be felt (fixed and mobile networks, internet, radio).

Risk Scenario 2

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
ESPIONAGE	Cybercriminals	Zero-Day	System configuration Technical information /statistics User rights policies Electricity Generation (OT) Electricity transmission & distribution (OT)	CVE Zero-day Dependencies on suppliers and managed (security) service providers	Economic Reputational Societal

Description

Context

A resourceful cybercrime group targets a smart meter manufacturer's proprietary technology. In particular, criminals are interested in a new wireless communication interface for smart meters, the adoption of which by EU power grids is growing fast. The manufacturer operates in a third country outside of the EU and has a weak cyber posture making it an easy target for the cybercrime group.

Technical

Following extensive reconnaissance against the manufacturer's external facing systems, the cybercrime group identifies and successfully exploits an authentication bypass vulnerability in the software used by the company's VPN servers. The vulnerability exploited, allows bypassing all client certificate checks with an invalid certificate. This enables the attacker to successfully authenticate as any user and gain access to restricted VPN network resources. The attacker uses their access to gather sensitive information about the smart meters' design.

Impact

Despite the absence of immediate interruptions to energy supply and/or downtime as a result of the attack, the stolen technology is a critical component for the EU power and telecommunications grids. The attacker could potentially switch all appliances of all clients at the same peak consumption time creating a huge demand that will create an enormous instability in the system. This can result in rolling blackouts as consumers will be compromised and would need to remain disconnected until at least they move away from the smart operation mode and then be reconnected only progressively. From an industry point of view, the attack may lead to several impactful consequences, from reduced foreign direct investment (as there is lack of confidence about the protection of sensitive information), to a slowdown in R&D advancements and trade disputes or even diplomatic tensions.

Risk Scenario 3

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
HYBRID ATTACK TO CAUSE A LARGE-SCALE ENERGY NETWORK OUTAGE	State-sponsored actors Cybercriminals	Ransomware / wiperware Zero-Day	Electricity Generation (OT) Electricity transmission & distribution (OT)	Zero-day Dependencies on suppliers and managed (security) service providers	Outage Social/societal

Description

Context

In the context of ongoing military operations, a state sponsored cyberwarfare group is engaged in the delivery of targeted simultaneous attacks against several power plants connected on a country's power grid leveraging a recently developed wiper and a range of zero-days vulnerabilities and backdoors in wind turbines, solar panels and electric cars.

Technical

The cyberwarfare group was able to leverage a zero-day vulnerability in a product used by multiple power plants in the EU to gain foothold to their IT environments. From there, the group leveraged the lack of adequate IT/OT network segregation wherever applicable, to move laterally to OT networks where it deployed its custom-made wiper malware.

At the same time, the well-resourced group exacerbates the attack by targeting back-up options. At first, all wind turbines are being shut off during windy conditions by leveraging a backdoor in a critical component that was manufactured in a third country that (indirectly) supports the cyberwarfare group's cause. The same then happens for solar panels produced within the third country. Finally, some electric cars start drawing more from the grid than they should, further increasing the load on the grid.

Impact

As a result of the activity of the wiper on the affected power plants, several OT systems are rendered unavailable. This keeps much of the generation off-the-grid, thus impacting the management and operation of the energy system by the transmission network operator of the country. This results in forced rolling blackouts which are worsened by the unavailability of backup generation from wind farms.

The resetting and commissioning of the affected OT systems lasts up to two weeks, by when the situation is fully back to normal. Additionally, though most or all Member States were affected, those who are heavily dependent on wind or solar energy as a secondary source might have to request support from other Member States while they are dealing with their own situation. This requires effective cooperation at EU level.

The rolling blackouts may also cause additional multi-sectoral cascading effects and potentially black starts in several countries. Public rail and road systems (e.g., bus and rail schedules, train operations, signalling systems or track switches) that are successfully disrupted, would be in some cases paralysed. Public administration would likely cease most of its operations for the days of the total blackout, except for emergency services. The impact of the power outages on the health system would be far-reaching and result in an increased need for emergency care. With limited power and reliance on generators, hospital services are immediately reduced and healthcare facilities are often not able to provide basic services. Payment systems would also be severely affected, with significant consequences for the retail sector where particularly access to food could pose a major problem.

Risk Scenario 4

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
GAS SHORTAGE	State-sponsored actors Hacktivists	(spear)phishing / whaling Trojan horse	Operating systems Fossil-fuel power stations (including natural gas)	CVE Dependencies on suppliers and managed (security)	Outage Economic Social/societal

				service providers	

Description

Context

A severe unexpected weather event developing in a European region strikes several countries at the end of the winter, cooling the area down to unusually low temperatures when overall gas reserves are at a significantly low level after a particularly cold winter. Amidst geopolitical tensions, a state-sponsored threat actor takes advantage of peak winter and targets an EU-based gas company with operations across multiple Member States.

Technical

By sending weaponised phishing emails to the company's personnel containing malicious macro-enabled Excel attachments, the threat actor is able to gain foothold in the company's network. At the time of the attack, numerous hosts at the company's site run a vulnerable OS version with critical vulnerabilities unpatched. The attacker exploits one such vulnerability on an affected host, enabling them to not only achieve remote code execution but also to move laterally across the company's network. The poor segregation in the company's IT and OT environments enables the attacker to mount an attack against the remote terminal units (RTUs) of the gas distributions system by detecting an outdated/insecure SCADA protocol that is supporting RTUs that control the downstream flow of liquified natural gas (LNG). As they are unable to differentiate between an authentic and un-authentic SCADA communication, the vulnerable RTUs are used to control the connected physical processes and cause a disruption in the provision of gas.

Impact

The low level of supply at the moment of the attack creates immediate effects on the EU wide gas distributing networks and additional cascading effects to the EU electricity production. A widespread shortage of gas for about 10 days causes significant political, social, and economical issues across the affected EU MS. Supply to industrial consumers will likely be disrupted, which in extreme cases can cause severe economic damage or safety problems. Gas supply would be prioritised for critical production of electricity to prevent a black-out in the system. This can be done at the expense of the gas supply for heating, including to households.[22] The shortage could be so severe that it could also affect electricity production that is reliant on gas (gas-fired electricity

[22] The resort to such extreme measure is necessary to prevent a full gas and electricity disruption. As many heating systems require electricity to start, and as gas distribution is partially dependent on electricity, a blackout in the electricity sector would leave a significant portion of the population without gas supply during a blackout.

power plants), which depends on a steady supply of natural gas (in this case disrupted at source). Solidarity provisions among Member States will kick in to provide gas supply to households and minimum critical services.

Risk Scenario 5

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
VENDOR LOCK-IN INTRODUCES VULNERABILITIES IN PRODUCTS	State-sponsored actors	Backdoor	Electricity Generation (OT) Electricity transmission & distribution (OT)	CVE Dependencies on suppliers and managed (security) service providers	Outage Economic Social/societal

Description

Context

A large number of electricity providers across the EU source a large amount of power grid components from a single supplier at a third country, that has a near monopoly on the production of such components. As a result of global shortage and shifts in trade terms (import/export) the availability of new components and/or relevant updates for existing ones gets drastically reduced. This causes affected electricity providers to stall projects for the modernisation of power grids since they cannot switch to different vendors for those components due to backwards compatibility and interoperability issues, which leaves their power grids exposed to unpatched vulnerabilities. A state-sponsored actor decided to exploit these vulnerabilities.

Technical

The state-sponsored actor takes advantage of a pre-authentication integer-overflow vulnerability against a specific smart metering product line, that allows for remote code execute and rebooting of the meter. The attack is employed at scale, causing severe disruptions in the advanced metering infrastructure (AMI) communication flow.

Impact

A mass disconnection of meters causes circuit breaker trips resulting in temporary outages until power on the grid can be rebalanced. Those sudden and wide-spread power outages across the EU triggers a cascading effect on critical infrastructure and essential services. Communication networks fail, leaving authorities struggling to coordinate response effects. Hospitals,

transportation systems and businesses suffer severe disruptions leading to economic losses and public unrest.

Risk Scenario 6

	Threat Actor(s)	Threats	Assets	Vulnerabilities	Harms
DIPLOMATIC ROW EXACERBATES VENDOR LOCK-IN CONSEQUENCES	State-sponsored actors	Backdoor	Electricity Generation (OT) Electricity transmission & distribution (OT)	CVE Dependencies on suppliers and managed (security) service providers	Economic Reputational

Description

Context

A couple of low-level problems appear at the electricity provider who is covering large parts of critical electricity infrastructures of multiple Member States. It is uncovered that a backdoor has been installed into a hardware component that is supplied by a single provider. To make matters worse, this supplier is based in a non-EU country with which diplomatic relations recently deteriorated after an incident.

Technical

After further investigations, there is a suspicion that the backdoor had been installed by the supplier itself (or at least with their knowledge), as no external breach was identified. Additionally, the supplier defaults on delivering spare parts, referring to a raw materials shortage. However, this shortage is not observed elsewhere on the market. The electricity provider is deeply dependent on this supplier for 80% of their equipment. It is not possible to use a different supplier without having to change a large part of the network, which would mean investing vast sums of money and resources (3-4 months). This would cause the provider to breach its multiple legal obligations by not providing electricity. Meanwhile, the host state of the company in question refuses to provide any clarity on the situation.

Impact

The supplier is forced to start slowly replacing the infrastructure of this provider, which costs a huge amount of money. The supplier therefore dramatically increases its fares to the customers,

causing serious economic impact on the citizens of this region. The government must provide financial support to these people, resulting in public spending of tens of millions of euros.

5. Conclusions for areas of improvement

In accordance with the request by the Council, this report has presented the risk evaluation and the risk scenarios from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries. This section sets out the overall conclusions on how to prepare for the identified scenarios.

(1) Resilience and cybersecurity posture (Addresses Scenarios TRS1, TRS2, ERS1, ERS3, ERS4, ERS5)

a. Where needed, Member States should exchange good practices and develop guidelines covering human resources security, access control policies and asset management, with a particular focus on vetting and termination or change of employment procedures (e.g. clearance for sensitive roles and security functions). Member States are encouraged to formally support such procedures and aim for more consistency across the EU.

b. Coordinated efforts to share good practices on mitigating ransomware, together with vulnerability monitoring (e.g. national CSIRT or supplier information) and coordinated vulnerability disclosure (CVD) (e.g. under the NIS2 Directive), should be intensified.

c. In addition, synergies and information exchange between computer security incident response teams (CSIRTs) and law enforcement, as well as efforts to 'follow the money' trail of organised crime, should be enhanced to improve mitigation and deterrence. Furthermore, policy coordination with international partners should be promoted and intensified, for example through the Counter Ransomware Initiative.

d. The NIS2 Directive's 'all-hazards approach' implies the importance of assessments involving all relevant authorities, including Critical Entities Resilience (CER) Directive competent authorities, on the security and resilience of physical infrastructure such as submarine cables.

e. The Cyber Resilience Act (CRA) improves security at product-level through security requirements which decrease the likelihood of any scenario that includes a vulnerability mentioned in any common vulnerability exposure (CVE) database. It is recommended that Member States promote an early and smooth transition for energy and telecommunications entities to achieve the requirements laid down in the CRA. The transition for entities may include promoting familiarisation with the EU product regulation framework, hiring staff needed to fulfil the CRA requirements and putting in place relevant processes.

f. ENISA should facilitate an exchange of good practices on the mitigation of very large DDoS attacks, between national authorities and large operators of telecommunications networks and core Internet infrastructure.

g. In collaboration with BEREC, ENISA should develop technical guidelines on the security of home routers.

(2) Collective cyber situational awareness and information sharing (TRS3, TRS4, ERS2)

a. Member States and EU institutions bodies and agencies should improve the EU's situational awareness and the ability to detect and monitor cyber threats and incidents in the wider geopolitical context, in particular in the telecoms and electricity sectors which are typical targets for APTs. Collective situational awareness contributes to timely mitigation efforts and minimise spillover effects.

b. Member States should step up sharing within and among entities in the telecommunications and electricity sectors of timely and actionable information on physical, as well as cyber, espionage activities. Existing entities, such as Information Sharing and Analysis Centres (ISACs), and networks, such as the CSIRTs Network and EU-CyCLONe, should be leveraged to their full potential.

c. A coordinated 'call for action' to fight rising levels of cyber influence operations and disinformation campaigns conducted by state-sponsored actors and APTs, through identifying the main actors and relevant threats, techniques and procedures, sharing lessons learned, and promoting the EU Code of Practice on Disinformation and similar initiatives should be organised.

(3) Contingency planning, crisis management and operational collaboration (TRS2, ERS1, ERS5)

a. In order to mitigate the risk of spillover and to better prepare for multi-sectoral crises, communication lines between sectors as well as with cybersecurity authorities should be enhanced, including at an EU level. Operational collaboration (e.g. cross-sector contingency plans, collaborative exercises including entities and sectoral competent authorities) is crucial to be able to mitigate cross-sector spillover and cascading effects.

b. Increased efforts should be made to ensure that cyber crisis management procedures at EU level, including those involving EU-CyCLONe and the CSIRTs Network (e.g. roles and responsibilities, communication means and information flows between the operators and relevant competent authorities, the maintenance of network and information security) have a link to sectoral stakeholders, especially in sectors of high spillover risk.

(4) Supply chain security (TRS1, ERS5, ERS6)

a. Supply chain attacks can quickly have a cascading and impactful effect on entities within the same sector or even in other critical sectors where entities

use the same supplier[23]. A preliminary assessment of supply chain cybersecurity risks stemming from dependencies on high risk third-country providers of critical hardware and software components should be undertaken. Such assessment should highlight for instance: the level of assurance of ICT services, ICT systems or ICT products vis-a-vis required security levels; the degree of third-party vendor lock-in; the existence of secure software development lifecycle (SDLC) processes; whether secure by design and zero trust policies are in place and the likelihood of interference by the government of a non-EU country without adequate legal or judicial constraints.

b. From a policy development perspective, efforts between Commission and the Member States efforts towards an EU framework for supply chain security, as well as towards Union-wide risk assessments focusing on critical supply chains and sharing best practices, should be intensified.

c. Member States should also continue to implement the 5G toolbox measures, which address the supply chain security of telecommunications networks, including 5G in particular, as previously stated on the Council Conclusions on ICT supply chain security of 17 October 2022.

d. Member States and the Commission should analyse supply chain vulnerabilities in rapidly expanding areas, such as wind farms, solar farms and smart grids, leveraging, for example, the newly established Smart Energy Expert Group and its Working Group on cybersecurity.

e. Where needed, managed shared services provider supervision and overall supply chain supervision should be enhanced, given that the compromise of MSPs or MSSPs could lead to impactful cascading effects, as already stated in the Council Conclusions on ICT supply chain security.

Future risk assessments

As per the invitation of the Council, Member States and cyber networks are strongly invited to take into account this evaluation, the building blocks and the scenarios when defining and prioritising measures and support at EU and, where appropriate, national level. Furthermore, it is strongly recommended that the building blocks and scenarios presented here serve as an inspiration for creating future cyber exercises at national and EU-wide level including sectoral exercises in the telecommunications and energy sectors.

This report has also laid the foundations for a standardised toolbox for future EU-level risk assessments. It is recommended that this toolbox is improved upon through international

[23] Council conclusions on ICT supply chain security, approved 17.10.2022; https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf

collaboration and deliberation in order to make the process more efficient and results of future risk evaluations more readily comparable.

Annex 1: Relationship between this report and related exercises

This report builds on and complements the following related and parallel exercises.

- The Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), which entered into force on 16 January, mandates the Commission, ENISA and Member States to carry out **coordinated security risk assessments of critical supply chains**, with the aim of identifying measures, mitigation plans and best practices to counter threats and vulnerabilities emanating from critical dependencies and other risks associated with the supply chain as well as potential non-technical risk factors, such as undue influence by a third country.

- The Council, in its 9 December 2022 recommendation on 'a Union-wide coordinated approach to strengthen the resilience of critical infrastructure', brings together a wide range of cybersecurity actions and outlines a coordinated approach to strengthening physical and digital resilience of critical infrastructure on the basis of risk assessments and **stress tests of critical infrastructure resilience, focussing on the energy, digital infrastructure communications, transport and space sectors**.

- The findings of the 'EU coordinated **risk assessment of the cybersecurity of 5G networks**', published on 9 October 2019, the **Toolbox on the cybersecurity of 5G networks** published on 29 January 2020, the related progress report published on 15 June 2023, and the **risk assessment of the cybersecurity of Open RAN** published on 11 May 2022 by the NIS Cooperation Group remain relevant for this report. In addition, the threats, vulnerabilities and risk scenarios of the **risk assessment of communications networks and infrastructures** ('Nevers risk assessment') published on 21 February 2024 were taken as a basis for the telecommunication part of this report. The telecommunications sector scenarios build on and synthesise the 10 scenarios identified in the Nevers risk assessment.

- The **risk preparedness plans in the electricity sector by national competent authorities** submitted by EU countries in 2022 pursuant to Regulation (EU) 2019/941. These plans include an assessment of various risk scenarios, focussing on the result of a successful attack and on preventing the damage of such an attack. The identification of electricity crisis scenarios has to be performed every four years, as per the regulation, unless circumstances warrant more frequent updates. The methodology used for such identification in the first round was annexed to the regulation and is currently under revision. Additionally, the **Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows** (Commission Delegated Regulation (EU) 2024/1366) entered into force in June 2024 and provides for cybersecurity risk assessments at Union, Member State, regional and entity levels.

- The Joint Communication on a **European Economic Security Strategy** identified four categories of risks for further assessment: resilience of supply chains, including energy security; physical and cyber-security of critical infrastructure; technology security and leakage; weaponisation of economic dependencies and economic coercion. The Commission committed in the Joint Communication to assess the risks of technology security and leakage on the basis of a list of strategic technologies critical for economic security. In its **Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States**, the Commission proposed a list of critical technologies in view of a risk assessment to be pursued collectively with Member States by the end of 2023. Out of these, the Recommendation identified 4 technology areas, which present the most sensitive and immediate risks related to technology security and technology leakage, namely advanced semiconductors, artificial intelligence, quantum technologies and biotechnologies. These technology areas should, as a matter of highest priority, be subject to a collective risk assessment with Member States by the end of the year.

- An **EU-NATO Task Force** on Resilience of Critical Infrastructure was set up to reinforce common security. This Task Force was announced jointly by President von der Leyen and NATO Secretary-General Stoltenberg on 11 January 2023 and formally launched on 16 March 2023. The EU-NATO Task Force presented a final assessment report on 29 June 2023, which maps out the current security challenges and identifies four key sectors of cross-cutting importance: energy, transport, digital infrastructure and space. The report presents targeted recommendations to strengthen the resilience of critical infrastructure.

Annex 2 – Risk scenario building blocks

This annex describes the building blocks used for constructing scenarios and includes a brief description for every block.

Annex 2.1: Threat actors

Threat actors are 'actual individuals, groups, or organisations believed to be operating with malicious intent'. This definition is derived from STIX v2, following ENISA's preference for the definition - based on its interoperability - in their upcoming cybersecurity ontology.[24] In real-life incidents the precise threat actor is often unknown. However, the motivation and resources of a threat actor, even if their exact identity is unknown, are nevertheless an important element to consider when deciding on a mitigation strategy and therefore an important building block in scenario building. Therefore, rather than mentioning individual actors, threat actors are grouped in sector-agnostic categories based on their motivation.

	THREAT ACTOR	COMMENTS
TA1	**State-sponsored actors**	These actors motivated by geopolitical considerations and enlisted by their government to attack an opposing country's critical infrastructure, institutions, and businesses. The aim could be destabilisation of the target country or stealing confidential or potentially lucrative information. State-sponsored actors can be either a government agency or an external group.
TA2	**Cybercriminals**	Threat actors motivated by financial gain. This category includes criminal infrastructure providers, mass scammers, automated hackers and 'big game hunters' that dedicate considerable time and resources on attacking a highly lucrative target.
TA3	**Hackers-for-hire**	Actors also motivated primarily by financial gain but can have a secondary, indirect motivation derived from the hiring actor. Their service delivery model revolves around the delivery of services in the areas of Vulnerability Research and Exploitation, Malware Payload Development, Technical Command and Control, Operational Management, and Training and Support
TA4	**Hacktivists**	Actors motivated predominantly by ideological views and typically not motivated by financial gain. Hacktivists seek to

[24] ENISA (2022) *Cybersecurity Ontology 1.1* (working paper).

		spread their message. In some cases a subgroup of hacktivists – cyber-terrorists – may be considered as they mostly aim to cause terror to achieve their goals.
TA5	**Malicious insiders**	Actors with multiple potential motivations but a unique access to secure systems, assuming a higher level of clearance. These actors can be either financially, ideologically or otherwise personally motivated and can work as a proxy for other threat actors.
TA6	**Thrill seekers**	Actors motivated primarily by personal satisfaction. Some aim to learn about networks, others aim to push the limits for fun. Their technical expertise might vary greatly. Though they don't always seek to cause harm, thrill seekers can still cause unintended damage by interfering with a network's cybersecurity and opening the door to future cyberattacks.

Annex 2.2: Threats

Threats are defined by the International Organization for Standardization (ISO) as a 'potential cause of an unwanted incident, which can result in harm to a system or organization'.[25] These building blocks are largely based on the 'threat' and 'threat type' categories of ENISA's Cybersecurity Ontology, which are, in turn, based on the ISO's description[26]. To ensure a holistic approach that reflects the results of the conducted survey, some modifications and additions have been made to ENISA's structure. Furthermore, to remain within the scope of this assessment, only threats based upon clear malicious intent have been included.

		THREAT	COMMENTS
Malware & technical threats	**T1**	**Virus**	A type of malware that attaches itself to legitimate programs or files and can replicate to spread to other files or systems when the infected program or file is executed.
	T2	**Worm**	A self-replicating malware that spreads across networks and computer systems independently, often without user interaction.

[25] ISO/IEC 27000:2018
[26] ENISA (2022) Cybersecurity Ontology 1.1 (working paper).

	T3	**Trojan horse**	A deceptive software that appears legitimate but contains malicious code or functionality, allowing attackers to gain unauthorised access or control of a system.
	T4	**Rootkit**	Set of tools and techniques that conceal the presence of malicious software or activity on a compromised system, often granting unauthorised access.
	T5	**Ransomware / wiperware**	Malware that encrypts a victim's files or system and demands a ransom for the decryption key, often used for extortion. Wiperware is technically similar but used for immediate destruction of the data.
	T6	**Keylogger**	Software or hardware that records keystrokes on a computer or mobile device without the user's knowledge, potentially capturing sensitive information.
	T7	**Grayware**	Software that exhibits potentially unwanted or suspicious behaviour, falling between legitimate software and malware in terms of threat level.
	T8	**Fileless malware**	Malware that operates in memory without leaving traditional file traces on a victim's system, making it harder to detect.
	T9	**Adware**	Software that displays unwanted advertisements, often in a disruptive or intrusive manner, to generate revenue for the attacker.
	T10	**Malvertising**	Malicious advertisements that deliver malware or redirect users to malicious websites when clicked, exploiting vulnerabilities in ad networks.
	T11	**Spyware**	Software that secretly collects and transmits user data or activity without consent, often for espionage or advertising purposes.
	T12	**SQL Injection**	SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve.

	T13	**Backdoor**	A hidden entry point or vulnerability in software or systems that allows unauthorised access or control.
	T14	**Browser hijacker**	Software that modifies a user's web browser settings without permission, often redirecting them to unwanted websites or search engines.
	T15	**Crimeware**	Malicious software designed specifically for cybercriminal activities, such as stealing financial information or conducting fraud.
	T16	**Malicious Mobile App**	Mobile applications that contain malware or malicious functionality, posing a threat to the security and privacy of mobile device users.
	T17	**Scraper**	Software or scripts that automatically extract data from websites or online services, often used for illegitimate purposes.
	T18	**Rogue security software**	Fake antivirus or security software that deceives users into believing their systems are infected, then prompts them to pay for a "solution."
	T19	**Cryptojacking**	Illegitimate use of a victim's computer or device to mine cryptocurrencies without their consent or knowledge.
	T20	**Zero-Day**	A software vulnerability that is unknown to the software vendor and has no available patch or fix, making it a valuable target for exploitation by attackers.
Online deception & manipulation	**T21**	**Blackmail**	The act of threatening to reveal sensitive or embarrassing information about a person or organisation unless a demand is met.
	T22	**Defacement**	Altering the appearance or content of a website, typically to convey a message or disrupt normal operations, often a form of digital vandalism.
	T23	**Disinformation**	The spread of intentionally false or misleading information with the aim of deceiving or manipulating individuals or the public.

	T24	**Domain hijacking**	Unauthorised takeover of a domain name, often for malicious purposes, such as redirecting website traffic or holding the domain for ransom.
	T25	**Smishing/Vishing**	Smishing (SMS phishing) involves sending deceptive text messages to trick individuals into revealing sensitive information, while Vishing (voice phishing) is a form of phishing conducted through voice calls.
	T26	**(spear)phishing / whaling**	Phishing is a deceptive practice where attackers send fraudulent emails or messages, often with the goal of tricking recipients into revealing sensitive information. Spear Phishing is highly targeted phishing, while Whaling is phishing targeted at high-profile individuals or senior executives.
	T27	**Steganography**	The practice of hiding data or messages within other data, such as embedding text within an image or audio file, to conceal the existence of the hidden information.
	T28	**Watering hole attack**	A watering hole attack is a targeted attack designed to compromise users within a specific industry or group of users by infecting websites they typically visit and luring them to a malicious site. The end goal is to infect the user's computer with malware and gain access to the organisation's network.
	T29	**DNS poisoning**	In a DNS poisoning attack, an attacker exploits vulnerabilities in the DNS server or its associated infrastructure to inject false or malicious DNS records into the cache. These false records can redirect users to malicious websites or servers.
	T30	**Deepfakes**	Deepfake AI is a type of artificial intelligence used to create convincing images, audio and video hoaxes. The term describes both the technology and the resulting bogus content. Deepfakes often transform existing source content where one person is swapped for another.
	T31	**AI text generators**	AI text generators are used to create highly convincing fake messages, including for phishing emails or human-like responses by bots on social media platforms.

Insider threat	**T32**	**Persuasion**	Persuading existing employees to spy or act out malicious behaviour. This can be done through bribery, ideological conviction or other means of persuasion.
	T33	**Infiltration**	Infiltration of a targeted critical entity by a person with malicious intent. This can be either directly or indirectly via e.g. third-party supporting services.
Physical	**T34**	**Physical damage / sabotage**	Inflicting physical damage to critical infrastructure.
Attacks against availability/integrity	**T35**	**DDoS attack**	Attacking the availability of a website using a network of compromised computers (bots) controlled by a central entity (botmaster).
	T36	**Jamming**	Satellite jamming is a form of electronic anti-satellite (ASAT) attack that interferes with communications traveling to and from a satellite by emitting noise of the same radio frequency (RF) within the field of view of the satellite's antennas. Considered a growing threat in military circles, satellite signal jamming is a routine operation in the ongoing war in Ukraine.
	T37	**AI poisoning**	In an AI poisoning attack, adversaries inject malicious or misleading data into the training dataset.
	T38	**Spoofing**	The act of falsifying data or information to deceive or impersonate a user, system, or device. Spoofing can involve various forms, such as IP address spoofing, email spoofing, or DNS spoofing, and it is often used by attackers to gain unauthorised access, launch phishing attacks, or manipulate data traffic, all while appearing legitimate to the target.
	T39	**Meaconing**	Intercepting and altering GPS or other satellite navigation signals to deceive or disrupt the accurate positioning and navigation of devices, often with the intent to mislead or harm users.

Annex 2.3: Assets

An asset is any tangible or intangible thing or characteristic that has value to an organisation. There are many types of assets. Some of these include obvious things like machines, facilities, patents, and software. However, the term can also refer to less obvious things like services, information, and people, and characteristics like reputation and image or skill and knowledge. The assets here have been largely based on ENISA's mapping of telecommunications assets.[27] As much of the telecommunications infrastructure assets are present in other sectors, most of the blocks presented here are considered to be sector-agnostic while still specific to cyber-related threats. This allows for the asset blocks to be applied in the context of future sectors as well. The rest of the blocks are – and need to be – sector-specific to achieve a holistic overview. Sector-specific blocks of other sectors can thus be added in the future to enrich this set of building blocks.

		ASSET	COMMENTS
Hardware	A1	**Network devices**	Includes transport nodes, switches, routers, bridges, firewalls, gateways, repeaters, IDS/IPS/IRS and mediation devices.
	A2	**Servers**	A computer or computer program which manages access to a centralised resource or service in a network.
	A3	**Personnel terminals**	Includes PCs, laptops, etc.
Software	A4	**Operating systems**	The program that, after being initially loaded into the computer by a boot program, manages all of the other application programs in a computer.
	A5	**Device drivers**	Specialised software that operates a particular computer-connected device—offering a software interface to the hardware allows operating systems and other computer applications to access hardware functionalities.
	A6	**Firmware**	A form of microcode or program embedded into hardware devices to help them operate effectively.

[27] ENISA (2015) *Guideline on Threats and Assets*. https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Article_13a_Guideline_on_Threats_and_Assets_V_1_0.pdf

	A7	**Executable programmes**	A program that causes a computer to perform indicated tasks according to encoded instructions, as opposed to a data file that must be interpreted by a program to be meaningful.
Protocols	**A8**	**Essential addressing protocols**	Includes ARP, IPV5/IPV7, TCP/UDP, DNS, Whois.
	A9	**Routing protocols**	Includes BGP, MPLS, RIP, OSPF, ISIS.
	A10	**Connectivity protocols**	Includes NAT, 6to4, 4in6, PPPoE.
	A11	**Application protocols**	Includes e.g. remote administration-, email-, file transfer-, file transfer-, time-, monitoring-, remote logging-, back/revision control- and lawful interception protocols.
	A13	**Security protocols**	Includes e.g. IPsec, DNSSEC, RPKI, SSL/TLS, HTTPS, FTPS, IMAPS, SSNMP.
Information	**A14**	**System configuration**	The specific definition of the elements that define and/or prescribe what a system is composed of. Includes permissions, security parameters, configuration files, MAC allocations, IP allocations and port allocations.
	A15	**Network topology**	The physical and logical arrangement of nodes and connections in a network. Includes routing tables and network maps.
	A16	**Trending information**	Current information originating from the digital systems.
	A17	**Historical information / statistics**	Includes logs and other types of historical or aggregated information.
	A18	**Inventories**	Includes inventories of hardware, software, infrastructure and configurations.

	A19	**Operational information**	Includes information like status, events, alerts and shortages or disturbance information.
	A20	**Credentials**	A set of login or authentication data that verify a user's identity and grant them access to a particular system or service.
	A21	**User rights policies**	User rights govern the methods by which a user can log on to a system. User rights are applied at the local device level, and they allow users to perform tasks on a device or in a domain. User rights include logon rights and permissions.
	A22	**Lawful interception**	A security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organisations.
Services	**A23**	**Essential addressing**	Includes the domain name system, addressing units, and link layer, internet protocol and transport protocol addressing.
	A24	**Routing**	Includes addressing units, organisational mapping and route and RPKI servers.
	A25	**Applications**	Includes remote administration-, email-, www-, file transfer-, time-, monitoring-, remote logging-, backup/revision control-, issue tracking- and lawful interception applications.
	A26	**Security**	Includes public key infrastructure, identification, authentication and authorisation.
Interconnection	**A27**	**Internet Exchange Points (IXP)**	IXPs are common grounds of IP networking, allowing participant Internet service providers to exchange data destined for their respective networks.
	A28	**Backbone internet provider**	These include leased line and dark fibre providers.
	A29	**Server/data-centre provider**	Responsible for giving IT organisations data backup and recovery, networking, website hosting, data management etc.

Internet infrastructure	**A30**	**Cabling and linking**	Includes wireless (e.g. radio, Wi-Fi, 3/4/5G), wired (copper and fibre, both submarine and terrestrial) and physical connections (e.g. connectors and patch panels)
	A31	**Telecoms Buildings**	Includes data centres, landing points and street cabinets.
	A32	**Power supply**	Electrical device that supplies electric power to an electrical load. The main purpose of a power supply is to convert electric current from a source to the correct voltage, current, and frequency to power the load.
	A33	**HVAC systems**	An HVAC (Heating, Ventilation, and Air Conditioning) system regulates the indoor climate in a facility.
	A34	**Physical security**	Includes backup power supplies and (electric/smart) fences, walls, doors etc.
Human resources	**A35**	**Operators**	Operators may have direct access to secure systems.
	A36	**Administrators**	Administrators may have elevated access to secure systems.
	A37	**Support teams**	Support teams can have elevated access to secure systems or can be persuaded to provide false information to those who do.
	A38	**Developers**	Developers have the opportunity to insert malicious code before any security measures are implemented.
	A39	**Managers**	Managers can have elevated access to secure systems.
	A40	**Trainers**	Trainers can be responsible for teaching best cybersecurity practices and can be manipulated to spread false information.

	A41	**End users**	An individual who ultimately uses an IT product or service, often with a low level of (cybersecurity) expertise.
	A42	**Auditors**	Auditors can have extensive access to secure systems and possess specialised tools for penetration testing.
Electricity generation (OT)	**A43**	**Fossil-fuel power stations (including natural gas)**	Power stations that burn fossil-fuel to generate electricity. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A44	**Nuclear power station OT**	Power stations that use nuclear energy to generate electricity. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A45	**Geothermal power station OT**	Power stations that use geothermal energy to generate electricity. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A46	**Biomass-fuelled power station OT**	Power stations that use biomass fuels to generate electricity. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A47	**Solar thermal electric station OT**	Power station that uses solar energy to generate electricity. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A48	**Hydroelectric power station OT**	Power station that uses water power to generate electricity. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A49	**Wind power station OT**	Power station that uses wind as a source of energy. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A50	**Tidal power station OT**	Power station that uses tidal waves as a source of energy. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.

	A51	**Gas distribution network**	Infrastructure dedicated to the process of delivering gas (e.g. pipelines)
Electricity transmission & distribution (OT)	A52	**Transmission system operators (TSOs)**	TSOs are responsible for maintaining the frequency of the European transmission network by ensuring that production of electricity meets consumption demand at all times. They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
	A53	**Distribution system operators (DSOs)**	DSOs distribute electricity to customers, including residential and small and middle enterprises (SMEs). They rely extensively on Process Control Networks (PCN) and Supervisory Control and Data Acquisition (SCADA) networks.
Electricity market entities	A54	**Electricity exchange platforms**	Set up when the electricity market was liberalised to enable market players to anonymously negotiate same-day or next-day purchases and sales of electricity. Their objectives are to provide an open market, to organise competition and to establish a transparent reference price for market participants.
	A55	**Energy suppliers**	Responsible for the supply of electricity to end customers. Energy suppliers buy electricity on the wholesale market and sell to the end customers.

Annex 2.4: Vulnerabilities

Vulnerabilities are highly context-specific and dynamic. In traditional risk assessments, relevant vulnerabilities are derived from thorough analyses of asset inventories within electricity and telecommunications sector entities. However, this approach is too granular for an EU-level evaluation. Therefore, the vulnerabilities are derived from the research done for this report and are based on shared high-level concerns that were observed during the research. The more traditional technical vulnerabilities are encapsulated in a building block for known vulnerabilities (V1), which correspond to current CVE databases, and unknown vulnerabilities (V2).

	VULNERABILITY	COMMENTS
V1	**CVE**	Any information security vulnerability in critical infrastructure assets that can be found in registries which are being updated by Common Vulnerabilities and Exposures (CVE) Numbering Authorities (CNAs) and Roots.[28]
V2	**Zero-day**	Any information security vulnerability in critical infrastructure assets that was previously unknown to the developers or anyone capable of mitigating it.
V3	**Vulnerable physical infrastructure**	Physical infrastructure failures can lead to unauthorised access, non-functioning communication networks and non-delivery of energy supplies.
V4	**Dependencies on suppliers and managed service providers**	Operators in the telecoms sector are constantly innovating the network technology, which is acquired from third party suppliers and managed service providers. This means that operators are highly dependent on suppliers, for their network equipment and software, but also on MSPs and MSSPs for the maintenance and management of this equipment.
V5	**Dependency on technical expertise**	Technical expertise can be hard to come by for both sectors. Additionally, remote technical maintenance can introduce new attack vectors and problems with authentication.
V6	**Lack of targeted employee training**	ICS engineers often find themselves dealing with Industrial Internet of Things (IIoT) devices that need advanced configurations and third-party support. In many cases, engineers have limited access to the necessary resources for stable configurations. Instead, engineers with only a basic understanding of information technology (IT) systems take it upon themselves to manually configure devices and place them in their networks. Due to no formal training on networking, IT security policies, protocols, and cybersecurity, devices are often misconfigured and riddled with security holes and vulnerabilities. Additional environmental factors in ICS systems, including physical duress, system complexities, and isolation, may result in security gaps or inadequacies in the performance of individual duties and responsibilities.

[28] https://www.cve.org/

V7	**Lack of remuneration opportunities**	Especially energy sector job remuneration can be strictly regulated, making it hard for energy sector entities to attract highly skilled workers.
V8	**Emerging Energy Technologies**	With the rapid evolution of the energy system accelerated by the emergence of new technologies such as distributed energy resources (DERs), electric vehicles, advanced communications (5G+), the threat landscape is rapidly increasing.

Asset 2.5: Harms

ENISA's ongoing work on the Cybersecurity Ontology, which is based on the Cyber harm taxonomy, refers to several forms of harm (H).[29] In addition to these general types of harm, this report includes potential spill-over effects into other sectors as specific harms (SH). During the research done for this report, uncertainties on the chain of actions and responsibilities in a multisectoral crisis surfaced as a major concern. By making explicit any spillover harm, more targeted scenarios to test these particular interdependencies can be created.

	HARM	FROM	TO	COMMENTS
H1	**Physical**	-	-	Physical harm including bodily injury, property damage etc.
H2	**Economic**	-	-	Economic harm including financial loss, loss of shareholder value, job loss, market degradation etc.
H3	**Reputational**	-	-	Reputational harm including a reduced consumer base, deteriorated international relations etc.
H4	**Psychological**	-	-	Psychological or emotional harm including depression, panic/stress, anxiety, self-harm, virtual harm etc.
H5	**Social/societal**	-	-	Harms that hinder the normal functioning of society and government, such as loss of communications, disruption of electoral systems, loss of citizen trust in government etc.

[29] ENISA (2022) Cybersecurity Ontology 1.1 (working paper).

SH1	**Outage**	Electricity	Telecoms	Large scale outages caused by cyberattacks in the electricity sector can have severe adverse effects on the availability of telecommunications.
SH2	**Unavailability of telephone networks**	Telecoms	Electricity	Unavailability of transmission of voice communication over a distance. They can be analogue or digital and can include technologies like circuit-switched systems, which establish a dedicated connection between two parties for the duration of the call, and packet-switched systems, which divide the voice data into packets and transmit them over the network. VoIP is a type of telephone system that uses the internet to transmit and receive calls.
SH3	**Unavailability of radio and television networks**	Telecoms	Electricity	Unavailability of transmission of audio and visual information over a distance. Radio and television signals are transmitted through the air using technologies like broadcasting, which transmits signals over a wide area, and satellite, which uses artificial satellites orbiting the Earth to transmit and receive signals. Cable television uses a network of cables to transmit signals.
SH4	**Unavailability of the internet**	Telecoms	Electricity	Unavailability of any data communications over the Internet due to failures in the backbone infrastructure.
SH5	**Unavailability of satellite networks**	Telecoms	Electricity	Unavailability of satellite communication, which is often used for long-distance communication or in areas where there is no access to other communication networks. It requires the use of satellite dishes and antennas to transmit and receive signals.
SH6	**Unavailability of cellular networks**	Telecoms	Electricity	Unavailability of wireless communication networks that use cells, or small geographic areas, to transmit and receive signals. They rely on technologies like GSM, CDMA, and LTE to transmit and receive data. Cellular networks allow devices like phones and tablets to connect to the internet and make calls when they are not within range of a Wi-Fi network.