Cybersecurity and resiliency of Europe's communications infrastructures and networks

Follow-up to the Nevers Call of 9 March 2022

21 February 2024

NIS COOPERATION GROUP

Table of contents

1. Introduction

1.1. Policy context

The informal Council meeting of Telecom Ministers, which took place in Nevers on 9 March 2022, resulted in a joint call to reinforce the EU's cybersecurity capabilities[1]. It recognised that *"critical infrastructure such as telecommunications networks and digital services are of utmost importance to many critical functions in our societies and are therefore a prime target for cyberattacks"*. The threats to critical infrastructure, exacerbated by Russia's war of aggression against Ukraine, and the risk of critical dependencies in the digital sector, in particular on high-risk suppliers, are of major concerns for the EU. Ensuring the cybersecurity and resilience of those critical infrastructures is a main priority, all the more in the current geopolitical landscape.

The introductory text of the joint call explains that the Ministers, "*due to the current geopolitical landscape"*, want "*to undertake immediate cybersecurity reinforcement actions".* The joint call covers several points, including the resilience of communications networks, the need to strengthen the market via public-private collaboration, the rapid adoption of the Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive[2]), the operationalisation of the EU Cybersecurity Competence Centre, the further strengthening of the EU-CyCLONe and the EU cyber crisis management network (CSIRTs Network), the need to build an ecosystem of trusted cybersecurity service providers and the Emergency Response Fund for Cybersecurity.

Point 4 of the Nevers Call asks relevant authorities, such as the Body of European Regulators for Electronic Communications (BEREC), the EU Agency for Cybersecurity (ENISA), and the NIS Cooperation Group to make recommendations to EU Member States and the Commission based on a risk assessment in order to reinforce the resilience of the EU's communications infrastructures and networks. This call has been reiterated in the conclusions adopted by the Council on 23 May 2022 on the EU's cyber posture[3].

To follow up on this call, the NIS Cooperation Group, with the support of the Commission and ENISA and in consultation with BEREC, conducted a high-level risk assessment on communications infrastructures and networks. This report contains the main threats and vulnerabilities identified in this risk assessment, develops a set of risk scenarios and makes a number of strategic and technical recommendations.

1.2. Objectives and scope

The objective of this report is to follow-up on point 4 of the Nevers Call by assessing risks and formulate recommendations, which, depending on Member States' contexts, could be implemented in the short-term, based on a high-level risk assessment, to address potential gaps in the protection of EU's communications networks and infrastructures. Recommendations also include areas which require further detailed assessment.

The scope of the risk assessment, in terms of threats and scenarios, has been agreed among Member States as follows: the risk assessment and gap analysis focus on the risks of cyber-attacks on the EU's

[1] https://presse.economie.gouv.fr/download?id=92155&pn=2131 - Joint call to reinforce the EUs cybersecurity capabilities-pdf

[2] Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

[3] Council conclusions on the development of the European Union's cyber posture, 9364/22, 23 May 2022.

communications networks and infrastructures (including physical attacks on the networks and information systems, in line with the all-hazard approach of the NIS2 Directive), by a hostile third country, i.e. nation state actors, but also organised crime groups and hacktivists acting in support of nation states.

In this context, the full range of cybersecurity incidents against which the operators need to protect, is not considered, leaving out of scope, for instance, incidents caused by natural phenomena, climate change, human errors, involuntary bugs, misfunctions and misconfigurations, cyber-attacks with a purely financial aim, such as scams and fraud, etc.[4] These other incidents and attacks must however still be considered by the operators when securing their systems and networks. Annex 2 contains a longer list of threats relevant for telecom operators.

The networks and information systems assets in scope of this risk assessment are:

- Public electronic communications networks:
    - Mobile networks, including the signalling networks;
    - Fixed networks;
    - Satellite networks;
- Core Internet infrastructure:
    - Routing of Internet traffic;
    - Submarine and underground cables;
    - Internet exchange points (IXPs) and data centres;
    - Networks and systems used for the provision of Top-level domain registries (TLDs) and Domain Name System (DNS) services.

Out of scope are web certificates and qualified trust service providers, the (so-called over-the-top) number-independent interpersonal communications services, as well as cloud services, unless operators use them to deliver the above-mentioned networks or infrastructures. Also out of scope are the end-user devices, such as smartphones, personal computers (PCs), home routers, and targeted threats on such devices such as smartphone spyware, because they are not an integral part of the networks or infrastructures and generally speaking not under the control of the operators. However, scenarios where such devices are used to attack the networks and infrastructures are considered.

Regarding issues related to 5G networks, the findings of the EU Coordinated risk assessment of the cybersecurity of 5G networks[5] published in October 2019 and the mitigating measures of the EU Toolbox on 5G Cybersecurity (EU Toolbox)[6] of January 2020 remain valid and relevant for the purpose of the present risk assessment.

1.3. Methodology

This report is based on the results of a risk assessment performed by Member States in the NIS Cooperation Group, with support from the Commission and ENISA and in consultation with BEREC, between April 2022 and December 2023. The assessment was conducted building on the methodology of the EU Coordinated risk assessment for 5G networks and the cybersecurity analysis of Open Radio

[4] ENISA, Telecom Security Incidents 2021, 27 July 2022, https://www.enisa.europa.eu/publications/telecom-security-incidents-2021

[5] NIS Cooperation Group, EU-wide coordinated risk assessment of 5G networks security, 9 October 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[6] NIS Cooperation Group, Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Access Networks[7]. The data was gathered through a questionnaire and further discussions with Member States within the NIS Cooperation Group. In the first stage of this process, Member States evaluated the main threats and vulnerabilities linked to the public electronic communications networks and the core Internet infrastructure, and the spill-over effects between these sectors and other critical sectors. Based on these findings, Member States developed a list of risk scenarios. In a second stage, Member States discussed and agreed on a common set of recommendations. This report summarises the outcome of this process.

This risk assessment is complementary to the general, more technical work done by the ECASEC group of EU telecom security authorities, who developed and maintain a framework of technical security measures under the European Electronic Communications Code (EECC), and the work done by the NIS Cooperation Group in the framework of the EU Toolbox. In addition, this report also provides information to the ongoing cross-sector cyber risk evaluation requested by the Council conclusions on the EU's cyber posture[8].

1.4. Existing and upcoming frameworks and measures

There are several policy frameworks and rules in place or in preparation in the EU to protect electronic communications networks.

1.4.1. European Electronic Communications Code (EECC)

The European Electronic Communications Code (EECC) is the main EU policy framework for the telecom sector[9]. Adopted in 2018, these rules apply to all electronic communications services and networks in the EU. Currently, the EECC has been transposed by most EU countries, with the Commission supporting Member States in the implementation process. Security requirements for the telecom sector are contained in Article 40 of the EECC (which replaces Article 13a of the Framework Directive):

- Article 40 asks Member States to ensure that operators take "*appropriate*" cybersecurity measures, and report significant incidents to the national authorities;
- Article 41 asks Member States to ensure that the national competent authority, for instance a telecom national regulatory agency (NRA) or a cybersecurity agency, depending on the national setting, has the powers to audit telecom operators and to enforce measures in case of cybersecurity deficiencies.

In terms of supervision of these security requirements, Member States have taken diverse approaches. For instance, where binding rules apply to mobile network operators, they may cover different types of technical and organisational measures. In Member States where security measures are further clarified in more technical and practical detail (often via secondary legislation), they often refer to the ENISA framework of detailed technical telecom security measures[10], which was developed with all Member States to implement the EECC and contains a detailed list of relevant telecom security measures.

---

[7] NIS Cooperation, Report on the Cybersecurity of Open Radio Access Networks, 10 May 2022, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks

[8] Council conclusions on the development of the European Union's cyber posture, 9364/22, 23 May 2022.

[9] Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code.

[10] ENISA Guideline on Security Measures Under the EECC, last update on 7 July 2021, https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

Besides specific security requirements for individual telecom operators, several Member States have started national initiatives addressing common sector-wide threats and risks, such as national roaming agreements in case of a crisis, mutual aid and assistance to address power supply dependencies, or cross-sector collaboration to address Distributed denial-of-service (DDoS) attacks.

1.4.2. NIS Directive (NIS1 and NIS2)

Security requirements for key parts of the Internet infrastructure, the public core of the open Internet, are contained in the NIS Directive[11], which covers IXPs, DNS providers and TLDs. Under the NIS Directive, entities providing such services, which are identified as Operators of Essential Services (OES) by the respective Member States, are subject to ex-ante supervision under Article 16 of the Directive, and have to take appropriate security measures and to report incidents to the national authorities.

The revised NIS Directive, referred to as NIS2, will repeal and replace Articles 40 and 41 of the EECC, with effect from 18 October 2024, streamlining the cybersecurity policy framework, adding providers of public electronic communications networks and providers of public electronic communications services to the 'digital infrastructures' sector[12]. Under the NIS2 Directive, the Commission has to issue implementing acts on security measures and incident reporting, for several entities under the NIS2 digital infrastructure sector, including for TLDs, DNS, and content delivery networks (CDNs). The NIS Cooperation Group already published detailed technical security measures for TLD registries[13] and is drafting a guideline on security measures for the DNS providers. In addition, the NIS2 allows the NIS Cooperation Group, together with the Commission and ENISA, to conduct EU-wide risk assessments in critical supply chains.

1.4.3. The Resilience of Critical Entities Directive

The Resilience of Critical Entities (CER) Directive[14] covers the physical resilience of critical entities against man-made and natural hazards, in coherence with the NIS2 Directive which covers cybersecurity risks. The Directive focuses on all relevant non-cyber natural and man-made risks, including cross-sectoral or cross-border, that may affect the provision of essential services, such as natural disasters, accidents, public health emergencies and antagonistic threats, including terrorist offences, sabotage and hybrid threats. The Directive covers eleven sectors, including digital infrastructure.

1.4.4. EU Coordinated risk assessment on 5G cybersecurity and EU Toolbox on 5G cybersecurity

The risks associated with 5G have already been identified and analysed in detail by Member States, with the support of the Commission and ENISA, in the EU Coordinated risk assessment published in October 2019. The report identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities (technical and non-technical) and a number of strategic risks associated with 5G

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[12] Member States have to transpose the NIS2 Directive into national law by 17 October 2024. This report therefore refers to the EECC as Member States have not yet transposed the NIS2 Directive.

[13] NIS Cooperation Group, Technical Guideline: Security Measures for Top-Level-Domain Name Registries, 23 March 2022.

[14] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities.

networks. The report presents five risk scenarios with nine concrete risks, linked to insufficient security measures; the 5G supply chain; the modus operandi of main threat actors; interdependencies between 5G networks and other critical systems; and end user devices.

To mitigate these risks, the EU Toolbox recommends a set of strategic and technical measures, as well as corresponding supporting actions to reinforce their effectiveness, which may be put in place in order to mitigate the identified risks. Strategic measures include measures concerning increased regulatory powers for authorities to scrutinise network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities, as well as possible initiatives to promote a sustainable and diverse 5G supply and value chain in order to avoid systemic, long-term dependency risks. Technical measures include measures to strengthen the security of 5G networks and equipment by addressing the risks arising from technologies, processes, human and physical factors. Member States are currently implementing the different measures at national level.
Additionally, ENISA published the 5G Security Controls Matrix[15], which is a comprehensive and dynamic matrix of security controls and best practices for 5G networks, to support the national authorities in Member States with implementing the technical measures of the EU Toolbox.

1.4.5. Cybersecurity Act

The Cybersecurity Act[16], which entered into force in 2019, creates a framework for European cybersecurity certification schemes for products, processes and services. Once in place, certification schemes will also enable producers to demonstrate that they have included specific security features in the early stages of products' design, and users to ascertain the level of security assurance, on an EU-wide basis. The framework provides an essential supporting tool to promote consistent levels of security. ENISA is currently working with an established ad-hoc working group of market stakeholders and Member States on a candidate certification scheme related to 5G, and on another candidate scheme for cloud services. The Implementing Regulation for the European Common Criteria-based cybersecurity certification scheme has been adopted and published in January 2024[17]. In accordance with Article 67, the impact, effectiveness and efficiency of the Cybersecurity Act should be evaluated by 28 June 2024.

1.4.6. Cyber Resilience Act

The Cyber Resilience Act (CRA)[18], for which a provisional political agreement has been reached in December 2023, requires manufacturers of connectable software and hardware products intended for the EU market to ensure that such products are developed in line with security-by-default and security-by-design principles and that their security is maintained throughout their lifetime, for instance through testing and security updates. The CRA covers a wide range of products deployed by network operators, such as routers and switches. It has the potential to increase transparency on the security of such products and facilitate supply chain security management for critical infrastructure

[15] ENISA 5G Security Controls Matrix, 24 May 2023, https://www.enisa.europa.eu/publications/5g-security-controls-matrix

[16] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

[17] Commission Implementing Regulation of 31.1.2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[18] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

covered by the NIS2 Directive, including operators of public electronic communications networks and core Internet infrastructure. The agreement reached is, as of February 2024, subject to formal approval by both the European Parliament and the Council.

1.4.7. Cyber Solidarity Act

The proposed Cyber Solidarity Act[19] aims to strengthen solidarity at Union level through enhancing common Union detection and situational awareness of cyber threats and incidents and reinforcing preparedness and response capacities across the Union against significant or large-scale cybersecurity incidents.

2. Threats and vulnerabilities

This section summarises the main threats and vulnerabilities for the communications networks and infrastructures identified by Member States in the risk assessment. An overview of the main threats and vulnerabilities can be found in annexes 1, 2 and 3.

2.1. Threat actors

The relevant threat actors for the threats and risks identified in this risk assessment are:

- State actors or state-backed actors from a hostile third country: the motivations of this category of threats actors are primarily political;
- Organised crime groups, motivated predominantly by financial gain;
- Hacktivist groups: these threat actors have a political agenda, and may have less sophisticated capabilities. Their goal is to either perform public attacks that help them raise awareness on a particular cause, or to cause damage to organisations they are opposed to. The ultimate goal is to find a way to benefit their cause or gain awareness for their causes;
- Insiders, within an otherwise trusted organisation: an insider may work for an organised crime group, a hacktivist group or a state actor, or have other individual motivations.

However in practice, it is not always clear which actors are behind a certain physical or cyber-attack. Attribution of an attack to a specific actor is notoriously difficult in cybersecurity, because different attackers may be using similar techniques and tools or share attack infrastructure, knowingly and unknowingly. In some third countries, there is not a clear dividing line between state actors and organised crime groups working on behalf of these state actors. Different threat actors may also be collaborating or working for each other. Some attack techniques and tools, which were previously only used by attackers with sophisticated capabilities, such as state actors and organised crime groups, have become easier to use and more common place, and are now being used by less sophisticated attackers, such as hacktivists. There is also a black market of attack tools, where organised crime groups offer advanced tools and services to attackers with limited technical skills. Examples are services like ‘botnets-for-hire’, ‘ransomware-as-a-service’, and ‘DDoS-by-the-hour’.

[19] Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209 final. It should be noted that the proposed Regulation might be subject to changes during the negotiation process.

2.2. Threats

Communications networks and infrastructures are underpinning the functioning of society and economy. They are highly critical and therefore attractive targets for all types of cyber-attacks, for disruptions, espionage and intelligence gathering, but also for fraud and financial crime[20]. The main threats identified in this risk assessment and of strategic importance from an EU perspective are listed below.

T1. Wiper/ransomware attacks - The goal of a ransomware attack is to encrypt files and other data, asking the victim to pay a ransom to receive a decryption key. Ransomware attacks have been dominating the cybersecurity threat landscape in the last couple of years. A wiper attack is often similar in terms of the attacking methods/techniques used, but instead of encrypting the data, the data is simply deleted (or encrypted with a key that is deleted). Ransomware attacks are typically carried out by organised crime groups, while wiper attacks are typically carried out by state actors and/or hacktivists groups.
A sophisticated wiper, like NotPetya[21], could propagate to the data and systems in the infrastructure of network operators, particularly if the telecom/network infrastructure is not sufficiently segregated from the corporate information technology (IT) environment used for office tasks. A large-scale data-destroying wiper or ransomware attack on central infrastructure, or assets underpinning the central infrastructure, could take a long time to recover from.

T2. Supply chain attacks – Supply chain attacks in general involve two steps. First, the network or systems of a supplier are attacked. For instance, a vulnerability is introduced in a piece of hardware or software sold by the supplier. In the second stage of a supply chain attack, the actual target is attacked, for example, an operator of communications networks or infrastructures. Supply chain attacks may be used by state actors, but also by organised crime or hacktivist groups.
Supply chain attacks can have a lot of impact, because they allow an attacker to target many operators at once. For example, in the SolarWinds case, one supply chain attack was used to target hundreds of critical entities in the EU and across the globe. Another reason why supply chain attacks are an attractive method for attackers is the fact that attackers may be able to circumvent the defences and detection capabilities of the telecom operator or service provider, by first targeting the supplier, which may have weaker defences and detection capabilities. The potential impact of supply chain attacks is exacerbated by the fact that suppliers often have regular (e.g. daily) access to equipment for the purpose of technical support and maintenance.

T3. Attacks on a Managed Service Provider (MSP)[22], Managed Security Service Provider (MSSP) or other third-party service provider - In a cyber-attack on a M(S)SP[23] or another third-party service provider, the attacker targets the telecom operator or service provider indirectly. Similar to supply chain attacks, this type of attack is typically used to circumvent the defences and detection capabilities of the telecom operator or service provider. State actors, organised crime groups and hacktivists could carry out such attacks, but also attackers with less sophisticated capabilities, depending on the security posture of the M(S)SP or third-party service provider. M(S)SPs may have regular (e.g. daily) access to equipment for the purpose of technical support, maintenance and updates.

[20] There are many other threats which operators may need to consider and which are out of the scope of this risk assessment, for instance natural phenomena, climate change, human errors, involuntary bugs, misfunctions and misconfigurations, cyber-attacks with a purely financial aim, such as scams and fraud, etc.
[21] https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware
[22] MSPs can be for example equipment suppliers helping the operators solve bugs on their networks.
[23] Managed Service Provider or Managed Security Service Provider.

T4. Network intrusions - Network intrusions are used for espionage, exfiltration or the preparation of further cyber-attacks. Network intrusions are stealthy by nature and hard to detect but their impact can be long-lasting and unpredictable. Network intrusions are typically carried out by state actors, for espionage purposes, but organised crime groups may also use them to gain valuable information, which they can sell on the black market, use to blackmail the victim, or to help them for another cyber-attack.
Public electronic communications networks are highly attractive targets for espionage. Detecting and preventing network intrusions is an important challenge for telecom operators, particularly when it comes to espionage attacks and network intrusions from sophisticated state actors. As an example, according to the United States (US) Cybersecurity and Infrastructure Security Agency along key US and international government agencies, malicious activity by a People's Republic of China (PRC) state-sponsored cyber actor, known as Volt Typhoon, has compromised US critical infrastructures seeking to preposition itself on IT networks for disruptive or destructive cyberattacks against US critical infrastructure.[24]

T5. Distributed denial-of-service (DDoS) attacks - DDoS attacks are highly visible cyber-attacks which flood networks or systems with traffic so they become unavailable. DDoS attacks can be carried out by state actors, for example to silence activists or disrupt a foreign government, by organised crime groups, for example to extort, or hacktivists groups and script kiddies acting in support of a state actor. The level of preparation and protection against DDoS attacks varies. In general, telecom operators are often well equipped to handle DDoS attacks, being in control of the networks. This may not always be the case for operators in other critical sectors, although there are dedicated (commercial) services in the market to protect from large-scale DDoS attacks.

T6. Physical attack/sabotage - Physical attacks and sabotage targeting data centres, underground cables, submarine cables, cable landing points or satellite stations are a concern because much of this infrastructure is exposed and difficult to supervise, e.g. submarine cables laid in international waters. Some Member States rely on a few main international backbone connections, and have limited and suboptimal solutions to redirect traffic. A coordinated sabotage action could have a significant impact on the functioning and continuity of the networks.
A large-scale coordinated attack on submarine cables which would damage several cables at once could be difficult to mitigate and may have long-lasting impact. Firstly, repairing submarine cables is difficult in particular when they are in deep waters or under the ice. Secondly, the number of cable repair ships is limited and their availability-on-demand is not guaranteed.

T7. Nation state interference on supplier - A state actor in a third country may exercise pressure on suppliers in order to introduce backdoors or vulnerabilities to facilitate subsequent cyberattacks, serving their national interests. The degree of exposure to this risk is strongly influenced by the extent to which the supplier has access to the network/infrastructure and by the risk profile of the individual supplier[25]. Presence of the high-risk supplier's technology in the Member State's infrastructure can increase the risk for significant disruptions to network operations, whether due to disconnection of supplies, failure to provide service, failure to provide updates, or the use of backdoors in components. Suppliers may have regular (e.g. daily) access to equipment for the purpose of technical support, maintenance and updates. Another example of supply chain interference is the possibility of extortion from a third country through the threat of terminating updates or service in general.

---

[24] https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf

[25] Although this attack may look similar to a supply chain attack in terms of methods and techniques, the difference is that, in a supply chain attack, the supplier is not involved and has no knowledge of the attack.

Infrastructure hosted in third countries (i.e. outside the EU) may be more exposed to interference by a third country, for example, if a network operation centre (NOC) or security operation centre (SOC) is hosted outside EU borders. Similarly, the same applies where a submarine cable crosses international waters, or lands in a third country.

T8. Interconnection attacks - Interconnection attacks target the interconnections between operators, for example the mobile network interconnections, also referred to as signalling or SS7, which is used by operators to find out where a specific mobile phone user is connected, or the global routing of Internet traffic, via the Border Gateway Protocol (BGP), which carries information about what are the preferred routes to take when sending Internet traffic from one place to another. Interconnections are by nature exposed to operators and providers outside the EU, which makes them more vulnerable to cyber-attacks by hostile third countries.
In the same category are attacks on the legacy telephony protocols, such as smishing and vishing, which allow attackers to spoof the phone number changing the calling line identification (CLI), and in this way hide malicious calls and messages behind a trusted phone number.

T9. Power cuts affecting communications networks and infrastructures - Power cuts are a major concern for telecom operators, whatever their nature. A cyber-attack might target the EU's power grid, taking it down locally, in order to cause outages of the radio network, in a particular region, for example a border region. Power cuts could also affect submarine cables which rely on repeaters.

T10. **Insider threats -** Telecom operators and service providers can be targeted by insiders, for example compromised personnel, who operate as agent for a nation state or an organised crime group. The impact of these attacks depends on how much access the insider has to sensitive data or critical infrastructure. This risk may be aggravated if operators outsource key business processes, particularly to third countries.

2.3. Vulnerabilities

There are several groups of vulnerabilities and dependencies which increase the risks of the above-mentioned threats, and may make them more difficult to mitigate for operators, or otherwise present a challenge for operators to secure their networks. The main groups of vulnerabilities identified during this risk assessment are:

Vulnerability 1 (V1). Vulnerable network equipment - Communications networks and infrastructures are composed of thousands of pieces of network equipment, located in the core network, but also in the access network. If this network equipment is not securely configured or has software vulnerabilities, they can allow an attack to gain a foothold within the operator's network. It is a challenge for operators to keep their network equipment secure, to patch known software vulnerabilities on time, to apply secure configurations and to apply general hardening measures. In particular, when suppliers do not apply secure software development, security-by-design and secure-by-default principles, it becomes even harder for operators to secure their network equipment.

V2. Vulnerable routing and interconnection protocols - Communications networks and infrastructures are essentially implementing a number of Internet routing and interconnection protocols, spanning across different networks and operators. Some of these protocols were designed several decades ago, without considering the risk of cyber-attacks, for example from rogue operators. While some of these network protocols have since been retrofitted with security enhancements, operators do not always apply these good practices to prevent these cyber-attacks.
For example, operators do not always apply egress (outbound) filtering to prevent reflection/amplification DDoS attacks. Operators also do not always implement security good

practices for BGP routing (specifically Route Origin Authorizations (ROA) and Route Origin Validation (ROV)[26]), which allow for route leaks and route hijacks. Operators do not always apply security measures to detect and block rogue signalling traffic in vulnerable mobile network interconnection protocols such as SS7, which are used for signalling and roaming. Also, the legacy protocols used for telephony allow for smishing and vishing attacks, which have been used to target two-factor authentication mechanisms relying on Short Message Service (SMS)[27].

V3. Vulnerable network management and operation - While most operators have a strong awareness of the risks posed by cyberattacks and the necessity to defend against threat actors, some networks are found vulnerable due to the insufficient implementation of both organisational and technical security measures. For example, an improper information security management system, including insecure administration practices (e.g. for management and network orchestration (MANO), for customer premise equipment (CPE), weak encryption, insufficient secret complexity and diversity), or insufficient security event monitoring may put networks, operators, and ultimately their clients, at risk.

V4. Vulnerable end-user devices - A single operator may be providing Internet access to millions of customers who are connecting their end-user devices to the Internet. If these end-user devices are vulnerable, for example unpatched home routers, vulnerable Internet of Things (IoT) devices or legacy PCs, they can be used by attackers to create large botnets for all sorts of other attacks. For instance, large botnets of compromised end-user devices have been used to create very large DDoS attacks, which are hard to mitigate, because the attack traffic comes from many different networks and the attackers can hide the real origin of the attack. There is also a risk that vulnerable end-user devices are used for espionage attacks.
A specific concern is the weak security of CPE, such as home routers, which provide the customer access to the Internet connection. These home routers are often provided by the operator as part of the Internet connection, but the management of these devices is in part the responsibility of the customer. For example, in the case of the Mirai botnet, an attacker compromised and disconnected a million home routers[28]. More recently, Russian state actors compromised routers belonging to private individuals and small and medium-sized enterprises (SMEs), adding them to an attack network of thousands of compromised devices[29].

V5. Vulnerable physical infrastructure - Communications networks and infrastructures also rely on physical infrastructure. While some physical infrastructure assets are implemented redundantly, some assets can be highly critical, such as large data centres, and areas of high concentration of cables (so-called 'chokepoints') such as the Suez-canal. Physical sabotage attacks can be used to target these physical infrastructure assets.
A specific concern are the submarine cables which, while redundant, are also exposed and hard to protect. At national level, the responsibility for protecting these submarine cables is not always clear and typically involves several different national authorities, including the telecom regulator, the cybersecurity agency, but could also include the coastguard, military, etc. When damaged, submarine cables are hard to repair, requiring specialised vessels which are scarce. In some areas, powerful

[26] Both ROA and ROV are based on the Resource Public Key Infrastructure (RPKI) framework. See for general BGP good practices https://MANRS.org and https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp
[27] Example of impact from smishing: https://www.wired.com/story/phone-spear-phishing-twitter-crime-wave/
[28] Mirai was an attack campaign where attackers created a large botnet of home routers, which were subsequently used for large-scale DDoS attacks: https://securityledger.com/2016/11/report-millions-and-millions-of-devices-vulnerable-in-latest-mirai-attacks/
[29] https://english.nctv.nl/binaries/nctv-en/documenten/publications/2022/07/04/cyber-security-assessment-netherlands-2022/Cyber+Security+Assessment+Netherlands+2022.pdf

icebreakers may be needed to repair submarine cables, which are even more scarce or belonging to a third country.

V6. Dependencies on suppliers and M(S)SPs - Operators are highly dependent on suppliers, with regard to both the provision of network equipment and software, and its maintenance and management. Such dependencies for the maintenance and management of this equipment also exist on M(S)SPs. Suppliers and M(S)SPs often have regular (i.e. daily) access to equipment for the purpose of technical support, maintenance and system updates. This means that the risk profile of suppliers and M(S)SPs used by operators is an essential factor to take into account. Operators are also increasingly using cloud and data centre services for the delivery of their services, which makes them more dependent on the security of these cloud services and data centres. In addition, the lack of standards enabling interoperable interfaces for network equipment could increase the dependency.
As regards submarine cables, there are only few main worldwide suppliers, of which only one is EU-based.

V7. Power supply dependencies - Communications networks and infrastructures are highly dependent on other entities providing critical information & communication technology (ICT) assets. The power grid is one of the most critical dependencies for the telecom sector. An energy outage could impact the mobile networks, and to some extent, also the fixed networks as street cabinets often rely on the power grid.
Conversely, the power grid is increasingly dependent on ICT solutions and network connectivity. This means that a network outage could also affect the electricity grid and make repair and recovery more difficult.

V8. Dependency on technical expertise - An important dependency for operators in this sector is the availability of technical experts and specialised personnel. The rapid technology evolution in the sector, combined with the security needs, makes it a challenge for operators to find adequately skilled personnel.
A lack of technical experts complicates the efforts of operators to mitigate some of the above-mentioned vulnerabilities, such as cyber-attack-vulnerable network devices, and in turn, increases the dependency on suppliers and M(S)SPs.

2.4. Spill-over effects

Cyber-attacks on the telecom sector would have impact and spill-over effects in many critical sectors. Network outages, for instance, would disrupt the overall economy and society:

- Access to emergency services and numbers, public warning systems would be disrupted, which would complicate emergency response in crisis situations. Additionally, the emergency services themselves may be disrupted, if their communications and systems depend on the public mobile networks.
- Digital payments would be disrupted, which in turn would affect access to public transport, toll roads and the possibility of people to buy essentials such as food. Many businesses which rely on online services would be disrupted.
- Secure communications between Member States, including exchanges of sensitive information, could be disrupted, with potential consequences on national security.
- Other critical sectors would be disrupted. For example, the health sector could be disrupted in case of a long-lasting network outage, because many hospitals rely on online services for scheduling appointments. While critical IT and operational technology (OT) systems in critical sectors often have a manual/offline backup, in case of a connectivity failure, the manpower may not always be available to transition to manual/offline operation.

- Recovery of the energy grid and energy supply would be more difficult if there are large-scale network outages (spill-back).

Espionage attacks, compromising sensitive data, could also have a major impact. For example, it could impact the safety of individuals, the security of systems or networks used in other critical sectors, and/or on the confidentiality of intellectual property, trade secrets, etc.

3. Risk scenarios

This section describes the main risk scenarios of strategic importance from an EU perspective, according to their level of risk identified by Member States. Annex 4 maps the risk scenarios to threats, vulnerabilities and recommendations. The 2019 EU Coordinated risk assessment already identified nine risk scenarios, specifically for 5G networks, which remain valid and relevant for the purpose of this risk assessment[30]. The identified risk scenarios cannot be assessed in isolation and independently of each other. Given the complexity of critical infrastructure such as telecommunications networks and digital services and their interdependencies, there is a wide variety of attack sectors. It is therefore possible for several risks to materialise at the same time, and can result in even greater damage.

Risk scenarios with a high level of risk

R1. Wiper attack to cause a large-scale network outage - An organised crime group, colluding with a state actor, launches a sophisticated wiper/ransomware attack (like NotPetya), using first one or more zero-day vulnerabilities, to perform a network intrusion, and then dropping a piece of wiper/ransomware malware, which wipes key data, configurations and software. The attacker targets several telecom operators at once, wiping the virtualised network functions of several telecom operators across the EU, as well as wiping the core network functions of a satellite networks provider. There are network outages across the EU and there is unexpected impact across the economy. Some operators are able to restore backups and bring their networks back online within a day, but several telecom operators will take several days to restore their systems and networks.

R2. Supply chain attack to gain access to the infrastructure of operators – An organised crime group executes a supply chain attack, by first targeting a supplier or M(S)SP with a weak security posture, in the supply chain of an operator, and then targeting several telecom operators at once. The supplier or M(S)SP has a weak security posture and deploys a small but critical piece of software to several operators. In the first stage of the attack, the attacker alters source code or changes a system configuration file, introducing a new vulnerability in the software or an insecure security system configuration (such as an altered firewall rule). The organised crime group collaborates with a state actor from a hostile third country and sells the 'backdoor' access. In the second stage of this supply chain attack, the attacker uses the vulnerability to gain access to the network infrastructure of several EU telecom operators. The attacker uses this access to move laterally and compromise several other systems. The goal of the attacker is not to disrupt the communications infrastructures, but to perform espionage on subscribers of these operators. After several months, the supply chain attack is detected, because one operator realises there is an unknown vulnerability in the software of the supplier or M(S)SP. An investigation by cybersecurity agencies leads to the conclusion that the software

[30] The nine risk scenarios resulting from the 2019 EU Coordinated risk assessment are: Misconfiguration of networks; Lack of access controls; Low product quality; Dependency; State interference through the 5G supply chain; Exploitation of 5G networks by organised crime; Significant disruption of critical infrastructures or services; Massive failure of networks due to interruption of electricity supply or other support systems; IoT exploitation.

vulnerability was not a mistake but introduced on purpose by a cybercrime group, and later exploited by a state actor for espionage purposes. As with many espionage attacks, the impact of the attack is not immediately felt, but it affects national security and the security interests of the Union.

R3. Network intrusion as a preparation for future cyber-attacks - An organised crime group, which normally only performs ransomware attacks, has managed to perform several network intrusions inside the infrastructure of several EU telecom operators in different EU countries. The crime group has not directly exploited this access, but instead created backdoors in the infrastructure and sold the backdoor access to a state actor. The goal of the state actor is to use the backdoor access later for future cyber-attacks, for instance eavesdropping on critical communications and the geolocation of specific subscribers, or to cause disruptions. The impact of this network intrusion is not immediately known, because it is used as a preparation for future attacks. It takes several months for the affected operators to detect the intrusion, because information sharing about threats and indicators of compromise (IOCs) is slow and limited within country borders.

R4. Third country interference on a supplier, M(S)SP or submarine cable - An EU telecom operator depends heavily on a supplier or M(S)SP in a third country, for a piece of software and for performing certain functions of their security operations centre. A state actor from a hostile third country exercises pressure over this supplier under its jurisdiction, to gain access to sensitive information handled by the supplier or M(S)SP, about the network/infrastructure assets of the EU telecom operator. In this case, the state actor gets a clear map of the critical ICT systems, what software versions they are running, and how they can be attacked. The state actor subsequently uses this information to conduct further attacks directly on the telecom operator, exploiting these vulnerabilities to conduct espionage attacks. In addition, the state actor threatens to put constraints on the supplier under its jurisdiction, and in this way tries to influence national security and foreign policy decisions of the EU country(ies) where telecom operators are dependent on this supplier.

Alternatively, the state actor interferes with a supplier or a consortium operating several (land and submarine) cables and landing points, which are critical for international connections of some EU Member States. The state actor exercises pressure on the supplier of these cables to gain access to sensitive data transmitted over the cable, for the purpose of espionage. While tapping of submarine cables on the seabed is difficult, tapping at the landing points is feasible.

R5. DDoS attack to cause a large-scale network outage - A state actor launches, with the support of hacktivist groups, large-scale DDoS attacks on the communications networks and infrastructures of several EU countries, with the aim of causing social unrest and disrupting economic activities, e.g. the disruption of digital and online payments, disruption of logistical processes, and digital services. While some operators are able to stem the flow, several operators across the EU do not manage to deal with the attack. The first DDoS attack waves cause large-scale outages for several hours. Some of the better equipped operators manage to mitigate the attack and restore access to the most critical customers, but, throughout the day, network outages affect the economy and society across the EU. The attackers use DNS amplification and a pre-prepared botnet of infected home routers and other end-user devices.

R6. Coordinated physical sabotage/attack on digital infrastructure - A state actor launches a coordinated physical sabotage/attack on multiple redundant but geographically closely located submarine cables, a cable landing station, and a large data centre which houses an IXP or functions as a hyperconnectivity hub. In addition, the state actor also conducts a physical sabotage/attack on a repair vessel. The intent of the attacker is to cause large-scale network outages, affecting Internet connectivity of an entire region in the EU that depends mostly on submarine cables. The submarine

cable attack take place in international waters, where it is unclear who has legal jurisdiction. The incident lasts several days, because repair is slow and there is a limited number of repair vessels.

R7. SS7 signalling attack to intercept communications and geolocation of target persons - A state attacker or organised crime group exploits vulnerabilities in the SS7 signalling protocol[31], to intercept the communications, phone calls and messages, as well as the approximate geolocation of a few specific mobile network subscribers, i.e. target persons of interest. Some of them have been using special mobile phones, with hardened software, but this does not thwart the attack, because the attack happens at the signalling protocol layer. The attacker uncovers sensitive information from the communications, and uses the geolocation information to launch physical attacks that threaten the safety of the target persons. The attack itself is not detected by the operators, because it is a small-scale attack and the operators have not implemented SS7 firewalls to block or detect this traffic. The physical attack is only detected much later because one operator notices a pattern. Only months later, and after a thorough investigation by security agencies, the connection between physical attacks and the malicious SS7 attack is made.

Risk scenarios with a high to moderate level of risk

R8. Smishing attack to gain access to critical systems in other sectors - A state actor executes a few targeted smishing attacks to capture two-factor codes, over a period of several weeks, to get access to specific systems used by several entities in critical sectors, such as the energy and transport sector. The impact of this cyber-attack is not fully understood at first, because the attacker uses valid two-factor authentication codes, and the attack is not always detected by the entity. The attacker uses the initial access to move laterally and plant backdoors in other systems. It requires a concerted effort of several months by multiple cybersecurity agencies to analyse the attack, to understand the final targets, and to help these entities mitigate the impact and prevent a re-occurrence by switching to other two-factor authentication methods[32].

Risk scenarios with a moderate level of risk

R9. Power cut to cause a regional network outage - A state actor targets the power grid in a certain region, causing a regional outage of the mobile and fixed network connections, because the power cut causes a large-scale outage of mobile network antennas, street cabinets, and also affects some transport networks and core infrastructure. Some network connections continue to work in the first hours of the incident, because antenna sites are battery-powered. However, because the damage to the power grid is substantial and the power cut takes several days, those batteries get depleted. As the networks are degrading, the disruption in the region worsens, affecting public transport and point of sale in toll roads causing traffic jams. The technical teams from energy companies and telecom operators, which are working to mitigate the power cuts, are also affected by these network outages. Operators rush to bring diesel generators to the area, to sustain the operation of a few larger connectivity sites, but they are not enough to sustain all the traffic.

Risk scenarios with a low level of risk

R10. Interconnection attack to cause a large-scale network outage - A state actor uses a network operator in a third country to launch an attack on the BGP to hijack network traffic, causing large-scale network outages, particularly affecting the connectivity with large overseas websites and cloud

[31] SS7 is used for example to enable international roaming between operators in different countries.

[32] While phishing is a common attack vector, it is out of scope of this risk assessment (Phishing uses email, which is an over-the-top communication service out of scope of this risk assessment).

services. The network outages cause disruptions across the EU's society and economy for several hours, because many citizens use these websites and services. Some entities in critical sectors are affected as well because they rely on these overseas websites and cloud services. Larger operators are able to blacklist the rogue network operator, restoring normal Internet traffic for some citizens and entities in critical sectors within hours. Some operators, whose prefixes have been hijacked, lack the technical expertise to make the necessary changes to get traffic back to their networks, which means many businesses and citizens remain affected throughout the day. Subsequently the national cybersecurity agency spends several days working with operators, collecting and sharing good practices on how to better implement this protocol[33].

4. Recommendations

This section contains a number of recommendations for Member States, the European Commission, ENISA and BEREC, to mitigate the risks that have been identified. It is important to note that these recommendations are taking into consideration what is already in place at national and EU level to mitigate some of these risks (see also section 1.4.):

- **EECC and NIS Directive:** Under the EECC and the NIS Directive, national authorities supervise operators of public electronic communications networks and operators of core Internet infrastructure, assess threats and cybersecurity risks for their services, and take appropriate security measures, including technical and organisational measures to protect the security and resilience of services and networks. A complete and detailed set of technical and organisational measures can be found in the ENISA technical guidelines on security measures under the EECC[34].
- **EU Toolbox:** The EU Toolbox contains strategic and technical measures which Member States should implement to ensure that 5G networks are secure and resilient.

In addition, the **CRA** aims to address the cybersecurity of connected devices. Once adopted, the CRA will also provide a legal framework for improving the cybersecurity of customer premise equipment which would help mitigating several of the earlier-described risks, such as the risk of attackers forming large botnets for DDoS attacks (see risk scenario R5).

Moreover, the proposed **Cyber Solidarity Act** aims to improve preparedness, detection and response to cybersecurity incidents across the EU. Among other things, it proposes to build a network of Security Operation Centres (SOCs) interconnected across the EU, to improve detection of cyber threats and improve situational awareness. Better detection and better situational awareness would help mitigating several of the risks described.

A table with the strategic and technical recommendations, mapped to stakeholders and risk scenarios, can be found in annex 5.

[33] The same attack can also be used for eavesdropping.
[34] ENISA Guideline on Security Measures Under the EECC, last update on 7 July 2021.

4.1. Strategic recommendations

4.1.1. Resilience of international interconnections

Strategic Recommendation (SR) 1. Assess resilience of international interconnections and clarify mandate – Member States should assess the security and resilience of international interconnectivity, interconnections and satellite connections. Member States should clarify which national authorities have the mandate to supervise these international interconnections. In particular, as regards submarine cables, the Commission asked Member States to describe their submarine cables, who has the responsibility to protect them, and who has the mandate to supervise the cable operators, in the context of the Commission Study on Resilience of Undersea Cable Infrastructure requested in the Council Recommendation of 9 December 2022[35]. To complement those developments, Member States should map foreign jurisdiction obligations imposed upon operators which have submarine cables on their territory.

SR2. Assess criticality, resilience and redundancy of core Internet infrastructure, such as submarine cables – In general, it seems that there is a lack of information and understanding about the criticality, resilience, and redundancy of core Internet infrastructure, including submarine cables. For instance, as regards submarine cables, there is little information about their capacity, if the current network architecture is sufficiently redundant, if there is failover capacity when an incident happens, if there is sufficient repair capacity, if submarine cable operators are taking appropriate security measures, etc. To address this recommendation, the European Commission already looked at the criticality and resilience of submarine cables in the context of the Study on Resilience of Undersea Cable Infrastructure requested in the Council Recommendation of 9 December 2022. In addition, ENISA published a report which highlights some of the challenges around the protection of submarine cables[36].

4.1.2. Supply chain risks

Supply chain risks related to 5G networks, especially related to high-risk suppliers, are addressed in the EU Toolbox. The strategic measures of the EU Toolbox remain relevant and valid for the purpose of the present risk assessment. The second Progress Report on the EU Toolbox implementation[37] published on 15 June 2023 highlights that a vast majority of Member States have reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox. However, some of the key measures have not been fully implemented yet in all Member States. Given the importance of the connectivity infrastructure for the digital economy and dependence of many critical services on 5G networks, Member States should achieve the implementation of the EU Toolbox without delay. In particular regarding suppliers, the report recommends that Member States:

- Ensure they have comprehensive and detailed information from MNOs about the 5G equipment currently deployed and about their plans for deploying or sourcing new equipment;
- In assessing the risk profile of suppliers, Member States should consider the objective criteria recommended in the EU Toolbox. In this context, it is evident that 5G suppliers exhibit clear

[35] Council Recommendation 15623/22 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, 9 December 2022.

[36] ENISA, Undersea cables – What is at stake?, 31 August 2023, https://www.enisa.europa.eu/publications/undersea-cables

[37] NIS Cooperation Group, Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, 15 June 2023, https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

differences in their characteristics, in particular as regards their likelihood of being influenced by specific third countries which have security laws and corporate governance that are a potential risk for the security of the Union. Furthermore, designations made by other Member States concerning high-risk suppliers should be taken into account, with a view to promote consistency and a high level of security across the Union;

- Based on the assessment of suppliers, Member States should impose restrictions on high-risk suppliers without delay, i.e. considering that a loss of time can increase vulnerability of networks in the Union and the Union's dependency on high-risk suppliers, especially for Member States with a high presence of potential high-risk suppliers[38];
- To effectively mitigate risks, Member States should ensure that the restrictions cover critical and highly sensitive assets identified in the EU Coordinated risk assessment, including the Radio Access Network;
- For types of equipment covered by the restrictions, operators should not be allowed to install new equipment. If transition periods are allowed for the removal of existing equipment, they shall be defined to ensure the removal of equipment in place within the shortest possible timeframe, taking into account the security risk of keeping equipment from high-risk suppliers in place, and should not be applied to allow the continued deployment of new equipment from high-risk suppliers.

SR3. Create transparency on the landscape of suppliers and M(S)SPs used for fixed networks, fibre technology, submarine cables, satellite networks and other important ICT suppliers – There is a need to collect systematic and thorough information about the suppliers and M(S)SPs for mobile networks (see recommendation of the second Progress Report above), fixed (fibre) networks, satellite networks, submarine cables and other important ICT suppliers. Member States competent authorities, together with BEREC, should map the relevant supply chains, collect and aggregate information about the operator's reliance on suppliers and M(S)SPs for fixed (fibre) networks, satellite networks, submarine cables and other important ICT suppliers in order to identify any potential supply chain vulnerabilities and dependencies. In addition, national competent authorities in the Member States should exchange information about suppliers, and together with ENISA and in consultation with BEREC, should prepare an aggregated mapping of the supplier landscape for fixed (fibre) networks, satellite networks, submarine cables, and other important ICT suppliers. This would allow for a discussion about if there is a need to look at the risk profile of suppliers in these sectors and potential risks of dependencies.

4.1.3. Situational awareness and operational collaboration

SR4. Involve the sector in cyber exercises and operational collaboration – Operational collaboration with operators of public electronic communication networks and core Internet infrastructure is important to be able to mitigate large-scale cyber-attacks. ENISA should regularly involve these operators in cyber exercises. The Commission and ENISA should consider how to involve the region's Internet Registry (RIPE NCC) and large Internet exchange points in operational collaboration.

SR5. Foster information sharing and improve situational awareness about threats for the operators – For a timely and efficient response to cyber threats, it is important to improve situational awareness within the sector and to foster information sharing between operators in this sector and with other critical sectors. Member States should foster information sharing about threats, for instance by supporting Information Sharing and Analysis Centres (ISACs), and where needed, support the creation

[38] Based on the definition of 5G networks provided in the Commission Recommendation of 26 March 2019 on the cybersecurity of 5G networks, the EU Toolbox also includes legacy networks elements based on previous generations of mobile and wireless communications technology such as 4G or 3G.

of national, regional and multi-country SOCs. The tactics, techniques and procedures used by attackers during known past high-profile attacks should be studied to make sure corresponding safeguards are in place to prevent replay. The Commission should provide funding support via the DIGITAL Europe Programme for the creation of ISACs and SOCs. In addition, network operators should be encouraged to implement an information security management system aligned with both generic and sector-specific best practices (e.g. ISO/IEC 27001[39], NIS2 Directive).

4.1.4. Support operators with technical measures

SR6. Provide funding support through relevant funding programmes to operators for technical measures against cyber-attacks in their networks – The European Commission should provide support possibilities for Member States and entities in the telecom and digital infrastructure sectors with implementing technical measures that partially mitigate the earlier described risks, such as technical audits and scans of networks, the creation of interconnection firewalls, anti-phishing filters, for example via foreseeing funding possibilities under the DIGITAL Europe Programme.

4.1.5. Physical attacks on digital infrastructure

SR7. Exchange good practices among national authorities about physical attacks on digital infrastructure - Cyber-attacks on digital infrastructures, such as public communications networks and core Internet infrastructure, are in the scope of the NIS Directive (NIS1 and/or NIS2) and the CER Directive. However, the national competent authorities under the NIS Directive could learn from good practices developed by other national authorities, for instance in the context of protecting other critical infrastructure from physical attacks. The competent national authorities responsible for the public electronic communications networks and core Internet infrastructure under the NIS Directive, should collaborate with the CER competent authorities to exchange good practices about how to mitigate physical attacks on critical infrastructure.

SR8. Extend physical stress testing of critical infrastructure to include digital infrastructure – In its Recommendation of 9 December 2022[40], the Council asked Member States to encourage and support critical infrastructure operators, at least in the energy sector, to conduct stress tests, where relevant. Such tests fall within the competence of Member States, who should encourage and support critical infrastructure operators to conduct such tests, where assessed as beneficial and in accordance with their national legal frameworks. Member States could extend this stress testing to critical digital infrastructure, such as critical submarine cables, satellite infrastructure, critical underground cables and large (critical) data centres.

4.2. Technical recommendations

4.2.1. Mobile and fixed networks

The technical measures of the EU Toolbox remain relevant and valid for the purpose of the present risk assessment. The second Progress Report on the EU Toolbox implementation showed that Member States have all reported taking steps to reinforce technical requirements. The focus now should be on enforcing these measures and ensuring a strong level of supervision. Particular attention should be given to technical measure 01 of the EU Toolbox (Ensuring the application of baseline security

[39] ISO/IEC 27001 is a standard which defines requirements that an information security management system (ISMS) must meet.

[40] Council Recommendation 15623/22 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, 9 December 2022.

requirements) which provides a minimum set of security requirements to be fulfilled by public electronic communications networks and services, technical measure 08 (Raising security standards in suppliers' processes through robust procurement conditions) and the incident management aspects of technical measure 05 (Ensuring secure 5G network management, operation and monitoring).

Technical Recommendation (TR) 1. – Continue supporting Member States with the implementation of the technical measures of the EU Toolbox – ENISA should continue supporting Member States with the implementation of the technical measures of the EU Toolbox. In addition, Member States are also recommended to make use of ENISA's 5G Security Controls Matrix as a tool to support the implementation of the technical measures.

TR2. Exchange good practices to support the detection and prevention of signalling attacks – Mobile network signalling and roaming protocols used in 2G, 3G, 4G and 5G networks, like SS7, Diameter and GTP-C, are vulnerable to a wide range of targeted cyber-attacks. State actors in third countries, as well as organised crime groups, could use these vulnerabilities to geolocate and eavesdrop individuals or to target authentication mechanisms systems in other critical sectors. Member States should raise awareness about signalling attacks and ensure that telecom operators are taking appropriate measures to prevent them[41].

TR3. Exchange good practices to mitigate smishing attacks – In the last couple of years, there has been a wave of smishing (and vishing) attacks, which are used by attackers mainly (but not only) to target two-factor authentication codes sent via SMS[42]. Member States should exchange information on their national measures and good practices for preventing smishing and vishing attacks.

TR4. Exchange good practices and develop technical guidelines on the security of home routers – While there are many vulnerable user devices, such as IoT products, which are connected to the networks, CPE and in particular home routers are deployed by telecom operators at scale, by thousands, sometimes millions. If these Internet modems are shipped with software vulnerabilities, then attackers can create botnets with thousands or even millions of infected devices. This in turn would give attackers a large foothold for subsequent attacks, for launching massive DDoS attacks (see risk scenario R5) or for targeting the sensitive information of subscribers. In collaboration with BEREC[43], ENISA should develop technical guidelines on the security of home routers.

4.2.1. Network traffic routing security (Telecoms-as-a-shield)

TR5. Exchange good practices and develop technical guidelines about blocking of cyber-attacks by operators - It is not always clear if operators of public electronic communications networks and core Internet infrastructure are allowed to filter or block cyber-attacks, under the EU's telecom security rules, the EU's net-neutrality rules, communications secrecy laws and other legal aspects, including the protection of personal data and EU fundamental rights. Member States should exchange good

[41] In 2022, ENISA developed a basic SS7 security checklist for national telecom authorities. This checklist was shared only privately with the EU's telecom security authorities. An earlier ENISA publication gives a general overview of threats and measures. ENISA, Signalling Security in Telecom SS7/Diameter/5G, 28 March 2018, https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g

[42] A more secure alternative for two-factor authentication via SMS would be to use a mobile authenticator application.

[43] In 2020, BEREC published guidelines on the identification of the Network Termination Point, clarifying which customer premise equipment falls under the responsibility of the operator.

practices about filtering and blocking of cyber-attacks[44]. ENISA should, in collaboration with the sector, BEREC and national authorities, develop technical guidelines about how filtering and blocking can be done, within net-neutrality and communications secrecy laws and in compliance with the Open Internet Regulation[45].

TR6. Facilitate sharing of good practices on mitigating very large DDoS attacks - While most entities in critical sectors should be able to mitigate normal-size DDoS attacks with standard DDoS protection methods and services, which are readily available in the market, very large DDoS attacks may be difficult to mitigate even for large operators with advanced capabilities. ENISA, in collaboration with BEREC, should facilitate an exchange of good practices on the mitigation of very large DDoS attacks, between national authorities and large operators of public electronic communications networks and core Internet infrastructure.

4.2.2. Submarine cables

TR7. Exchange good practices and develop technical guidelines on the resilience of submarine cables - Member States should exchange good practices about the resilience of submarine cables, for instance within the NIS Cooperation Group and with the CER authorities. Good practices from the energy sector for the protection of submarine power cables should be considered. Based on this exchange of good practices, ENISA should develop technical guidelines for national competent authorities in the Member States to support them in supervising the security of submarine cables and landing stations.

4.2.3. Satellite communications networks

TR8. Develop good practices in the area of securing satellite networks – Member States competent authorities have a lot of experience with the supervision of mobile and fixed network operators. However, there is much less experience and knowledge about the security of satellite networks, and particularly low-orbit satellite networks. ENISA should collaborate with BEREC and Member States national competent authorities to improve the understanding about this subsector and, if needed, support them with specific technical guidelines.

4.2.4. Core Internet infrastructure

TR9. Raise awareness of BGP security and promote good practices for the security of global Internet routing – The issues with BGP security are well known[46] and there are industry initiatives addressing these issues (such as Mutually Agreed Norms for Routing Security (MANRS)). ENISA and Member States should raise awareness about BGP security and promote the adoption of good Internet routing practices.

---

[44] In the past, ENISA published a guideline which aims to clarify some of these issues, mostly within the context of EU net neutrality rules. ENISA, Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation, 12 December 2018, https://www.enisa.europa.eu/news/enisa-news/enisa-produces-guidelines-for-assessing-security-measures-in-the-context-of-net-neutrality

[45] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open Internet access.

[46] ENISA published a basic checklist of good practices for Border Gateway Protocol routing. ENISA, 7 Steps to shore up the Border Gateway Protocol, 17 May 2019, https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp

TR10. Develop guidelines to support Member States with cybersecurity supervision of IXPs and CDNs – Although Member States have over a decade of experience in supervising operators of public communications networks, they have much less experience when it comes to cybersecurity supervision of IXPs (in scope of NIS1) and CDNs (in scope of NIS2). The NIS Cooperation Group should develop guidelines for security measures for IXPs and CDNs to support NIS competent authorities with supervising this subsector.

5. Conclusions and next steps

Ensuring the cybersecurity and resilience of communications networks and infrastructures is a key priority for the Union, even more so in the current geopolitical landscape. In response to the Nevers Call of European Telecom Ministers of 9 March 2022 and building on the coordinated work already done at EU-level to strengthen the security of 5G networks, the NIS Cooperation Group assessed risks for the connectivity infrastructure as a whole, covering the public communications networks (mobile and fixed networks, satellite networks) as well as the core Internet infrastructure (routing of Internet traffic, submarine and underground cables, IXPs and data centres, TLDs and DNS). The focus of this risk assessment was on the risk of cyber-attacks on the EU's communications networks and infrastructures (including physical attacks on network and information systems) by a hostile third country.

Firstly, based on this high-level risk assessment, Member States identified the following key threats for the communications networks and core Internet infrastructure:

- Wiper/ransomware attacks;
- Supply chain attacks;
- Attacks on a M(S)SP or other third-party service provider;
- Network intrusions;
- DDoS attacks;
- Physical attack/sabotage;
- Nation state interference on a supplier;
- Interconnection attacks;
- Power cuts affecting communications networks and infrastructures;
- Insider threats.

Secondly, based on these threats, and considering a number of vulnerabilities and dependencies, Member States identified a set of ten key risk scenarios, in addition to the risk scenarios already identified in the EU Coordinated risk assessment of 5G networks:

- Wiper attack to cause a large-scale network outage;
- Supply chain attack to gain access to the infrastructure of operators;
- Network intrusion as a preparation for future cyber-attacks;
- Third-country interference on a supplier, M(S)SP or submarine cable;
- DDoS attack to cause a large-scale network outage;
- Coordinated physical sabotage/attack on digital infrastructure;
- SS7 signalling attack to intercept communications and geolocation of target persons;
- Smishing attack to gain access to systems in other sectors;
- Power cut to cause a regional network outage;
- Interconnection attack to cause a large-scale network outage.

Thirdly, based on this risk assessment, Member States put forth a number of strategic and technical recommendations. As regards strategic aspects, it is recommended to:

- Assess resilience of international interconnections and clarify mandate;
- Assess criticality, resilience and redundancy of core Internet infrastructure, such as submarine cables;
- Implement the recommendations related to suppliers in the second Progress Report on the EU Toolbox implementation;
- Create transparency on the landscape of suppliers and M(S)SPs used for fixed networks, fibre technology, submarine cables, satellite networks and other important ICT suppliers;
- Involve the sector in cyber exercises and operational collaboration;
- Foster information sharing and improve situational awareness about threats for operators;
- Provide funding support to operators for technical measures against cyber-attacks in their networks;
- Exchange good practices among national authorities about physical attacks on digital infrastructure;
- Extend physical stress testing of critical infrastructure to include digital infrastructure.

As for technical aspects, it is recommended to:

- Implement the recommendations related to technical measures in the second Progress Report on the EU Toolbox implementation;
- Continue supporting Member States with the implementation of the technical measures of the EU Toolbox;
- Exchange good practices to support the detection and prevention of signalling attacks;
- Exchange good practices to mitigate smishing attacks;
- Exchange good practices and develop technical guidelines on the security of home routers;
- Exchange good practices and develop technical guidelines about blocking of cyber-attacks by operators;
- Facilitate sharing of good practices on mitigating very large DDoS attacks;
- Exchange good practices and develop technical guidelines on the protection of submarine cables;
- Develop good practices in the area of securing satellite networks;
- Raise awareness of BGP security and promote good practices for the security of global Internet routing;
- Develop guidelines to support Member States with the cybersecurity supervision of IXPs and CDNs.

Given the criticality of the infrastructures and networks in scope of this report and in view of the fast-evolving threat landscape, and without prejudice to the Member States' competences as regards national security, Member States, Commission and ENISA are encouraged to implement these resilience-enhancing measures as soon as possible, based on the work that has already started on the implementation of some of the recommendations. This report also provides information to the ongoing cross-sector cyber risk evaluation and scenarios on the telecommunication and part of the energy sectors requested by the Council conclusions on the EU's Cyber Posture.

6. Annexes

Annex 1. Threats

Threats	Risk scenarios
T1. Wiper/ransomware attacks	R1
T2. Supply chain attacks	R2
T3. Attacks on an M(S)SP or other third-party service provider	R2, R4
T4. Network intrusions	R1, R3
T5. Distributed denial-of-service (DDoS) attacks	R5
T6. Physical attack/sabotage	R6, R8
T7. Nation state interference on a supplier	R4
T8. Interconnection attacks	R7, R10, R8
T9. Power cuts affecting communications networks and infrastructures	R9
T10. Insider threats	R4

Annex 2. Telecom security threat landscape

This annex gives a broader overview of threats relevant for operators. ENISA has been collecting major incident reports from the EU's telecom sector over the last decade. This reporting for the most part covers incidents that surpass large quantitative thresholds, based on the number of users and hours of the resulting service outages. In general, the major incidents reported (about 160 major incidents each year, from across the EU) fall into four main categories:

- System failures, typically software or hardware failures (about 60% of reported incidents);
- Human errors (about 20% of reported incidents);
- Natural phenomena (about 10% of the reported incidents);
- Malicious actions (about 10% of the reported incidents).

When looking at the detailed causes, the most common causes of reported incidents are:

- Hardware failures;
- Software bugs;
- Faulty software changes or updates;
- Overload;
- Policy or procedure flaws;
- Faulty hardware;
- Power cuts.

Telecom security incidents reported via this mandatory incident reporting process constitute only a part of all the cybersecurity incidents affecting telecom operators. For instance, Subscriber Identity Module (SIM) swapping and SS7 attacks are often not reported, because they do not result in large-scale outages.

GSMA, a global association for mobile network operators and suppliers, publishes a yearly threat landscape, which lists the following threats for mobile network operators:

- Supply chain attacks;
- Ransomware attacks;
- Malware;
- Spyware;
- Smishing;
- Attacks on critical national infrastructure;
- Fraudulent SIM swapping;

- Inter-connection attacks;
- Attacks on virtualised and cloud-based infrastructure;
- Human threats.

Annex 3. Vulnerabilities

Vulnerabilities	Risk scenarios
V1. Vulnerable network equipment	R2, R3
V2. Vulnerable routing and interconnection protocols	R1, R5, R7, R8, R10
V3. Vulnerable network management and operation	R1, R5, R7, R8
V4. Vulnerable end-user devices	R5
V5. Vulnerable physical infrastructure	R6
V6. Dependencies on suppliers and M(S)SPs	R1, R2, R4
V7. Power supply dependencies	R9
V8. Dependency on technical expertise	R1, R5, R10

Annex 4. Risk scenarios

The EU Coordinated risk assessment on the cybersecurity of 5G networks of 2019 identifies the following nine risk scenarios for 5G networks:

Risk categories	Risk scenarios
Insufficient security measures	Misconfiguration of networks
	Lack of access controls
5G supply chain	Low product quality
	Dependency
Modus operandi of main threat actors	State interference through 5G supply chain
	Exploitation of 5G networks by organised crime
Interdependencies between 5G networks and other critical systems	Significant disruption of critical infrastructures or services
	Massive failure of networks due to interruption of electricity supply or other support systems
End user devices	IoT exploitation

In addition, the present risk assessment identifies the following ten risk scenarios for communications networks and infrastructures:

Risk level	Risk scenarios	Threats	Vulnerabilities
High	R1. Wiper attack to cause a large-scale network outage	T1, T4	V1, V2, V3, V6, V8
	R2. Supply chain attack to gain access to the infrastructure of operators	T2, T3	V1, V6
	R3. Network intrusion as a preparation for future cyber-attacks	T4	V1
	R4. Third-country interference on a supplier, M(S)SP or submarine cable	T7, T3, T10	V6
	R5. DDoS attack to cause a large-scale network outage	T5	V2, V3, V4, V8
	R6. Coordinated physical sabotage/attack on digital infrastructure	T6	V5

	R7. SS7 signalling attack to intercept communications and geolocation of target persons	T8	V2, V3
High to moderate	R8. Smishing attack to gain access to systems in other sectors	T8	V2, V3
Moderate	R9. Power cut to cause a regional network outage	T6, T9	V7
Low	R10. Interconnection attack to cause a large-scale network outage	T8	V2, V6, V8

Annex 5. Recommendations

Recommendations	Risk scenarios	Relevant stakeholders
Strategic recommendations		
SR1. Assess resilience of international interconnections and clarify mandate	R6, R10, R9	Member States, European Commission, ENISA
SR2. Assess criticality, resilience and redundancy of core Internet infrastructure, such as submarine cables	R6, R9	Member States, European Commission, ENISA
SR3. Create transparency on the landscape of suppliers and M(S)SPs used for fixed networks, fibre technology, submarine cables, satellite networks and other important ICT suppliers	R2, R4	Member States, ENISA, BEREC
SR4. Involve the sector in cyber exercises and operational collaboration	R1 to R10	Member States, European Commission, ENISA
SR5. Foster information sharing and improve situational awareness about threats for operators	R1 to R10	Member States, European Commission, ENISA
SR6. Provide funding support through relevant funding programmes to operators for technical measures against cyber-attacks in their networks	R5, R1, R10, R7, R8	European Commission, ENISA
SR7. Exchange good practices among national authorities about physical attacks on digital infrastructure	R6	Member States
SR8. Extend physical stress testing of critical infrastructure to include digital infrastructure	R6, R9	Member States, European Commission
Technical recommendations		
TR1. Continue supporting Member States with the implementation of the technical measures of the EU Toolbox	Risk scenarios from the EU Coordinated risk assessment on 5G	Member States, ENISA
TR2. Exchange good practices to support the detection and prevention of signalling attacks	R4	Member States, ENISA
TR3. Exchange good practices to mitigate smishing attacks	R8	Member States, ENISA, BEREC
TR4. Exchange good practices and develop technical guidelines on the security of home routers	R5	Member States, ENISA, BEREC
TR5. Exchange good practices and develop technical guidelines about blocking of cyber-attacks by operators	R5	Member States, ENISA, BEREC

TR6. Facilitate sharing of good practices on mitigating very large DDoS attacks	R9	Member States, ENISA, BEREC
TR7. Exchange good practices and develop technical guidelines on the protection of submarine cables	R6, R9	Member States, European Commission, ENISA
TR8. Develop good practices in the area of securing satellite networks	R1	Member States, ENISA, BEREC
TR9. Raise awareness of BGP security and promote good practices for the security of global Internet routing	R10	Member States, ENISA
TR10. Develop guidelines to support Member States with the cybersecurity supervision of IXPs and CDNs	R6, R10	Member States, ENISA