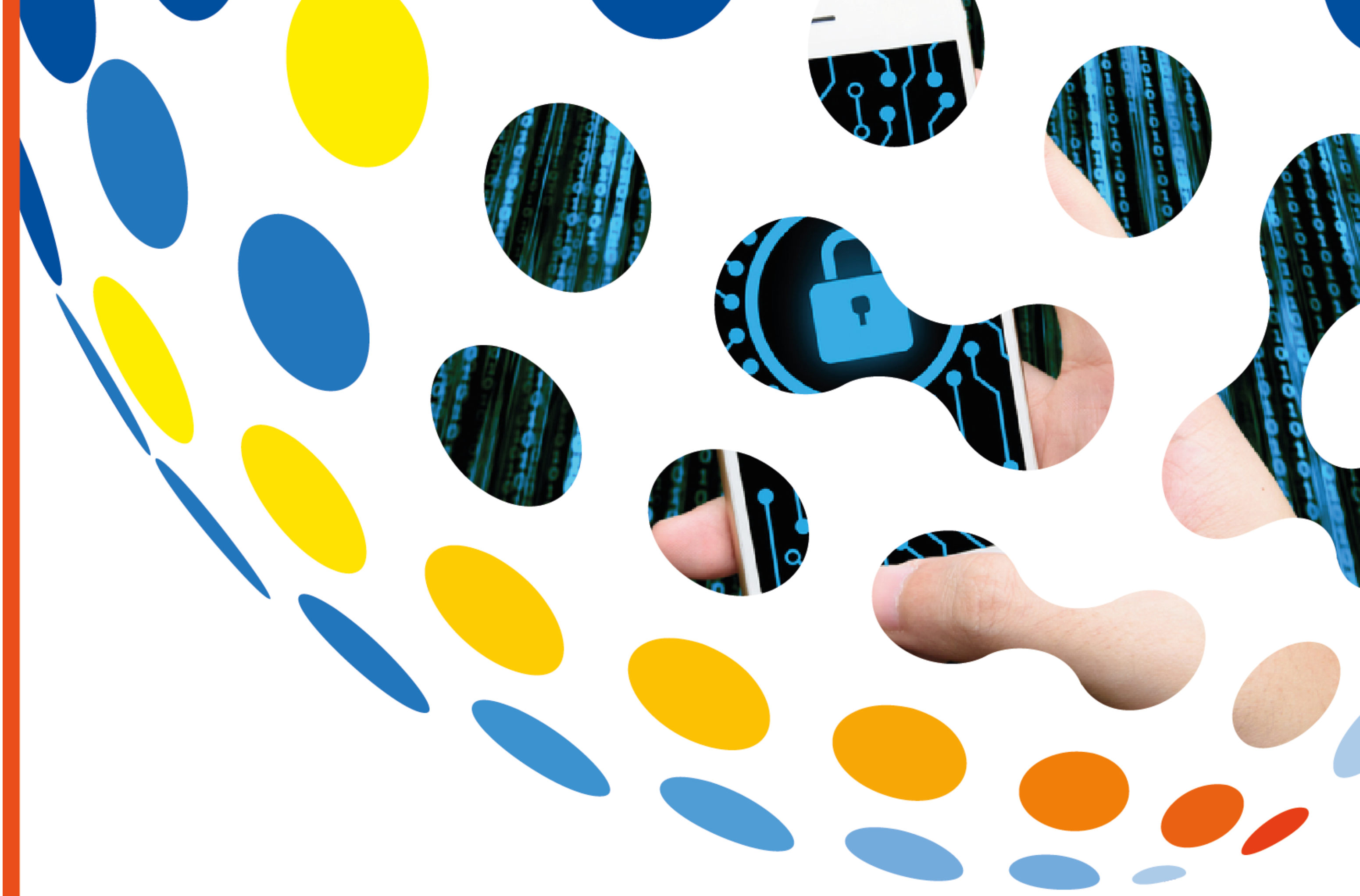

EU coordinated risk assessment of the cybersecurity of 5G networks

Report

9 October 2019

NIS COOPERATION GROUP

Table of content

1. Introduction

1.1. 5G networks will play a central role in achieving the digital transformation of the EU's economy and society. Indeed, 5G networks have the potential to enable and support a wide range of applications and functions, extending far beyond the provision of mobile communication services between end-users. With worldwide 5G revenues estimated at €225 billion in 2025[1], 5G technologies and services are a key asset for Europe to compete in the global market.

1.2. The cybersecurity of 5G networks is therefore essential to protect our economies and societies and to enable the full potential of the important opportunities they will bring. It is also crucial for ensuring the strategic autonomy of the Union.

Policy context and process

1.3. Following the support expressed by the European Council on 22 March to a concerted approach to the security of 5G networks, the European Commission adopted the Commission Recommendation Cybersecurity of 5G network[2] (hereafter 'The Recommendation'). The Recommendation identifies a number of concrete actions, which will support the development of a Union approach to ensuring the cybersecurity of 5G networks. In particular, it requests each Member State to carry out a national risk assessment of the 5G network infrastructure.

1.4. In July 2019, Member States submitted the results of their national risk assessments to the Commission and ENISA, based notably on a questionnaire. The information provided by Member States allowed the collection of information on main assets, threats and vulnerabilities[3] related to 5G infrastructure and main risk scenarios, describing potential ways in which threat actors could exploit a certain vulnerability of an asset in order to impact government objectives.

[1] ABI Research projection: https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue.

[2] (EU) 209/534 of 26 March 2019

[3] As defined by the ISO/IEC: 27005 standard.

1.5. Member States were asked to answer the questionnaire based on the results of their national 5G cybersecurity risk assessments, from the perspective of the governments (i.e. legislators/regulators), supported, where necessary, by other stakeholders' views (including network operators or suppliers). The work to develop national risk assessments involved a range of responsible actors in the Member States, such as, in particular, cybersecurity and telecommunication authorities, security, and intelligence services.

1.6. According to the Recommendation, these national risk assessments should form the basis for a coordinated Union risk assessment.

1.7. For this purpose, EU Member States agreed this high-level report, which was prepared with the support of the Commission and together with ENISA.

1.8. To complement this report, ENISA is finalising a dedicated threat landscape mapping, which consists of a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting them specifically.

1.9. This high-level report sets out the key common findings emerging from the national risk assessments of 5G networks carried out by each Member State. It highlights the elements that are of particular strategic relevance for the EU. As such, it does not aim at presenting an exhaustive analysis of all relevant aspects or types of individual cybersecurity risks related to 5G networks.

1.10. This report represents a first step in a process aimed at ensuring the solid and long-term security of 5G networks. As the 5G technology and the connected applications evolve, and in view of the fast-moving threat environment, this report may be reviewed annually or when necessary within the NIS Cooperation Group. Any future reviews should take into account relevant developments at national level.

1.11. The coordinated Union risk assessment will serve as a basis for the preparation of a toolbox of possible risk mitigation measures. This is in line with the Recommendation, which calls on Member States to agree on a toolbox by 31 December 2019. This will be carried out within the NIS Cooperation Group.

Scope: 5G networks and related applications

1.12. This report takes as a basis the definition of 5G networks provided in the EU Commission Recommendation:

> *‘5G networks means a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy networks elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network.’*

1.13. 5G networks will provide virtually ubiquitous, ultra-high bandwidth and low latency connectivity not only to individual users but also to connected objects. Thanks to these technical characteristics, 5G networks are expected to serve a wide range of applications and sectors. As mentioned in the Recommendation, these could include a *‘diverse range of services essential for the functioning of the internal market as well as for the maintenance and operation of vital societal and economic functions – such as energy, transport, banking, and health, as well as industrial control systems. The organisation of democratic processes, such as elections, is also expected to rely more and more on digital infrastructure and 5G networks’.*

1.14. In this context, it should be noted that while the main properties and functions of future 5G networks are already well known and described in particular in the 3GPP norm, the technology and its precise architecture is still evolving. Moreover, since 5G networks have not been yet fully rolled out in EU Member States, potential new use cases are not yet in operation. This creates certain limitations, which have been taken into account in the risk assessment process.

Key technological novelties of 5G networks

1.15. From a technological perspective, 5G networks will make use of a number of new technical features, compared to the current situation in existing networks:

- A move to software and virtualisation through ***'Software Defined Networks (SDN) and Network Functions Virtualisation (NFV) technologies'***. This will represent a major shift from traditional network architecture as functions will no longer be built on specialised hardware and software. Instead, functionality and differentiation will take place in the software. From a security perspective, this may bring certain benefits by allowing for facilitated updating and patching of vulnerabilities. At the same time, such increased reliance on software, and the frequent updates they require, will significantly increase the exposure to the role of third-party suppliers and the importance of robust patch management procedures.

- ***'Network slicing'*** will make it possible to support to a high degree the separation of different service layers on the same physical network, thus increasing the possibilities to offer differentiated services over the whole network. Network slicing features will require the roll-out of a new core network, i.e. replacing the 4G core network with a 5G core network, following the so-called "Stand-Alone" network architecture.

- Enhanced functionality at the edge of the network and a less centralized architecture than in previous generations of mobile network: this is reflected both in enhanced connectivity options within the radio access network, and in support for '***Mobile Edge Computing'***, which allows the network to steer traffic to computing resources and third-party services close to the end-user, thus ensuring low response times.

1.16. These new features will bring numerous new security challenges. In particular, they will give additional prominence to the complexity of the telecoms supply chain in the security analysis, with various existing or new players, such as integrators, service providers or software vendors, becoming even more involved in the configuration and management of key parts of the network. This is likely to intensify further the reliance of mobile network operators on these third-party suppliers. In addition, the distribution of responsibilities will also become more complex, with the specific challenge that some new players lack familiarity with the mission-critical aspects of telecom networks. This source of risk will become even more important with the advent of network slicing, the differing security requirements per slice and the subsequent increase in attack surface.

1.17. Moreover, some sensitive functions currently performed in the physically and logically separated core are likely to be moved closer to the edge of the network, requiring relevant security controls to be moved too, in order to encompass critical parts of the whole network, including the radio access part. If not managed properly, these new features are expected to increase the overall attack surface and the number of potential entry points for attackers, as well as increase chances of malicious impersonation of network parts and functions.

1.18. At the same time, 5G technologies and standards could improve security compared to previous generations of mobile networks, due to several new security functions, such as stricter authentication processes in the radio interface. These new security features will however not all be activated by default in the network equipment, and therefore their implementation will greatly depend upon how the operators deploy and manage their networks.

1.19. 5G security issues are increasingly being addressed in the work undertaken by standards bodies, notably within the workgroup Service and System Aspects 3 (SA3)[4] of the 3rd Generation Partnership Project (3GPP)[5].

1.20. The SA3 Working Group is also addressing the lawful interception requirements in 5G systems and is intending to produce all specifications needed to meet those requirements. Indeed, a new integrated approach and new processes are needed for maintaining the possibility of timely response to law enforcement and judicial needs, in

[4] The Service and System Aspects 3 (SA3) Working Group is responsible for security and privacy in 5G standards.

[5] The 3GPP is the main global body for developing standards for mobile communications, a collaboration between seven Organisational Partners, from Europe (ETSI), USA (ATIS), China (CCSA), Japan (ARIB, TTC), Korea (TTA) and India (TSDSI). 3GPP technical specification groups have standardised industry security features in 3G, 4G and now 5G standards.

particular through lawful interception functions[6]. Regional standards bodies are also involved in this work.

5G ecosystem and deployment in the EU

1.21. The EU 5G Action Plan[7] aims at boosting EU efforts for the deployment of 5G infrastructures and services across the Digital Single Market. It sets out a roadmap for public and private investment on 5G infrastructure in the EU and a target of the end of 2020 at the latest for the launch of commercial 5G networks. The specific timing of the deployment of 5G networks varies among Member States and among mobile network operators. Member States are at various stages of their national process of licensing relevant spectrum bands. A number of EU operators have already launched commercial offerings but large-scale 5G deployment on an EU-wide basis will only really begin in 2020. This also implies differences in how advanced operators are in the process of procuring 5G equipment and services and defining potential new security requirements.

1.22. According to available information on mobile operators' deployment plans, some of the new functionalities described above will be introduced following a phased approach. In a first phase (very short or short-term), 5G deployment will consist primarily in 'Non-Standalone' networks, where only the radio access network is upgraded to 5G technology, and otherwise still relies on existing 4G core networks, which will provide enhanced mobile broadband performances to end-users. This first upgrade will build primarily on infrastructure already in place, meaning that the security of future 5G networks may be to a certain extent determined by current network equipment and its configuration.

1.23. During subsequent phases (short/mid-term to long-term), deployment of 'Standalone' 5G networks, including 5G core network functions, and the introduction of the previously described new functionalities in 1.15 which will underpin innovative and

[6] From a cybersecurity perspective, risks related to the potential compromise of lawful interception functions in 5G networks are addressed in other sections of this report.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "5G for Europe: An Action Plan" - COM(2016)588 and Staff Working Document - SWD(2016)306.

critical services, will require and result over time in a much more extensive change in the network architecture.

1.24. The main stakeholders in the 5G networks infrastructure are:

- **Mobile network operators (MNOs):** entities providing mobile network services to users, operating their own network with the help of third parties[8].

- **Suppliers of mobile network operators:** entities providing services or infrastructure to MNOs in order to build and/or operate their networks. This category includes:
  - Telecom equipment manufacturers;
  - Other third-party suppliers, such as cloud infrastructure providers, systems integrators, security and maintenance contractors, transmission equipment manufacturer.

- **Manufacturers of connected devices and related service providers**: entities providing objects or services that will connect to the 5G networks (e.g. smartphones, connected vehicles, e-health) and related service components hosted in 5G control plane as defined in Service Based Architecture or Mobile Edge Computing.

- **Other stakeholders:** including service and content providers and end-users of 5G mobile networks.

1.25. All these stakeholders constitute important security stakeholders, both in terms of contributing to the cybersecurity of 5G networks as well as potential entry points or vectors for attacks. It is therefore important to assess risks related to their position in the 5G ecosystem in order to ensure they operate in an appropriately secure manner.

[8] Mobile virtual network operators (MVNOs) and critical infrastructure operators from another sector than telecommunications, which could operate 5G networks for their own activities or on behalf of third parties, would fall under a similar category of stakeholders.

1.26. Among them, two stakeholders are of particular relevance to the cybersecurity of 5G networks: on the one hand, mobile network operators have a central, decision-making role, giving them leverage on the overall secure operation of their networks, and on the other hand, telecom equipment manufacturers, who are responsible for the provision of software and hardware required to operate networks.

1.27. Mobile network operators providing services in the EU are subject to Union and to Member States' national law. In particular, they may be subject to general authorisation, i.e. a legal framework[9] ensuring rights for the provision of electronic communications networks or services and laying down sector-specific obligations, which responsible national authorities have the power to enforce. Mobile network operators providing services in the EU show a number of differences in certain aspects such as ownership, market strategies, market positioning as well as strategies regarding the selection of suppliers for equipment, systems and services. For instance, certain operators are deploying and running their networks using multiple equipment suppliers while other tend to rely on one supplier, for some or for most parts of their network.

1.28. The market for telecom equipment is mainly characterised by a handful of global companies capable of supplying large telecommunications operators with the technology required. From a market share perspective, the main suppliers are Huawei, Ericsson and Nokia. Other suppliers include ZTE, Samsung and Cisco[10]. Some of these suppliers are headquartered in the EU (Ericsson and Nokia) while the others are headquartered outside the EU. Their corporate governance presents notable differences, for example in terms of level of transparency and type of corporate ownership structure.

1.29. In addition, other important third-party suppliers of mobile network operators include a range of sub-contractors, providing a variety of services (e.g. network management and maintenance, data centres, etc.). The move to software-based networks and their

[9] EU framework in the field of electronic communications (Directive 2002/21/EC) and the Electronic Communications Code (Directive 2018/1972), which replaces the EU Framework and must be transposed by Member States.

[10] Cisco provides virtualised RAN solutions but does not supply a complete range of equipment and services as the other companies mentioned.

virtualisation will further facilitate the possibility that key network functions will be managed by such sub-contractors, which may be located in a different Member State than the mobile network operator's or in a third country.

1.30. Also relevant is the general context of complex and interdependent nature of the global supply chain and the fact that a large part of the manufacturing and third line support of many systems is undertaken outside the EU.

2. EU Member States' assessment of 5G cybersecurity risks

Methodology

2.1. This document follows the approach set out in the ISO/IEC: 27005 risk assessment methodology. It reflects the assessment of a set of parameters:

- the main types of threats posed to 5G networks,
- the main threat actors,
- the main assets and their degree of sensitivity,
- the main vulnerabilities,
- the main risks and related scenarios.

2.2. As all future use cases are not yet fully known. The EU approach to the assessment of 5G cybersecurity risks is therefore modelled on assumptions about use cases and possible scenarios.

A. Threats and threat actors

Threats

2.3. The deployment of 5G networks is taking place in a complex global cybersecurity threat landscape, notably characterised by an increase in supply-chain attacks.

2.4. Overall, threats considered most relevant are the main traditional categories of threats: this concerns threats related to the compromise of confidentiality, availability and integrity.

2.5. More specifically, a number of threat scenarios targeting 5G networks were found to be particularly concerning:

- Local or global 5G network disruption (Availability);
- Spying of traffic/data in the 5G network infrastructure (Confidentiality);
- Modification or rerouting of the traffic/data in the 5G network infrastructure (Integrity and/or Confidentiality);
- Destruction or alteration of other digital infrastructures or information systems through the 5G networks (Integrity and/or Availability).

2.6. An important difference compared with threats to existing networks concerns the nature and intensity of potential impacts of threats. In particular, greater reliance on economic and societal functions on 5G networks could significantly worsen the potential negative consequences of disruptions. As such, the integrity and availability of those networks will become major concerns, on top of the existing confidentiality and privacy requirements.

2.7. The severity of specific threat scenarios to 5G networks may thus vary according to a number of factors, in particular:

- the number and type of users impacted;
- the length of time of the event before detection or remediation;
- the type of services impacted (public security, emergency services, health, governmental activities, electricity, water, etc.) and the extent of damage or economic losses;
- the type of information breached.

Threats actors

2.8. The table below describes the various threat actors assessed by the Member States.

TITLE	DESCRIPTION
Non-Adversary/ Accidental	Non-adverserial/accidental threats manifest themselves as events that result from human error, natural phenomena, and systems failures.
Individual hacker	Individual hackers represent amateur criminal or hobbyist hackers driven by financial motivation or a desire for notoriety.
Hacktivist group	This threat actor has a political agenda. Their goal is to either create public attacks that help them distribute propaganda, or to cause damage to organizations they are opposed to. The ultimate goal is to find a way to benefit their cause or gain awareness for their issue.
Organised crime group	Organised crime groups are motivated by financial gain.
Insider	In the context of the security of 5G networks an insider threat refers to an insider working within a mobile network operator, or a mobile network's supplier. An insider may work for an organised crime group, a hacktivist group or a State actor, but individual motivations are not excluded.
State actor or state-backed actor	The motivations of this category of attacker are primarily political.
Other possible actors: Cyber-terrorists and corporate entities	Cyber terrorists are motivated by political aims and are likely to have very similar capabilities as an organised crime group. Corporate entities may seek to gain competitive advantage in the technological area through Intellectual Property (IP) theft, theft of sensitive commercial data or by causing reputational or operational damage to their global competitors through cyberattacks.

2.9. The relevance of the threat actors in the 5G context has been assessed by combining two parameters: the estimation of their capabilities (resources) and their intention to perform or attempt attacks against 5G network infrastructures (motivation).

2.10. Threats posed by States or State-backed actors, are perceived to be of highest relevance. They represent indeed the most serious as well as the most likely threat actors, as they can have the motivation, intent and most importantly the capability to conduct persistent and sophisticated attacks on the security of 5G networks.

2.11. The combination of motivation, intent and a high-level capability enables States to perpetrate attacks that can be very complex and have a major impact on essential services for the general public, deteriorating the trust in mobile technologies and operators. For example, States or State-backed actors can cause large-scale outage or significant disturbance of telecommunications services by exploiting undocumented functions or attacking interdependent critical infrastructures (e.g. power supply).

2.12. In relation to State and State-backed actors, a particular threat stems from cyber offensive initiatives of non-EU countries. Several Member States have identified that certain non-EU countries represent a particular cyber threat to their national interests, based on previous modus operandi of attacks by certain entities or on the existence of an offensive cyber programme of a given third State against them.

2.13. It is also noted that insiders or subcontractors can in certain circumstances also be considered potential threat actors, especially if leveraged by States as they could be used as a channel for a State to gain access to critical target assets.

2.14. Further categories of actors could also be considered to have an important motivation to target 5G networks in order to serve their interest, i.e. organised crime groups, corporate entities seeking to gain competitive advantage in the technological field through Intellectual Property (IP) theft or cyber terrorists.

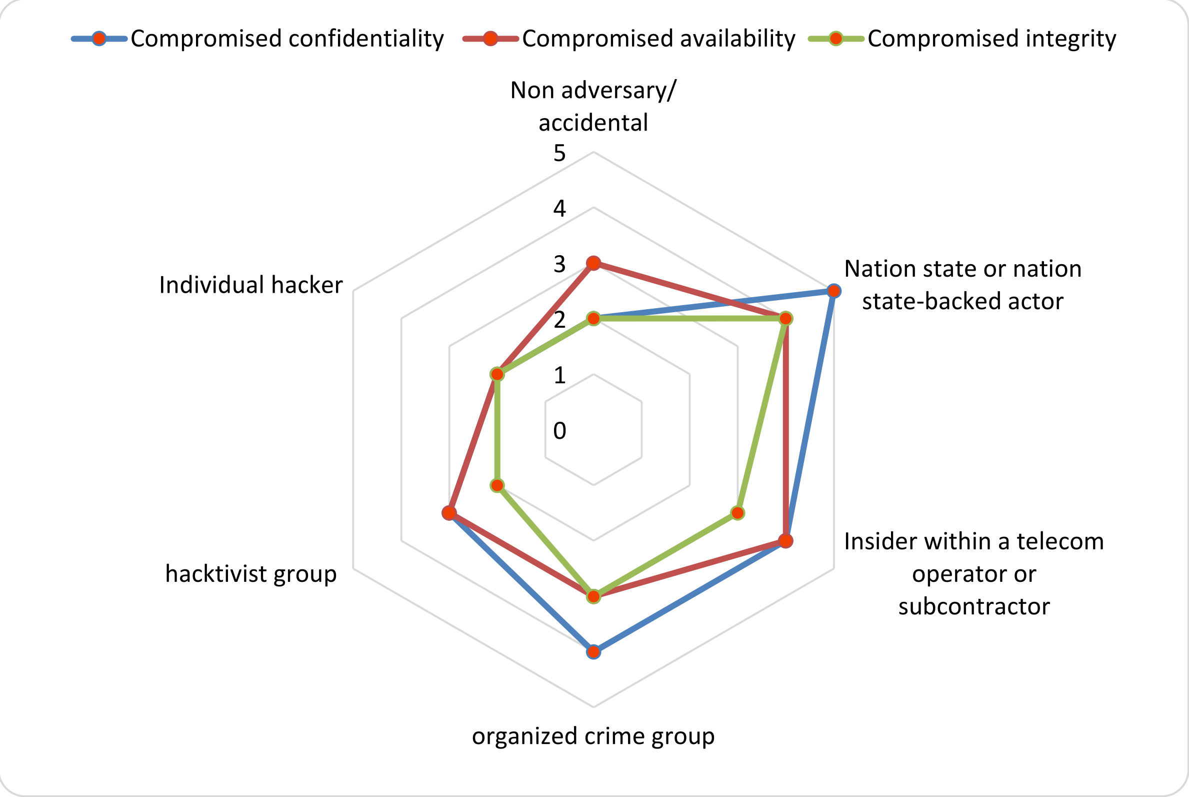

Figure 1 - Consolidated view on threat category by threat actor

2.15. As is illustrated in the chart[11], it was found that the most severe threats were posed by compromised confidentiality, availability and integrity associated with a State or State-backed actor.

2.16. Other more severe threats included:

- Compromised confidentiality and availability associated with an insider within a telecom operator/subcontractor, and
- Compromised confidentiality associated with an organized crime group.

B. Assets

2.17. The introduction of 5G represents a larger transition for operators in terms of changes in network operations than any of the previous transitions. The new functions and processes will require a thorough re-design of current networks, even though in the first phases they will continue to be based on existing 3G and 4G networks. Moreover, 5G technology is still under development and the architecture of 5G networks is not entirely fixed yet.

2.18. The assessment of the sensitivity of the main network assets presented below is based on the responses provided by Member States. Attributed ratings reflect views expressed by a large majority of Member States.

2.19. Network assets were assessed by types of logical and functional parts:

Functions that are defined in the 3GPP norm:

- ***Core functions***, providing a number of services to subscribers;
- ***Access functions***, connecting subscribers to their network provider.

Underlying Functions not defined in the 3GPP norm:

[11] Figure 1 is based on input provided by Member States. Member States were asked to fill in a table that provided a score from 0 (lowest risk) to 5 (highest risk) for each combination of threat actor and threat category. The chart displays the mean average of the scores that the Member States entered for each combination. The highest average score was 5, and there was no average score lower than a 2.

- ***Transport and transmission functions***, keeping the access network connected to the core;
- ***Internetwork exchanges***, connecting different networks with each other[12];
- ***Management systems and supporting services,*** notably managing the end-to-end network orchestration but also other less critical services such as billing or network performance.

Assessment criteria

2.20. The following main criteria were considered in order to assess the sensitivity of the various assets:

- The type of impact, i.e. whether the materialisation of a threat leads to compromised confidentiality, and/or availability, and /or integrity of the network;
- The scale of the impact, e.g. in terms of users, duration, number of base stations or cells affected, sensitivity of the information altered or accessed.

2.21. The following table presents the main categories of elements and functions and their overall level of sensitivity, and lists a number of key elements identified by Member States for each category:

CATEGORIES OF ELEMENTS AND FUNCTIONS	EXAMPLES OF KEY ELEMENTS	
Core network functions	**CRITICAL**	User Equipment Authentication, roaming and Session Management Functions
		User Equipment data transport functions
		Access policy management
		Registration and authorization of network services
		Storage of end-user and network data
		Link with third-party mobile networks
		Exposure of core network functions to external applications
		Attribution of end-user devices to network slices

[12] In the context of a mobile network, Internet Exchange Points and Transit Providers provide the services that are used by MNOs to connect to other MNOs and to the Internet (IPS domain as defined in 5GPPP 5G architecture or Data networks as defined in 3GPP TS23.501). Within this document, the term Internetwork exchange points refers to the non-telecommunication-specific infrastructure that provides this service. This infrastructure is outside the premises of the MNOs.

NFV management and network orchestration (MANO)	**CRITICAL**	
Management systems and supporting services (other than MANO)	**MODERATE/HIGH**	Security management systems
		Billing and other support systems such as network performance
Radio Access network	**HIGH**	Base stations
Transport and transmission functions	**MODERATE/HIGH**	Low-level network equipment (routers, switches, etc)
		Filtering equipment (firewalls, IPS...)
Internetwork exchanges	**MODERATE/HIGH**	IP networks external to MNO premises Network services provided by third parties

2.22**. Core network** functions of the 5G network are generally considered as critical. Indeed, affecting the core network may potentially compromise the confidentiality, availability and integrity of the entire network services (whereas compromises of other components may have a more limited impact, e.g. affecting only a specific function or area). Furthermore, the most sensitive data is transmitted through the core network components.

2.23. **Management systems and supporting services** (MANO and other management systems and supporting services) are considered as important even though these systems do not carry traffic since they control important network elements and can therefore be used to conduct malicious acts, such as sabotage and espionage of serious consequences. Moreover, the loss of availability or integrity of these systems and services can disrupt significantly the functioning of 5G networks.

2.24. **Among the core functions and management systems/supporting services,** a number of elements and functions have been considered to be of particularly high importance, notably: the NFV Management and Network Orchestration (MANO), core access and control functions, security functions, lawful interception functions, cryptographic infrastructures necessary to configure and operate 5G networks and specific management functions.

2.25. **Access network** functions were also rated with relatively high sensitivity. However, the assessment of the degree of sensitivity of specific elements within the access functions varies according to a number of factors. Furthermore, in the coming development phases of 5G, traditionally less sensitive parts of the network are gaining importance and becoming more sensitive, such as for instance certain elements in the radio access part of the network, depending on the extent to which they handle user data or perform smart or sensitive functions. Moreover, when edge computing is introduced, certain core network functions are expected to be moved physically farther out in the network, closer to the access sites.

2.26. **Transport and transmission** functions were rated as moderately to highly sensitive. However, similarly to the access functions, the assessment of the degree of sensitivity of specific elements within the transport and transmission functions varies according to a number of factors.

2.27**. Internetwork exchanges** functions were rated as moderately to highly sensitive, depending on their role in the interconnection between MNOs.

Assets other than technical
(user groups, geographical areas, critical infrastructures)

2.28. When considering key assets, a number of entities and categories of users can be considered as requiring particular attention, namely:

- Operators of essential services under NIS Directive and critical infrastructure operators;
- Government entities, law enforcement, Public Protection and Disaster Relief (PPDR), military;
- Key sectors/entities not covered by cybersecurity regulations;
- Strategic private companies;

- Areas or entities for which there is no back-up solution in place in case of 5G network failure.

2.29 In addition, a number of Member States have identified geographic areas that are particularly sensitive, based on an analysis of the demographic, economic, societal and national security factors. Indeed, certain areas could suffer greater disruption due to the concentrations of economic and societal reliance on network and information systems (e.g. as in the case of smart cities) or because sensitive entities or categories of users are located in them.

C. Vulnerabilities

Vulnerabilities related to hardware, software, processes and policies

2.30. As any digital infrastructure, 5G networks can be associated with a range of generic technical vulnerabilities, which may affect software, hardware or arise from potential deficiencies in the security processes of any of the various stakeholders[13]. Furthermore, in the early stage of deployment, vulnerabilities in the existing 3G and 4G infrastructure shall also be duly considered.

2.31. While many of these vulnerabilities are not specific to 5G networks, their number and significance is likely to increase with 5G, due to the increased level of complexity of the technology and of the future greater reliance of economies and societies on this infrastructure.

2.32. In particular, as 5G networks will be largely based on software, major security flaws, such as those deriving from poor software development processes within equipment suppliers, could make it easier for actors to maliciously insert intentional backdoors into products and make them also harder to detect. This may increase the possibility of their exploitation leading to a particularly severe and widespread negative impact.

2.33. Moreover, new types of technical vulnerabilities related to specific 5G technologies are likely to appear, affecting for example the technology used in SDN and NVF, including

[13] Reviews of the practices of one of the major network equipment suppliers as regards 4G equipment and services have been for instance carried out by the UK Huawei Cybersecurity Evaluation Centre (HSCEC).

cloud systems, and their configuration. Lawful interception functions enabling authorised public authorities to gain access to networks will also become software-based. Such processes, if not properly managed, could be misused for malicious actions.

2.34. Another type of vulnerability in the context of massive 5G use by verticals may relate to data leakages between multiple virtual environments or slices (e.g. to spy on offers/data of a competitor). Slice isolation is a key problem identified by the industry and subject of intensive work today.

2.35. Certain process or configuration-related vulnerabilities are considered to be of special significance in the future 5G environment:

For all stakeholders, in particular mobile network operators and their suppliers:

- **Lack of specialised and trained personnel to secure, monitor and maintain 5G networks:** the fast-evolving threat landscape and technology and the complexity of 5G networks will lead to an increased need for IT security professionals with specialized knowledge (e.g. competence in the areas of cloud architecture).

- **Lack of adequate internal security controls, monitoring practices, security management systems and insufficiencies in risk management practices**: this affects the ability to prevent and reduce security risks to physical and IT assets that can be caused by error, accident, natural disasters, or malicious action. Generally, effective risk mitigation should be based on robust and regular risk assessments. Furthermore, up-to-date network asset inventory is needed to respond quickly and accurately to potential error situations or vulnerability disclosures.

- **Lack or inadequate security or operational maintenance procedures, such as software update/patch management:** this vulnerability will become much more acute in 5G networks, given the much higher frequency of maintenance and system patching they will require in order to ensure security and functionality and minimize the network's exposure to security risks. As 5G networks will involve a wider range of stakeholders, including new ones (e.g. virtualization platform suppliers and various other third party service providers), overall security responsibility will be essential.

- **Lack of compliance with 3GPP standards or incorrect implementation of standards:** this would translate into a lack of adequate baseline security measures. Indeed, while standards surrounding 5G continue to be researched and developed, these standards will aim to be more secure than previous iterations of mobile wireless communications

For mobile network operators:

- **Poor network design and architecture** (including lack of effective emergency and continuity mechanisms, inappropriate or misconfiguration for instance in virtualization or of administration or access rights, etc.): this may significantly increase the exposure to negative consequences (e.g. lack of isolation of low trust systems, potentially larger scope of security breaches).

- **Poor physical security for network and IT infrastructure**: deficiencies in physical security can lead to inadequate protection of personnel, hardware, software, networks and data from any malicious actions and events.

- **Poor policies for local and remote access to network components**: 5G networks will be composed of a large amount of virtual devices, which can be remotely accessed throughout the network. This vulnerability becomes significantly more acute in cases where the maintenance of networks will be performed by third-party suppliers.

- **Lack of or insufficient security requirements in the procurement process:** this vulnerability can take the form of inadequate strategies for the selection of suppliers or a lack of prioritisation of security over other aspects in the procurement process.

- **Poor change management process:** this vulnerability could limit the possibility to prevent human errors and unauthorised configuration changes

Supplier-specific vulnerabilities

2.36. The increased role of software and services provided by third party suppliers in 5G networks leads to a greater exposure to a number of vulnerabilities that may derive from the risk profile of individual suppliers.

2.37. The risk profiles of individual suppliers can be assessed on the basis of several factors, notably:

- The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks[14.] Such interference may be facilitated by, but not limited to, the presence of the following factors:
  - a strong link between the supplier and a government of a given third country;
  - the third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country[15];
  - the characteristics of the supplier's corporate ownership;
  - the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.

- The supplier's ability to assure supply.

[14] While a threat actor's direct access to or influence on the telecom supply chain may significantly facilitate its exploitation for malicious actions and make the impact of such actions significantly more severe, it should also be noted that actors with a high level of intent and capabilities, such as State actor, would seek to exploit vulnerabilities at any stage of the product lifecycle provided by any supplier.

[15] In this context, several Member States attribute a higher risk profile to suppliers that are under the jurisdiction of third countries conducting an offensive cyber policy.

- The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

2.38. The assessment of a supplier’s risk profile may also take into account notices issued by EU authorities and/or Member States national authorities.

Vulnerabilities stemming from dependency to individual suppliers

2.39. Important vulnerabilities stem from a lack of diversity in equipment and solutions used, both within individual networks and nationally.

2.40. Within individual networks, a large degree of reliance on a single supplier (monoculture) creates a dependency on specific solutions and makes it more difficult to procure solutions from other suppliers, especially where solutions are not fully interoperable.

2.41. As a result, EU-based operators who become overly dependent on a single equipment supplier are exposed to a number of risks caused by that supplier coming under sustained commercial pressure, whether due to commercial failure, being subject to a merger or acquisition, or being placed under sanctions.

2.42. At national and EU level, a lack of diversity of suppliers increases the overall vulnerability of the 5G infrastructure, in particular if a large number of operators source their sensitive assets from a supplier presenting a high degree of risk, as described above. Dependency of one or several networks also significantly affects national and EU-wide resilience and creates single points of failure.

2.43. Moreover, the presence of a limited number of suppliers on the market can decrease their incentives to develop more secure products. It can also have a negative impact on the leverage available to national authorities and operators to demand higher security guarantees, in particular for smaller Member States or operators.

2.44. Dependency may also have different implications, depending on which types of network elements are affected and on the interoperability of the various components.

D. Risk scenarios

2.45. Based on the findings concerning the various parameters set out in the previous sections of the report, a number of categories of risks of strategic importance from an EU perspective have been identified.

2.46. These risks are described in the paragraphs below and are illustrated by concrete scenarios, which reflect possible relevant combinations of the different parameters described in the preceding sections of this report (threat, threat actors, assets and vulnerabilities).

2.47. These identified categories of risks have a number of characteristics conferring them a particularly strategic importance:

- They are based on major threats scenarios that are relevant across the EU;
- They would lead to high, very high or potentially systemic impacts;
- Their likelihood is increasing with 5G networks or they are specific to 5G networks.

2.48. It should be noted that the risks and related risk scenarios highlighted below do not cover all existing risks or all relevant combinations of parameters but aim at describing possible attack paths that a threat actor can use to reach its target.

I. Risks scenarios related to insufficient security measures

2.49. As with current 3G and 4G networks, a large number of risks originate from systems that are poorly designed or badly set up and/or configured, and from weaknesses in security measures and processes put in place by mobile network operators. With the move to 5G networks, these risks are likely to become significantly more acute, due to the novel technological characteristics of these networks and their much higher degree of complexity. This might be further exacerbated by a lack of specialists, leading also to an increase in human errors. Furthermore, the decentralization of the 5G network infrastructure makes a robust and fault-tolerant service more complex to implement.

In particular, the risk of unauthorised access to important systems is already a challenge to manage. With the introduction of 5G networks, complex technical solutions will require additional support from different types of suppliers, which will be provided both onsite and via remote access. If suppliers have access to the network, it is possible for them to manipulate certain functionalities, e.g. the lawful intercept functionality, or to intercept and/or reroute data traffic, and to bypass audit mechanisms in a way that is not easy to detect for the operator.

Related risk scenarios:

- *Misconfiguration of networks:* Exploiting poorly configured systems and architecture, a State actor penetrates into the 5G network via its external interfaces, leading to the compromise of the network core functions, or exploits edge-computing nodes in order to compromise information confidentiality and disrupt distributed services.

- *Lack of access controls*: a subcontractor with administrator's privileges on the network performs adverse action, leading to confidentiality/integrity and/or availability breach. The subcontractor's action may be due to a legal requirement imposed by a third country or rogue behaviour of the contractor's staff.

II. Risk scenarios related to the 5G supply chain

2.50. There are a number of specific security risks associated with the 5G supply chain. They include, in particular:

- **faults or vulnerabilities in equipment**, as a result of legacy equipment, poor software engineering processes or poor vulnerability management,
- **dependency on any one supplier**, either at the level of an individual network, or on a nation-wide or EU-wide scale.

2.51. ***Low quality equipment.*** The higher degree of complexity of 5G networks and their higher reliance on software and services by third-party suppliers increases the risks posed by the existence of significant defects in supplied equipment and subsequent patching process. Unidentified vulnerabilities are a leading cause of potentially undetected, long-lasting intrusions into networks, and as such endanger the confidentiality, integrity and availability of 5G networks. In this context, significant vulnerabilities may derive from poorly written code and poor software engineering process. Inferior product quality may also arise from a lack of compliance with 5G standards or from a lack of implementation of certain standardised security functions.

2.52. ***Dependency.*** Furthermore, the reliance of an MNO on a single third-party supplier or the dominance of a supplier across networks exposes a number of major vulnerabilities. In particular, it increases the risk of the impact of any systemic failures or hostile exploitation. This risk also varies depending on the risk profile(s) of the supplier(s) and may be indirect in the sense that several different operators may rely on the same supplier for a critical part of their services. Furthermore, the dependency risk is exacerbated by potential difficulties of guaranteeing backwards compatibility between new 5G equipment and existing equipment, when using different suppliers. The risk of national dependency from a single supplier is particularly acute in the access part of the network where there are fewer market players.

Related risk scenarios:

- *Low product quality:* Espionage by state or state-backed actors using malware to abuse poor quality network components or unintentional vulnerabilities affecting sensitive elements in the core network, such as Network Virtualisation Functions.

- *Dependency:* A mobile network operator sources a large amount of its sensitive network components or services from a single supplier. The availability of equipment and/or updates from this supplier is subsequently drastically reduced, due to a failure by the supplier to supply (e.g. due to trade sanctions by a third State or to other commercial circumstances). In consequence, the quality of a supplier's equipment decreases due to priority given to guaranteeing supply over improvements in product security.

III. Risk scenarios related to modus operandi of main threat actors

2.53. Certain risk scenarios are directly associated with the typical capabilities and intent of main threat actors, e.g. their potential intentions to perform certain types of attacks and their ability to leverage certain attack vectors.

In particular, hostile third countries may exercise pressure on 5G suppliers in order to facilitate 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, in particular its most sensitive assets, and by the risk profile of the individual supplier. It also increases significantly, where there are insufficient security and access controls in place. Interference could occur in various ways, e.g. by exploiting embedded unintentional vulnerabilities or through deliberately injected vulnerabilities.

In addition, 5G networks can also be the target of sophisticated malicious action by organised crime for profit. Lesser potent actors such as organized crime groups may also trade network intrusion expertise for financial gain.

Related risk scenarios:

- *State interference through 5G supply chain:* a hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities.

- *Exploitation of 5G networks by organised crime:* By taking control of a critical part of the 5G network architecture, an organized crime group disrupts various services to ransom businesses relying on those services, or the mobile network operator itself.

- Alternatively, using a similar attack path, an organised crime group may also target end-users, e.g. by injecting false messages to the users of the network as part of a large-scale “phishing” attack or online scam, or by using the compromised network to gain access to confidential data about users (e.g. second-factor authentication codes) for further profit.

IV. Risk scenarios related to interdependencies between 5G networks and other critical systems

2.54. Given the foreseen interdependencies between 5G networks and many other systems in critical areas (e.g. health, autonomous vehicles, power, gas and water supply, defence), degradation or failure of 5G services may lead to significant disruptions of these systems.

Conversely, other critical infrastructures upon which 5G networks are dependent, such as power grids and ICS systems, have known vulnerabilities that can be the targets of cyber-attacks. The potential of loss of essential services to 5G network operators is possible either due to a service failure by the service provider (e.g. power supply) or because of a cyber-attack against a Critical Information Infrastructure depended entity. Control of a dedicated slice by an actor that is external to the network may also increase exposure to cyber threats. Over the past years, many threat actors have developed these capabilities, including state-backed actors.

The consequences of these two categories of risk scenarios are significantly aggravated in case of absence of effective emergency and continuity mechanisms.

Related risk scenarios:

- *Significant disruption of critical infrastructures or services*: Malicious hackers are able to compromise emergency services by gaining control of their dedicated network slice, thus compromising the availability of the service and the integrity of the information/data used for/within that service.

- *Massive failure of networks due to interruption of electricity supply or other support systems*: Massive outage of power supply due to natural disasters or to attacks to the energy grid by a state, a state-backed actor or an organised crime group.

V. Risk scenarios related to end-user devices

2.55. This risk scenario results from the massive increase in the number and diversity of devices (especially Internet of Things devices), which will be connected to 5G networks.

These devices will span an extremely wide range of security requirements and postures, such as industry automation control devices, shipping containers, climate sensors and next-generation tablets and smartphones.

A very large number of devices simultaneously attempting to gain access to the network can indeed cause an overload of the network. Considered together with the expected growing reliance of society on 5G networks, the security implications of allowing large numbers of poorly secured devices on the network can be significant.

Related risk scenario:

- *IoT exploitation:* A hacktivist group or state-backed actor takes control of low security devices like IoT (sensors, home appliances, etc.), in order to attack the network by overwhelming its signalling plane.

E. Existing mitigating measures/security baseline

2.56. At EU level, security requirements relevant to the 5G networks ecosystem and related critical systems are set out notably in EU telecoms legislation and in the NIS Directive. Under the EU telecommunications framework, obligations can be imposed on telecommunication operators[16] by the relevant Member State(s) in which it is providing service. The NIS Directive[17] requires operators of essential services in other fields (energy, finance, healthcare, transport, water, etc.) to take appropriate security

[16] Under the Telecoms Regulatory Framework (Article 13a of Directive 2002/21/EC as amended by Directive 2009/140/EC), Member States are required to ensure that telecoms operators: a) take appropriate measures to manage security risks and b) take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks. The Electronic Communications Code (Directive 2018/1972), which replaces the Telecoms Regulatory Framework and must be transposed by Member States, contains similar provisions.

[17] Directive (UE 2016/1148) on security of Network and Information Systems (NIS Directive).

measures and to notify serious incidents to the relevant national authority. The NIS Directive also foresees coordination between Member States in case of cross-border risks and incidents.

2.57. Other relevant frameworks at EU and national level include data protection and privacy rules (in particular the General Data Protection Regulation[18] and e-Privacy Directive[19]) as well as requirements applicable to critical infrastructures.

2.58. At national level, Member States have adopted diverse approaches to the implementation of the aforementioned security provisions and to their enforcement. Where binding rules apply to mobile network operators, they may cover different types of technical and organisational measures.

2.59. In addition, various security measures may already be applied by mobile network operators, for instance: technical measures (e.g. encryption, authentication, automation, anomaly detection) or process-related measures (e.g. vulnerability management, incident and response planning, user-privilege management, disaster recovery planning).

2.60. From a standardisation perspective, 3GPP SA3 has addressed several 5G security-related concerns, advocating, inter alia, end-to end encryption. However, the work carried out within these bodies does not deal with security concerns related to the deployment and configuration of the technology.

[18] Regulation (EU) 2016/679.

[19] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

3. Conclusions and way forward

3.1. This report identifies a number of important security challenges, which the advent of 5G networks are likely to give rise to or intensify, while taking into account the evolving nature of the 5G technology and environment.

3.2. While 5G networks technology and standards will also bring certain security improvements compared with previous network generations, several important challenges derive from the novel features in the network architecture and the wide range of services and applications, which may in the future rely extensively on 5G networks.

3.3. These security challenges are also linked to the greater access of third-party suppliers to networks and to interlinkages between 5G networks and third party systems, as well as to the degree of dependency on individual suppliers.

3.4. Specifically:

a) The technological changes introduced by 5G will **increase the overall attack surface and the number of potential entry points for attackers:**

- **Enhanced functionality at the edge of the network and a less centralised architecture** than in previous generations of mobile networks means that some functions of the core networks may be integrated in other parts of the networks making the corresponding equipment more sensitive (e.g. base stations or MANO functions);

- the i**ncreased part of software** in 5G equipment leads to increased risks linked to software development and update processes, creates new risks of configuration errors, and gives a more important role in the security analysis to the choices made by each mobile network operator in the deployment phase of the network;

b) These new technological features will give greater significance to **the reliance of mobile network operators on third-party suppliers and to their role in the 5G supply chain.**

This will, in turn, increase the number of attacks paths that could be exploited by threat actors, in particular **non-EU state or state-backed actors**, because of their capabilities (intent and resources) to perform attacks against EU Member States telecommunications networks, as well as the potential severity of the impact of such attacks.

In this context of increased exposure to attacks facilitated by third-party suppliers, the individual risk profile of suppliers will become particularly important, in particular where a supplier has a significant presence within networks or areas.

c) a major **dependency** on a single supplier increases the exposure to and consequences of a potential failure of this supplier. It also aggravates the potential consequences of weaknesses or vulnerabilities, and of their possible exploitation by threat actors, in particular where the dependency concerns a supplier presenting a high degree of risk.

d) If some of the new use cases envisioned for 5G come to fruition, 5G networks will end up being an important part of the supply chain of many critical IT applications, and as such not only confidentiality and privacy requirements will be impacted, but **also the integrity and availability of those networks will become major national security concerns and a major security challenge from an EU perspective.**

3.5. Together, these challenges create a new security paradigm, making it necessary to reassess the current policy and security framework applicable to the sector and its ecosystem and essential for Member States to take the necessary mitigating measures.

3.6. This requires identifying potential gaps in existing frameworks and enforcement mechanisms, ranging from the implementation of cybersecurity legislation, the supervisory role of public authorities, and the respective obligations and liability of operators and suppliers.

3.7. In order to address the above-described risks and to make full use of potential security opportunities linked to the 5G technology, various types of measures may be considered. Among these measures, some of them are already in place, at least partially. This concerns in particular security requirements applicable to previous generations of mobile networks and which remain valid for the future deployment of 5G networks. In addition, for many of the identified risks, particularly those affecting the core or access levels, contingency approaches have been defined through standardisation by 3GPP.

3.8. However, the fundamental differences in how 5G operates also means that the current security measures as deployed on 4G networks might not be wholly effective or sufficiently comprehensive to mitigate the identified security risks. Furthermore, the nature and characteristics of some of these risks makes it necessary to determine if they may be addressed through technical measures alone.

3.9. The assessment of these measures will be undertaken in the subsequent phase of the implementation of the Commission Recommendation. This will lead to the identification of a toolbox of appropriate, effective and proportionate possible risk management measures to mitigate cybersecurity risks identified by Member States within this process.

3.10. Consideration should also be given to the development of the European industrial capacity in terms of software development, equipment manufacturing, laboratory testing, conformity evaluation, etc.